Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea Magistrale in Informatica

CYBER RISK: UN NUOVO APPROCCIO ALLA VALUTAZIONE

Relatore:
Chiar.mo Prof.
DANILO MONTESI

Candidato:
MATTEO TISCORNIA

Correlatore:
Dott.
FLAVIO BERTINI

II Sessione
Anno Accademico 2015-2016

E se diventi farfalla
nessuno pensa più
a ciò che è stato
quando strisciavi per terra
e non volevi le ali.
Alda Merini

Indice

Elenco delle figure

Introduzione

Negli ultimi anni il crescente interesse sviluppato nell'ambito del cyber risk ha posto l'attenzione sulle possibili gravi conseguenze di un evento informatico per le imprese e le società. La continua espansione delle tecnologie come strumenti di lavoro e nella realtà di tutti i giorni attraverso la diffusione dei social network, dei dispositivi mobili e dei servizi cloud ha portato ad una maggiore vulnerabilità dell'intero spazio cibernetico. Molte aziende stanno iniziando a considerare la cybersecurity come un rischio d'impresa sempre più importante e di conseguenza si sono messe alla ricerca di metodi per assicurare la continuità del proprio business in caso di attacchi informatici.
In questo elaborato si è cercato di toccare tutti i punti fondamentali che riguardano l'intera gestione del cyber-rischio. Nel Capitolo 1 viene descritto lo scenario attuale delle minacce cibernetiche, dalla loro diffusione a come sono trattate a livello normativo e istituzionale. Una volta messo a fuoco il contesto si passa ad introdurre in termini generali la gestione del rischio nel Capitolo 2, indicando le misure opportune e le strategie per la corretta gestione di quest'ultimo. L'ulteriore specializzazione del rischio nello spazio cyber è affrontato nel Capitolo 3, nel quale si definisce l'area di competenza e l'attuale situazione del mercato assicurativo, ancora in fase embrionale. Sempre in questo capitolo sono descritti i due principali metodi di valutazione ed elaborazione del rischio, ovvero metodi qualitativi e quantitativi.
Dal momento che la cybersecurity è un tema molto importante, è stato fissato uno standard a livello internazionale al fine di proteggere i sistemi e le risorse per la sicurezza del paese con il Cybersecurity Framework realizzato

dal NIST. Nel Capitolo 4, oltre ad entrare nel merito di quest'ultimo si è illustrato l'allineamento fatto dal Laboratorio Nazionale di Cyber Secuity che declina il framework nelle caratteristiche socio-economiche dei diversi settori produttivi. Quest'ultimo può essere considerato il primo documento italiano in cui si definisce la metodologia che un'azienda può seguire per rendere più sicura la propria infrastruttura informatica.
A fronte di quanto premesso, nel Capitolo 5 si va a trattare in forma teorica quella che è la formula del rischio in ogni sua parte proponendo un nuovo modello adattato allo spazio cibernetico. Infine nel Capitolo 6 si riporta, oltre alla soluzione pratica del modello, la sua realizzazione, la modalità di attuazione e la sua successiva evoluzione.

Obiettivi

Questo studio vuole occuparsi della corretta formulazione del concetto di rischio contestualizzato nello spazio cibernetico, partendo da un'analisi delle due componenti principali della formula (probabilità e impatto) evidenziandone i limiti dell'applicabilità in questo contesto. L'obiettivo consiste nel riformulare il rischio prendendo in considerazione altri aspetti come la sicurezza e l'esposizione al rischio.
Tale problematica viene affrontata da un duplice punto di vista, ovvero:

- da un lato, da parte della singola entità che deve affrontare e gestire il cyber-rischio, quindi riuscire a trattare in modo coerente e il più preciso possibile la valutazione del rischio in modo da dare la consapevolezza della dimensione del problema;

- dall'altro, dalle entità nel loro complesso, andando a individuare i punti che le accomunano e studiando le possibili correlazioni tra di esse.

Per la realizzazione di tali obiettivi si è cercato di integrare quelli che sono i fondamenti teorici con le nuove proposte avanzate dalla comunità scienti-

fica, aggiungendo un'ulteriore considerazione sulle metodologie fin ad oggi avanzate.

Motivazioni

L'applicazione del modello proposto, attraverso lo strumento realizzato, permetterebbe alle singole organizzazioni di ottenere una prima valutazione del proprio valore di cyber-rischio. Dato che l'area dell'IT risk management è in forte crescita e continuo sviluppo, l'intero progetto potrebbe essere adottato e opportunamente approfondito, per esempio, da compagnie assicurative o società di consulenza finanziaria.
Inoltre, nel caso di una compagnia assicurativa, l'intero procedimento consentirebbe un supporto sia per la stipulazione delle polizze, aggiungendo informazioni sui profili dei propri clienti, sia per la raccolta del maggior numero di dati acquisibili relativi agli assicurati e all'andamento del mercato.
Il processo di gestione del cyber-rischio, nei suoi sviluppi futuri, dovrà convergere sempre più nelle scelte condivise, a partire da quella che è la semplice condivisione delle informazioni, fondamentale per un corretto affinamento delle delle tecniche di gestione.

Capitolo 1

Cybersecurity

In questo capitolo si introducono le definizioni base riguardanti la cybersecurity, seguite dallo scenario attuale delle minacce cibernetiche e da un approfondimento sulla violazione dei dati. In chiusura si fa un accenno a quelle che sono le direttive stabilite a livello nazionale.

1.1 Definizione

Nel gennaio 2008 il presidente degli Stati Uniti d'America emana una direttiva presidenziale per la sicurezza nazionale (NSPD-54/HSPD-23), nella quale si definisce con il termine cybersecurity *"Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation"* [20]. Ovvero, consiste nella capacità di proteggere o difendere l'uso del cyberspace adeguatamente esplicitato come *"The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries"*.
Esattamente cinque anni dopo, con il decreto del presidente del Consiglio dei

ministri 24 gennaio 2013, in Italia si ha una definizione equipollente di sicurezza cibernetica: *"condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica e procedurale rispetto ad eventi, di natura volontaria od accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi"* [9]. Sempre nello stesso decreto si definisce spazio cibernetico *"l'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi"*. In questo elaborato entrambe le terminologie, cybersecurty-sicurezza cibernetica e cyberspace-spazio cibernetico verranno considerate equivalenti in quanto convergono verso una definizione comune ed internazionale.

1.2 Minacce cibernetiche

La quantità ingente di dati aziendali e relativi allo status patrimoniale degli individui, che è in continua crescita all'interno dello spazio cibernetico, assieme al sempre maggior utilizzo di quest'ultimo per attività finanziarie, economiche e commerciali, rendono gli attacchi cibernetici una vera minaccia per l'impatto economico globale.
A seconda degli attori e delle finalità si distinguono quattro tipologie di minacce cibernetiche[1];

1. Cybercrime: complesso delle attività con finalità criminali come la truffa o la frode telematica, il furto d'identità, la sottrazione di informazioni o di creazioni e proprietà intellettuali;

[1] *"Complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanzia in particolare, nelle azioni di singoli individui o organizzazioni, statuali e non, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro modifica o distruzione illegittima, ovvero a danneggiare, distruggere o ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi"* [9].

2. Hacktivism: perseguimento di obiettivi sociali e politici attraverso la pirateria informatica, termine derivante dall'unione delle parole hacking e activism;

3. Espionage: acquisizione indebita di dati/informazioni sensibili, proprietarie o classificate;

4. Cyber Warfare: insieme delle attività e delle operazioni militari pianificate e condotte allo scopo di conseguire effetti in tale contesto.

La Figura 1.1, relativa ad un'analisi su 5.209 attacchi gravi di pubblico dominio che costituiscono il database del CLUSIT[2] [7], mostra la distribuzione degli eventi registrati negli ultimi cinque anni e mezzo suddivisi per semestre; dove nel primo semestre 2016 se ne sono verificati 521, contro i 495 del secondo semestre 2015 (+5%).

Invece dalla Figura 1.2 si evince che dal 2014 il cybercrime si è confer-

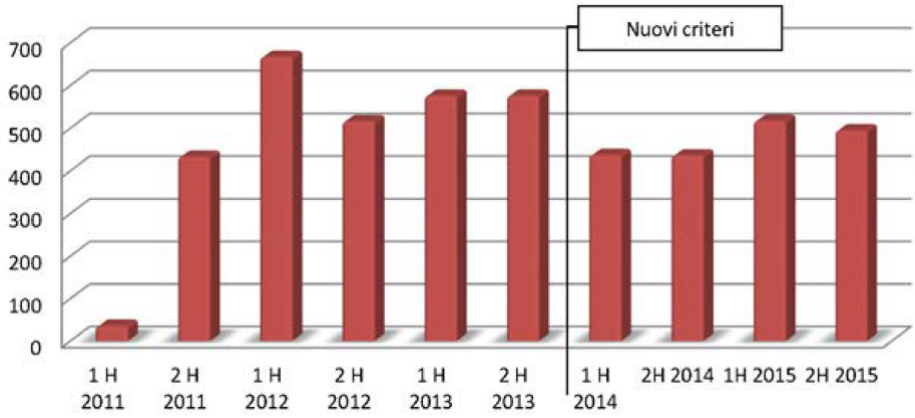


Figura 1.1: Numero di attacchi gravi di dominio pubblico (ordinate) per semestre (ascisse) [7].

mato come prima causa di attacchi gravi a livello globale, attestandosi al 60% dei casi analizzati. Nel primo semestre 2016 tale percentuale è salita a 71% mostrando un trend inequivocabile; inoltre dal 2015 si è assistito ad una

[2]Associazione Italiana per la Sicurezza Informatica, senza fini di lucro costituita a Milano il 4 luglio 2000.

larga diffusione di attività cybercriminali di piccola portata che in questo campione non sono rappresentate, come le quotidiane campagne di estorsione realizzate tramite phishing e ransomware che hanno colpito moltissime organizzazioni e cittadini italiani, di conseguenza si può supporre che questa crescita sia stata ancora maggiore. D'altra parte l'hacktivism diminuisce di 23 punti percentuali rispetto al suo picco del 2013, passando da oltre un terzo a meno di un quinto dei casi analizzati. Per quanto riguarda le attività di espionage, rispetto alla percentuale degli attacchi gravi registrati nel 2015 la quota di attacchi nel primo semestre 2016 è in crescita, mentre l'information warfare sembra essere in calo, probabilmente per mancanza di informazioni pubbliche in merito.

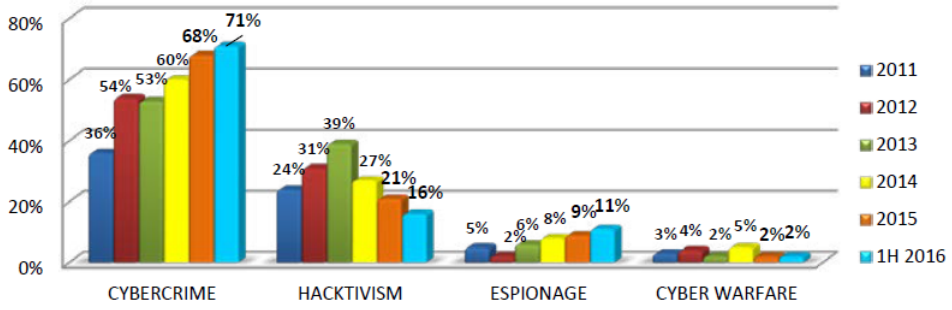


Figura 1.2: Distribuzione percentuale degli attaccanti: 2011 - 1H 2016 [7].

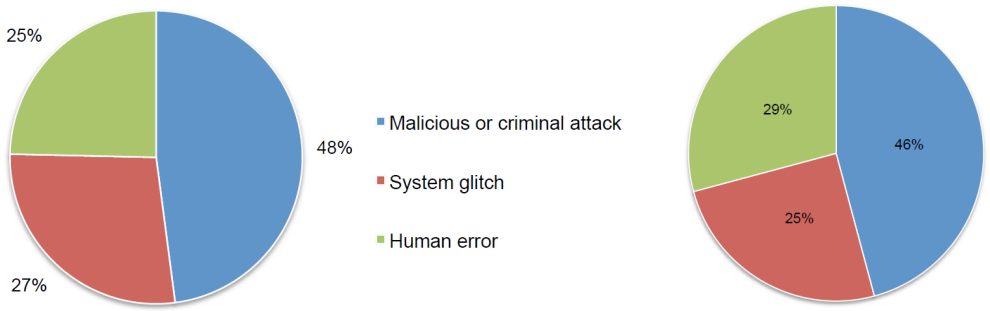
1.3 Violazione dei dati

ISO/IEC 27040 definisce un data breach (violazione dei dati) come una compromissione della sicurezza che porta alla distruzione accidentale o illecita, alla perdita, alterazione, rivelazione non autorizzata dei dati protetti: trasmessi, memorizzati o comunque elaborati.
I numeri riguardanti i casi di questo tipo di violazione sono in aumento, come riporta lo studio del Ponemon Institute [23], analisi condotta su 383 compagnie in 12 diversi paesi, in cui si mostra un aumento del 29% di costi totali rispetto alle stime fatte nel 2013. Tutte le organizzazioni partecipanti hanno

sofferto di data breach da circa 3.000 a poco più di 101.500 record compromessi, vedendo una crescita del 15% dell'aumento dei costi per perdita del singolo dato, sempre dal 2013. Ogni anno vengono analizzate compagnie diverse con caratteristiche comuni e dal 2005 sono state studiate un totale di 2.013 organizzazioni.
In questo report la violazione è definita come un evento in cui il proprio nome legato a una cartella clinica e/o un dato finanziario (es. carta di debito) di un individuo, sia in formato elettronico che cartaceo, è potenzialmente messo a rischio. Inoltre si sono identificate tre principali cause di una violazione dei dati: un attacco dannoso o penale, un glitch del sistema o un errore umano, i cui costi variano a seconda della causa e le garanzie in essere al momento della violazione dei dati. Per calcolare il costo medio di violazione dei dati sono stati raccolti sia i costi diretti che quelli indiretti sostenuti dall'organizzazione. Le spese dirette includono il coinvolgimento di esperti forensi, supporto esterno e fornitura di abbonamenti di monitoraggio del credito e sconti per futuri prodotti e servizi. I costi indiretti sono le indagini interne così come il valore estrapolato della perdita di clienti derivante dal fatturato o dalla diminuzione dei tassi di acquisizione dei clienti.
A livello globale, come rappresentato in Figura 1.3a, quasi la metà degli eventi sono di natura criminale mentre la restante divisa tra glitch del sistema ed errore umano. Vi sono percentuali simili (Figura 1.3b) anche nel caso specifico delle 24 organizzazioni italiane con un 46% derivante da intenzioni malevole e criminali.

La Figura 1.4 riporta i costi pro capite, ovvero i costi di un data breach diviso la dimensione dello stesso (numero di dati persi o rubati), classificati in base al settore di appartenenza. La media di tutti questi valori a livello globale (Figura 1.4a) è pari a 158$ e il settore sanitario risulta essere quello con le spese maggiori. Il settore sanitario, quello finanziario e quello dei servizi si trovano nelle primi posizioni anche nel contesto italiano, dove la media dei valori è pari a 112€, circa 122$.

I dati rubati o persi a causa di attacchi malevoli o criminali, come prevedi-



(a) Livello globale [23].

(b) In Italia [24].

Figura 1.3: Distribuzione del campione di riferimento in base alle cause della violazione dei dati

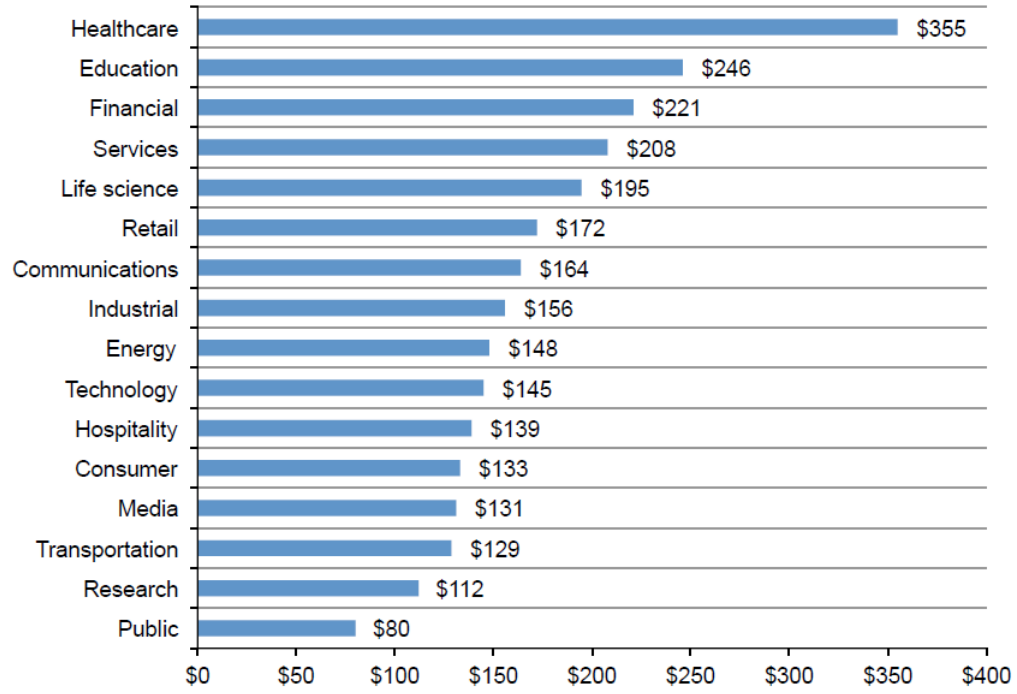
bile, comportano spese maggiori rispetto agli altri due casi; poi ci sono quelli per errore di sistema e in fine quelli per errore umano.
Nel corso degli anni la ricerca ha rivelato i seguenti sette macro-trend:

1. Fin dalla prima ricerca il costo della violazione dei dati non è variato in modo significativo. Così da suggerire che esiste un costo permanente a cui le organizzazioni devono essere preparate, per affrontarlo ed incorporarlo nelle loro strategie di protezione dei dati.

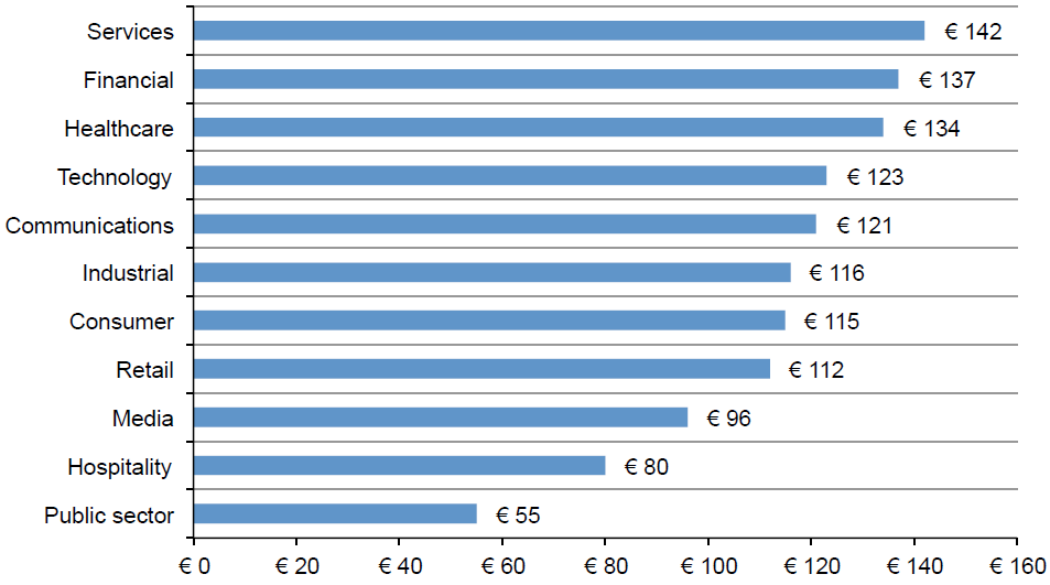
2. La più grande conseguenza finanziaria che ricade sulle organizzazioni è che un data breach porta a una perdita di business. A seguito di una violazione dei dati, le organizzazioni devono prendere misure adeguate per mantenere la fiducia dei clienti e per ridurre l'impatto finanziario a lungo termine.

3. La maggior parte delle violazioni dei dati continuano ad essere causate da attacchi criminali e dannosi. Individuare e contenere queste violazioni fa prendere molto tempo, di conseguenza esse hanno il più alto costo per record.

4. Nel corso degli anni i costi di rilevamento e di escalation sono aumentati, ciò suggerisce che siano stati fatti investimenti in tecnologie e competenze interne per ridurre il tempo di riconoscimento e contenimento.



(a) Livello globale [23].



(b) In Italia [24].

Figura 1.4: Costi pro capite nella classificazione per settore.

5. Settori regolamentati, come quello della sanità e quello dei servizi finanziari, hanno le violazioni dei dati più costose a causa delle multe e il tasso superiore alla media di perdita di affari e clienti.

6. I miglioramenti nei programmi di governance dei dati ridurranno il costo della violazione dei dati. I piani di risposta, la nomina di un Chief Information Security Officer (CISO), la formazione dei dipendenti, programmi di sensibilizzazione e una strategia di gestione della continuità operativa continuano a tradursi in risparmi sui costi.

7. Gli investimenti in alcuni controlli e attività come le soluzioni di sicurezza di cifratura e di endpoint sono importanti per la prevenzione della perdita di dati. Lo studio di quest'anno (2016) ha rivelato una riduzione del costo quando le aziende hanno partecipato alla condivisione di informazioni sulle minacce e utilizzato tecnologie dedicate alla prevenzione della perdita dei dati.

1.4 Il mercato nero dell'informazione

La risorsa principale dello spazio cibernetico sono indubbiamente i dati: le società che possiedono le informazioni degli utenti presentano valutazioni maggiorate. Dato che il valore commerciale dei dati è in crescita, negli ultimi tempi i criminali informatici sono artefici del cybercrime-as-a-service, fondando una vera e propria economia basata sulla vendita dei dati rubati. Si tratta di un sistema che offre la possibilità di accedere al cybercrime acquistando vari servizi, dai pacchetti di attacco cyber preconfezionati fino ad interi database di email e altri dettagli personali. Attorno a questa nuova tendenza si sviluppano le dinamiche tipiche del business moderno, veri e propri marketplace dove si sfruttano strategie di marketing e CRM.
Le principali tipologie di dati sono tre: dati personali, medici e finanziari.

1.4.1 Dati personali

La pubblicazione speciale 800-122 del NIST [19] riprende la definizione di Personally Identifiable Information dal documento GAO-08-536 [29], ovvero tutte le informazioni su un individuo mantenute da un'agenzia, tra cui tutte le informazioni che possono essere utilizzate per distinguere o tracciare l'identità di un individuo, come: nome, numero di previdenza sociale, data e luogo di nascita, nome da nubile della madre,dati biometrici e qualsiasi altra informazione alla quale è collegato o collegabile ad un individuo, come dati medici, educativi (scolastici), finanziari e informazioni sull'occupazione.
Nell'esempio seguente si riporta un'identità digitale rubata, in cui un potenziale compratore potrebbe assumere il controllo della della vita digitale di questa persona: socialmedia, posta elettronica e altro.
Il record in Figura 1.6, benché ricco di informazioni, richiede all'acquirente

Figura 1.5: Esempio di un'identità in vendita [15].

di vagliare una gran quantità di testo. Alcuni venditori offrono però un'interfaccia grafica accattivante per attirare i compratori, per esempio si permette ai compratori di scegliere gli individui in base ai loro account di posta elettronica, che è il primo passo per prendere il controllo di altre parti della vita delle vittime.

1.4.2 Dati medici

Strettamente legato al mercato delle identità rubate è quello delle informazioni mediche ottenute illecitamente. Un esempio di sottrazione illecita di informazioni di questo tipo è riportato in Figura 1.6. In questo caso il truffatore ha messo in vendita, sul noto online darknet market Alpha Bay, un file di testo di grandi dimensioni contenente nomi, indirizzi, codici fiscali e altri dati sensibili su decine di medici dell'ospedale Hilton Head Medical Center. Altri tipi di attacchi rivolti a strutture medico-sanitarie consistono

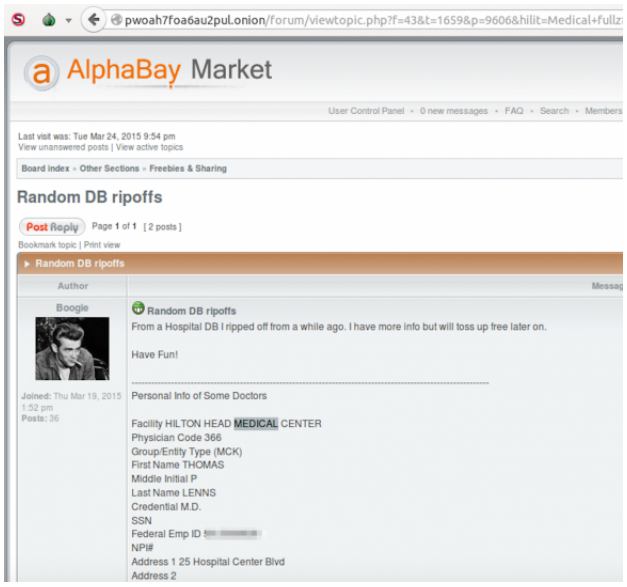


Figura 1.6: Un esempio di informazioni rubate da un servizio sanitario e messe in vendita [15].

in una richiesta di riscatto a seguito di una criptazione dei dati sensibili, grazie all'uso di specifici ransomware.

1.4.3 Dati finanziari

Il furto di dato finanziario più diffuso è quello degli estremi delle carte di pagamento, la cui sottrazione indebita colpisce particolarmente i commercianti. Il prezzo delle carte di pagamento, messe a disposizione in questi

mercati, varia in base alle informazioni disponibili insieme al numero della carta di pagamento:

- Il codice di verifica della carta CVV. CVV1 è il codice univoco a tre cifre contenuto nella banda magnetica della carta. CVV2 è il codice a tre cifre stampato sul retro della carta.

- Combinazione valida di numero di account primario (PAN), data di scadenza e codice CVV2 generata dal software. I generatori di numeri di carte di credito possono essere acquistati o reperiti gratuitamente online.

- Numero di carta scelto casualmente all'interno di un database violato, ed è casuale in merito a banca e tipo di carta.

- Tutti i dettagli della carta e del suo proprietario, come nome completo, indirizzo di fatturazione, numero della carta di pagamento, data di scadenza, codice PIN, codice fiscale, cognome da nubile della madre, data di nascita e CVV2. Possono includere anche il nome utente e password associati ad home banking. Con queste ultime credenziali il compratore può modificare l'indirizzo di spedizione o di fatturazione oppure aggiungerne altri.

1.5 Linee guida delle istituzioni italiane

A partire dal 2013 l'Italia si è dotata di un "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" [26] nel quale si fissano sei indirizzi strategici:

1. Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati;

2. Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese;

3. Incentivazione della cooperazione tra istituzioni ed imprese nazionali;
4. Promozione e diffusione della cultura della sicurezza cibernetica;
5. Rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali on-line;
6. Rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica.

Inoltre è stato articolato un "Piano nazionale per la protezione cibernetica e la sicurezza informatica" [27] che stabilisce il piano d'azione, da parte dei soggetti pubblici e privati, delle misure prioritarie per l'implementazione del Quadro Strategico. Gli undici indirizzi operativi che sono stati identificati sono:

1. Potenziamento della capacità di intelligence, della polizia e della difesa civile e militare;
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati;
3. Promozione e diffusione della cultura della sicurezza informatica, formazione e addestramento;
4. Cooperazione internazionale ed esercitazioni;
5. Operatività del Computer Emergency Response Team (CERT)[3] nazionale, del CERT-PA e dei CERT dicasteriali;
6. Interventi legislativi e compliance con obblighi internazionali;
7. Compliance a standard e protocolli di sicurezza;
8. Supporto allo sviluppo industriale e tecnologico;
9. Comunicazione strategica;

[3]Squadra per la risposta ad emergenze informatiche.

10. Risorse;

11. Implementazione di un sistema di Information Risk Management nazionale.

Inoltre nel febbraio 2016 è stato pubblicato un primo "Framework Nazionale di Cyber Security", frutto di un'inedita partnership tra pubblico e privato, il quale verrà ampiamente descritto nel Capitolo 4.

Capitolo 2

Gestione del rischio

In questo capitolo viene spiegato il processo, in ogni sua fase, mediante il quale si misura il rischio[1] e che tipo di strategie sono utilizzate per una corretta gestione, nello specifico contesto aziendale. In generale, il rischio può essere definito come la probabilità che accada un certo evento capace di causare un danno. Da tale probabilità si desume l'esistenza di una sorgente di pericolo in grado di trasformarsi in una conseguenza negativa.

2.1 I rischi dell'impresa

L'impresa[2] si trova quotidianamente ad affrontare un cospicuo numero di situazioni caratterizzate da incertezza e mancanza di prevedibilità. In tal senso si può definire il rischio come l'incertezza che eventi inaspettati possano manifestarsi producendo effetti negativi per l'organizzazione [10].
Queste situazioni possono mettere in dubbio il conseguimento, nel breve periodo, di un adeguato equilibrio economico, patrimoniale e finanziario e, nel

[1] Probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione [Art. 2, lettera s, D.Lgs. 81/08].

[2] Attività economica professionalmente organizzata al fine della produzione o dello scambio di beni o di servizi. Questa definizione la si deduce dalla definizione di "imprenditore" dagli articoli 2082 e 2083 del Codice civile.

medio e lungo termine, la creazione di valore e la sopravvivenza stessa dell'azienda. Queste situazioni vengono messe in relazione con il rischio d'impresa, ovvero con la possibilità che i risultati delle strategie differiscano da quelli specificati negli obiettivi aziendali e che conseguentemente non venga raggiunto lo scopo della massimizzazione del reddito attraverso la produzione efficiente ed efficace di beni e servizi.

Il risk management, in un'ottica aziendale, può essere definito come la funzione il cui compito è quello di identificare, valutare, gestire e sottoporre a controllo economico i rischi puri dell'azienda, cioè gli eventi che possono rappresentare una minaccia per il patrimonio fisico e umano dell'azienda e per la sua capacità di produrre reddito. Esso può essere considerato come un approccio scientifico al trattamento dei rischi puri, la cui nascita risale ai primi anni Cinquanta negli Stati Uniti.

All'inizio l'approccio era di tipo assicurativo e il compito del risk manager era quello di fronteggiare i rischi puri dell'impresa attraverso l'uso di coperture assicurative, occupandosi dell'ottimizzazione dei rapporti con le compagnie per ridurre le quote di premio pagate. Successivamente, in un ambito sia accademico che professionale, l'attenzione viene rivolta all'analisi del rischio e alle tecniche di "controllo fisico", il cui obiettivo diventa quello di prevenire gli eventi dannosi e limitare le perdite in caso di occorrenza di un sinistro, cercando di ridurre al minimo livello possibile il costo del rischio. Negli anni Ottanta emerge, quindi, una visione del risk management basata sulla capacità dello stesso di contribuire alla massimizzazione del valore economico e di mercato dell'impresa. In conclusione, l'attività di risk management contribuisce alla creazione di valore cercando di garantire una minore variabilità dei flussi attesi, trasformando costi incerti in altri prevedibili e un aumento di essi nel medio-lungo termine.

2.2 Fasi del processo di risk management

Al risk management compete la gestione, strategica e operativa, dei rischi puri e l'attività di supporto alle altre funzioni aziendali in come la gestione dei rischi imprenditoriali, con lo scopo essenziale di proteggere l'organizzazione dagli eventi sfavorevoli e dalle loro conseguenze sul valore aziendale. Detto ciò, ne deriva che gli effetti di un evento dannoso possono innescare reazioni a catena che si propagano all'interno e all'esterno dell'organizzazione. Gli effetti possono essere classificati in:

- danni diretti, che si generano immediatamente in seguito a un sinistro che colpisce l'attivo patrimoniale;
- danni da responsabilità civile, che influiscono sulla consistenza patrimoniale attraverso l'insorgenza di passività per risarcimenti dovuti a terzi a causa di danni a cose o persone provocati dall'attività dell'impresa;
- danni indiretti, che derivano dall'introduzione parziale o totale dell'attività di produzione del reddito, consistenti nel mancato profitto o nelle spese supplementari per consentire la riduzione della perdita di reddito;
- danni consequenziali che rimangono anche dopo la ricostruzione della situazione preesistente al sinistro, legati al deterioramento dei rapporti con i clienti e i fornitori, alla perdita di immagine, di credibilità sociale, di quote di mercato o di possibilità di espansione, di informazioni e alla difficoltà di accesso al credito.

2.2.1 Identificazione

La prima fase è quella dell'identificazione dei rischi, nella quale vengono raccolte ed elaborate tutte le informazioni necessarie a descrivere il profilo di rischio aziendale. Occorre, senza fare stime eccessive o insufficienti, mettere in evidenza:

- le unità di rischio, cioè le risorse aziendali che potenzialmente possono essere oggetto di eventi dannosi;
- i pericoli, cioè le cause di eventi sfavorevoli che possono colpire le risorse;
- le casualità, cioè le condizioni che favoriscono il verificarsi dell'evento negativo;
- le tipologie di effetti che ogni evento dannoso può provocare.

Per essere eseguita è necessaria da parte del risk manager un'approfondita conoscenza della realtà aziendale in modo da poter individuare le interrelazioni tra le parti, punti di forza e di debolezza, le reazioni a catena che potrebbero verificarsi.

2.2.2 Valutazione

La valutazione dei rischi, per una data unità di rischio e per un definito intervallo di tempo, consiste nell'identificazione della frequenza, della gravità e delle perdite potenziali relative ai rischi esaminati e nell'attuazione di analisi di convenienza tra diverse alternative di gestione volte a minimizzare il costo. Si tratta di determinare una funzione matematica f del tipo: $R = f(M, P)$, dove R è la magnitudo del rischio, M è la magnitudo delle conseguenze e P è la probabilità o frequenza del verificarsi delle conseguenze [22]. In questa fase vengono confrontate le diverse tecniche di gestione, considerando scenari alternativi, in modo da giungere a una soluzione ottimale in termini di efficienza e di efficacia.

2.2.3 Gestione

La gestione dei rischi consiste nella selezione, in base ai costi e ai risultati attesi, degli strumenti da applicare per rendere il rischio economicamente accettabile e nella realizzazione concreta di quelli selezionati. Le tecniche di gestione possono essere distinte in tecniche di controllo, che agiscono

direttamente sulle determinanti del rischio e le tecniche di finanziamento, che nell'ipotesi del verificarsi dell'evento dannoso agiscono sulle conseguenze economico-finanziarie di quest'ultimo. Le tecniche di controllo comprendono la prevenzione e la protezione attraverso l'uso di misure di sicurezza fisiche, di procedure e di formazione. Le tecniche di finanziamento trattano dell'individuazione dei mezzi finanziari necessari a fronteggiare le spese o gli investimenti per il ripristino della capacità produttiva perduta in seguito al sinistro.
In conclusione, attraverso l'identificazione, la valutazione e la gestione dei rischi, il risk manager ha il compito di rendere il profilo di rischiosità dell'impresa coerente con i suoi obiettivi, anche mediante la collaborazione, la comunicazione e l'integrazione con altre funzioni aziendali.

2.3 Tecniche di gestione dei rischi puri

Una volta identificati e valutati i rischi e le relative cause ed effetti, è necessario avanzare con una serie di interventi tecnici e organizzativi di prevenzione e protezione volti a limitare frequenza e intensità dei possibili sinistri. Tali interventi devono essere confrontati e valutati alla luce dei costi e dei benefici che comportano. I costi si distinguono in diretti, relativi alla dotazione degli strumenti di gestione del rischio e della loro manutenzione e indiretti, dovuti a tutti quei fattori che vanno a modificare l'ambiente attuale.
La tecnica di trasferimento del rischio maggiormente utilizzata dalle imprese rimane l'assicurazione, combinata nell'ottica di accrescimento del valore dell'impresa, con adeguati livelli di ritenzione.

2.3.1 Ritenzione

La ritenzione è una tecnica di finanziamento del rischio attraverso la quale l'impresa si fa carico, in tutto o in parte, delle conseguenze finanziarie di un sinistro, predisponendo interventi e programmi volti alla minimizzazione degli effetti sulle risorse aziendali. Le tecniche di ritenzione vengono intraprese in

relazione a rischi di bassa gravità ed elevata frequenza, il cui costo risulta sufficientemente prevedibile o comunque non sia economicamente conveniente trasferirlo. Le tecniche di ritenzione attiva sono:

- assorbimento nei costi di esercizio: se si tratta di perdite con un alto grado di attendibilità di previsione è possibile considerare queste ultime in sede di programmazione finanziaria d'esercizio;
- autoassicurazione: piano di accumulazione volto alla costituzione di un fondo gestito con criterio assicurativo;
- fondi di riserva: accantonamento di tipo generico utilizzabile al verificarsi dell'evento. Non è legato alla distribuzione delle perdite del rischio e varia a seconda della attività economica che sta passando l'impresa.
- indebitamento ex-post: non vengono intaccate le risorse finanziarie dell'azienda ma sorgono costi dovuti a interessi passivi.

Queste tecniche permettono un risparmio di costi rispetto al premio assicurativo dato che quest'ultimo oltre alla perdita attesa risente delle delle spese amministrative e del profitto dell'assicuratore. L'aspetto negativo della ritenzione è il mantenimento dell'incertezza dell'eventuale verificarsi e dell'effettivo ammontare della perdita.

2.3.2 Assicurazione

L'assicurazione è una tecnica di finanziamento del rischio attraverso cui l'impresa trasferisce a un altro soggetto giuridico (compagnia assicurativa) le conseguenze finanziarie dovute al verificarsi di un evento, caratterizzato da irregolarità nel momento di manifestazione e nell'entità della perdita, dietro il pagamento di una certa somma (premio). Il trasferimento del rischio avviene nei limiti e nelle condizioni stabilite nel contratto (polizza), il quale è anche uno strumento di cui l'impresa può usufruire per servizi aggiuntivi come analisi dei rischi, consulenza dei sistemi di prevenzione, assistenza tecnica e

giuridica. D'altra parte, le assicurazioni devono tener conto di un insieme di condizioni teoriche necessarie e sufficienti per l'assicurabilità dei rischi, riassumibili nelle seguenti considerazioni.

1. Esistenza di un grande numero di esposizioni indipendenti, controllate da persone interessate ad assicurarle. Questo requisito è essenziale affinché possa crearsi un portafoglio di rischi sufficientemente vasto, innescando il mercato assicurativo di stabilizzazione della perdita media. Infatti, se il rischio non colpisce un numero elevato di soggetti, l'assicuratore non potrà mai concludere contratti in quantità sufficiente per mantenere la variabilità della perdita media del portafoglio ad un livello economicamente accettabile.

2. Poter definire la perdita nel tempo, nel luogo, nella causa e nell'ammontare. In mancanza di tale requisito, non si potrebbe stabilire se la perdita possegga o no le caratteristiche che garantiscono l'indennizzo alla luce delle condizioni di polizza. Inoltre lo stesso indennizzo non potrebbe essere calcolato.

3. Valutabilità, con un sufficiente grado di credibilità della perdita attesa. Requisito che mette in condizione di fissare il premio, il quale richiede che siano soddisfatte le prime due condizioni e in più che il rischio sia relativamente stabile, ossia che le manifestazioni dannose future riflettano abbastanza fedelmente, per gravità e per frequenza, quelle passate. Per tale motivo gli assicuratori tendono ad essere molto prudenti verso la copertura dei nuovi rischi, derivanti da tecnologie di recente introduzione, per i quali non è stata ancora maturata sufficiente esperienza.

4. Casualità della perdita rispetto all'assicurato. Ovviamente non può essere concessa copertura per i danni causati intenzionalmente da chi li subisce, tuttavia sono rari i casi in cui l'assicurato non ha nessuna influenza, anche involontaria, sul verificarsi dell'evento. Allo stesso mo-

do, non dovrebbero essere assicurati eventi che si verificano certamente o che possono facilmente essere prevenuti dall'assicurato stesso.

Danni come quelli consequenziali, pur provocando effetti rilevanti, non possono essere assicurati, richiedendo da parte del manager interventi alternativi volti a ridurre l'impatto sulla solidità dell'impresa. Questo processo richiede la combinazione di informazioni interne all'impresa e di competenze tecniche specifiche, attraverso il quale dovrebbe instaurarsi un'interazione tra risk manager, intermediari e assicuratori.
Per i rischi puri caratterizzati da un'alta prevedibilità l'assicurazione piena risulta economicamente svantaggiosa, poiché il premio eccede il valore della perdita attesa per una quota pari ai caricamenti per spese di gestione e profitto dell'assicuratore. A tale proposito, vi sono strumenti contrattuali che lasciano a carico dell'impresa assicurata una quota dell'eventuale danno:

- la franchigia che consiste nella quota di danno esclusa dal risarcimento dell'assicuratore; può essere assoluta se la l'assicurazione risarcisce la differenza tra l'ammontare del danno e l'importo della stessa, oppure relativa se l'impresa si fa carico dei danni di entità inferiore al suo importo.

- lo scoperto, cioè la percentuale prestabilita del danno posta a carico dell'assicurato, calcolato sull'importo del sinistro indennizzabile;

- il massimale, che rappresenta l'ammontare massimo di indennizzo che l'assicuratore è chiamato a pagare.

In aggiunta vi è l'uso della regola proporzionale, per evitare casi di assicurazione parziale in base alla quale il risarcimento viene stabilito in relazione tra somma assicurata e valore effettivo dei beni.
La polizza può essere distinta concettualmente in quattro parti, la cui suddivisione non necessariamente si può ritrovare nel documento scritto.

1. Le dichiarazioni, nonché la parte descrittiva della polizza nella quale si identificano la persona beneficiaria del contratto, il bene, l'attività o

la persona assicurata, il tipo di copertura, il premio, i limiti di indennizzo e la durata del contratto. Nell'ambito del ramo danni, l'oggetto dell'assicurazione può essere di tre tipi: danni a cose, danni a persone e responsabilità da danno a terzi.

2. L'accordo, ovvero l'impegno formale da parte dell'assicuratore a risarcire la controparte per le conseguenze sofferte a causa degli eventi previsti in contratto. L'accordo precisa quali minacce e quali danni vengono coperti. A questo riguardo si distingue fra polizze all risks e polizze a rischio definito, definendo ciò che non è coperto oppure solo i rischi che vengono assunti.

3. Le esclusioni, si tratta di limitazioni alla copertura stabilite in relazione a certi eventi, persone, luoghi, beni, danni, periodi temporali, ecc. I motivi che spingono l'assicuratore a sottrarsi a certe fonti di responsabilità servono:

   - ad evitare l'assunzione di rischi non assicurabili;
   - togliere dalle coperture evenienze che sono tradizionalmente oggetto di altre polizze;
   - escludere le evenienze intenzionali o che potrebbero essere facilmente evitate dall'assicurato;
   - costruire polizze a copertura limitata per incontrare determinate esigenze di particolari segmenti di potenziale clientela;
   - eliminare quelle coperture che l'assicuratore ritiene non essere preparato a trattare.

Il premio assicurativo

Come discusso in precedenza, l'assicurazione può essere considerata come il trasferimento di un rischio dal contraente all'assicuratore. Il rischio è di natura stocastica, così da poter essere considerato come una variabile casuale. Per costruzione si assume anche che sia una variabile casuale non negativa

in quanto i rischi che assumono valori negativi non sono realistici nell'assicurazione danni. L'industria assicurativa esiste perché la gente è disponibile a pagare un prezzo per essere assicurata. Il corrispettivo pagato dall'assicurato, a fronte dell'impegno aleatorio preso dall'assicuratore con la stipula del contratto di assicurazione, è definito premio. Nella tecnica attuariale esistono diverse configurazioni di premio [8]. Infatti si parla di:

- Premio equo, che corrisponde al valore atteso del totale dei risarcimenti aleatori a carico dell'impresa di assicurazione durante il periodo assicurato.

- Premio netto, che, al pari del premio equo, corrisponde all'importo necessario all'assicuratore per fronteggiare i risarcimenti, con la sostanziale differenza che il premio netto ricomprende al suo interno anche il cosiddetto caricamento di sicurezza, non presente nel premio equo. Il caricamento è il guadagno atteso dal contratto assicurativo per l'impresa nel periodo di copertura. Tale conformazione di premio ha il ruolo di limitare eventuali perdite qualora la gestione del portafoglio di contratti sia negativa a causa di errori di stima o di un inaspettato aumento della sinistrosità.

- Premio di tariffa, detto anche commerciale, che è pari alla somma tra premio puro e caricamenti per spese, destinati a coprire i costi di gestione ed amministrazione. Il premio di tariffa è pertanto il premio che l'assicuratore chiede a fronte di una copertura; tuttavia non corrisponde al prezzo effettivamente pagato dall'assicurato. Al fine di individuare il reale premio pagato dall'assicurato, al premio di tariffa è necessario aggiungere le tasse previste dalle norme vigenti.

Principali metodi di calcolo del premio netto . Il premio netto (o puro) è la somma fra premio equo e caricamento di sicurezza, nonché il premio che permette all'assicuratore di raggiungere l'equilibrio tecnico della propria gestione, garantendo la solvibilità dell'impresa e la capacità di far fronte agli

impegni presi nei confronti degli assicurati. Il premio netto può pertanto essere definito come $\Pi = H(X)$, dove H è un funzionale che associa un numero reale Π a ciascuna possibile distribuzione di probabilità del risarcimento globale X. A seguire i più importanti principi di calcolo del premio [32].

- **Principio del valore atteso** $H(X) = (1+\theta)\mathbb{E}[X]$, $\theta > 0$. Si tratta di un principio di calcolo spesso utilizzato nella pratica assicurativa proprio per la sua semplicità. Il vantaggio dell'applicazione di tale principio risiede nel fatto che i dati utilizzati sono i medesimi impiegati nel calcolo del premio equo; lo svantaggio è connesso invece al calcolo del caricamento di sicurezza, che prescinde dalle misure di rischio.

- **Principio della varianza** $H(X) = \mathbb{E}[X] + \alpha VarX$, $\alpha > 0$. Come il precedente, include il risk load che è proporzionale alla varianza del rischio. La capacità del caricamento di sicurezza di rappresentare il guadagno atteso per l'impresa dipende però dalla capacità della varianza di quantificare correttamente il rischio derivante da X. Per poter valutare ciò, è necessario analizzare la distribuzione di probabilità di X: se è simmetrica e le code sono corte, allora la varianza è da considerarsi una buona misura di rischio. A differenza del principio del valore atteso il principio della varianza richiede pertanto l'analisi di ulteriori informazioni e dati rispetto a quelli utilizzati per il calcolo del premio equo.

- **Principio dello scarto quadratico medio** $H(X) = \mathbb{E}[X] + \beta\sqrt{VarX}$, $\beta > 0$. In questo caso il risk load è proporzionale alla deviazione standard del rischio. Il vantaggio rispetto al principio della varianza consiste nel fatto che β non è legato a nessuna unità di misura. I due principi sono in ogni caso molto simili; in particolare può essere determinato lo stesso ammontare di premio puro applicando i due principi, poiché $\beta = \alpha Var(X)$.

- **Principio dell'utilità attesa** Secondo questo principio, il premio puro è calcolato come soluzione dell'equazione:

$$\mathbb{E}[u(H(X) - X)] = 0 \tag{2.1}$$

Il premio puro è il premio di indifferenza, per una data funzione di utilità u. L'utilità attesa del guadagno aleatorio, pari a $H(X) - X$, non deve essere inferiore all'utilità attribuita alla situazione antecedente la stipula del contratto. In altre parole, in base a questo principio, il premio puro è quel premio che rende indifferente, in termini di utilità attesa, la situazione precedente all'assunzione del contratto e quella seguente, cioè è il minimo premio che rende il contratto non svantaggioso per l'assicuratore. Consideriamo a titolo esemplificativo l'applicazione di questo principio in caso di un'utilità quadratica $u(x) = x - \frac{1}{2B}x^2$ per $x \leq B$ e B parametro legato alla ricchezza disponibile; sostituendo nella 2.1 la funzione di utilità e sviluppando l'equazione si ottiene un'approssimazione del premio puro uguale a $H(X) \approx \mathbb{E}(X) + \frac{1}{2B}Var(X)$. In questo caso il caricamento di sicurezza cresce al crescere della varianza del risarcimento aleatorio e della quantità $\frac{1}{B}$, che misura l'avversione al rischio.

- **Principio del percentile** Il caso in cui $X > H(X)$ indica una situazione di perdita economica per l'assicuratore. In relazione al principio del percentile, il premio puro dev'essere calcolato come: $Pr[X > H(X)] = \epsilon$ dove ϵ $(0 < \epsilon < 1)$ è la probabilità di conseguire una perdita sul singolo contratto e indica un percentile convenientemente piccolo. Tanto più alta sarà la probabilità di subire una perdita, tanto maggiore sarà il premio puro. Per poter applicare il principio del percentile è necessario assegnare una distribuzione di probabilità ad X. Indicata con F la funzione di ripartizione dei risarcimenti avremo $1 - F(H(X)) = \epsilon$. L'unicità e l'esistenza della soluzione di quest'ultima formula sono assicurate solo nel caso in cui la funzione F sia continua e monotona crescente in senso stretto.

Tali criteri soddisfano alcune proprietà, riportate di seguito, espresse con notazione formale dove χ denota l'insieme di variabili non-negative sullo spazio di probabilità $(\Omega, F, \mathbb{P})$. X, Y, Z, etc. denotano i membri tipici di χ e la funzione H che va da χ all'insieme di numeri reali non-negativi.

- Indipendenza, $H(X)$ dipende soltanto da una funzione cumulativa $S_x(t) = P\{\omega \in \Omega : X(\omega) > t\}$;
- Risk loading (caricamento di sicurezza), $\forall X \in \chi, H(X) \geq \mathbb{E}[X]$;
- Subadditiva, $\forall X, Y \in \chi, H(X + Y) \leq H(X) + H(Y)$;
- Monotona, se $X(\omega) \leq Y(\omega)\ \forall \omega \in \Omega$, allora $H(X) \leq H(Y)$;
- Maximal loss, il premio è limitato da una una possibile perdita massima $H(X) \leq$ ess sup(X);

Premio tariffa Il premio di tariffa P_T, o commerciale, è il premio richiesto al contraente, che tiene conto delle spese che gravano sull'impresa. Il premio di tariffa si calcola aggiungendo al premio puro i cosiddetti caricamenti per spese. Le spese che rientrano a far parte del caricamento sono di acquisizione dei contratti, di incasso dei premi e di gestione amministrativa.
Gli oneri provvigionali di acquisizione e le spese di incasso sono commisurate in termini di una percentuale α del premio tariffa P_T, mentre per le spese di gestione, il recupero dei costi avviene mediante l'applicazione di una percentuale β, sempre sul premio tariffa. Indicando con P il premio puro, il premio tariffa è uguale a $P_T = P + (\alpha + \beta)P_T = P(1 + \gamma)$ con $\gamma P = \frac{\alpha+\beta}{1-(\alpha+\beta)}P$. I coefficienti di caricamento α e β sono diversi a seconda del ramo di rischio e dipendono dal volume del portafoglio e dalle condizioni di mercato.

Processo di tariffazione La tariffazione è il processo che conduce l'assicuratore alla determinazione del premio da richiedere agli assicurati. Come

già detto, il premio è definito sulla base della valutazione probabilistica della prestazione aleatoria dell'assicuratore o del risarcimento totale dovuto in conseguenza dei sinistri, che hanno colpito i rischi assicurati nel periodo di copertura della polizza.

I portafogli assicurativi sono formati da un insieme di rischi fra loro eterogenei, e tale eterogeneità è dovuta a fattori endogeni, insiti nella particolare natura del rischio, ma anche a fattori esogeni tipicamente ambientali o socio-economici. Mediante le tecniche di tariffazione l'assicuratore suddivide la collettività di rischi in sottogruppi o classi, che presentano caratteristiche analoghe, in modo da poter attribuire ai rischi appartenenti alla stessa classe la medesima base tecnica. Attraverso tale processo i premi vengono pertanto differenziati per gli assicurati, a seconda del diverso profilo di rischio.

Questa differenziazione dei premi avviene in due fasi. Nella prima fase, detta personalizzazione o tariffazione a priori, si differenziano i premi in funzione di caratteristiche dei rischi, osservabili al momento della conclusione del contratto, prima di disporre di qualsiasi tipo di informazione sulla sinistrosità dell'assicurato derivante dall'esperienza. L'assicuratore individua dei sottogruppi di rischi analoghi, le classi tariffarie o classi di rischio, sulla base di variabili tariffarie, per poi valutare i premi da attribuire ad ogni classe. Per cercare di formulare previsioni sulla sinistrosità dell'assicurato può essere più efficace l'osservazione della sua "storia assicurativa", tanto che per alcune coperture è previsto un aggiustamento del premio a posteriori. Questa è pertanto la seconda fase del processo di tariffazione, ovvero la personalizzazione o tariffazione a posteriori.

Capitolo 3

Cyber risk

Avendo discusso in termini generici della gestione del rischio nel capitolo precedete, ora lo si cala nello specifico contesto dello spazio cibernetico. Dopo un accenno al mercato assicurativo si presentano le due principali metodologie di elaborazione e valutazione del rischio.

3.1 Contestualizzazione del rischio nello spazio cibernetico

Il tema del cyber risk rappresenta un punto critico nel processo di analisi e riduzione dei rischi cui un'azienda può incorrere nella conduzione della propria attività. Data la larga diffusione di tecnologie e modelli di business sempre più basati sulla rete, dove vengono possedute e scambiate informazioni sensibili, l'adozione di efficienti ed efficaci strumenti di gestione del cyber-rischio (cyber risk management) assume rilevanza cruciale, in quanto da essa possono dipendere le sorti stesse dell'impresa. Serve analizzare le possibili tipologie di danni e costi per capire se si ha bisogno di una polizza cyber e quali caratteristiche questa deve avere per tutelare il proprio business. Nello spazio cyber, si possono distinguere tre tipologie di danni:

- Danni materiali diretti: Riguardano i danni subiti da beni materiali (server, rete, PC o qualsiasi altro dispositivo elettronico) e direttamente

causati dall'evento di natura tradizionale (incendio, terremoto, furto, atto maldestro o doloso, ecc.).

- Danni materiali indiretti: Si tratta sempre di danni materiali ma a conseguenza di danni diretti, per esempio uno sbalzo di tensione che danneggia una scheda che a sua volta lede la macchina di produzione da essa controllata.

- Danni immateriali diretti e indiretti: Si tratta della compromissione dell'integrità di un software e/o l'insieme logico di informazioni. Esempi di questa categoria possono essere l'incendio che brucia il server con il suo contenuto informativo, l'involontaria (o volontaria) cancellazione di un database contenenti informazioni sensibili piuttosto che l'azione di un virus o di un malware.

La copertura assicurativa di tali rischi è l'ultima fase di un processo ben definito che parte con l'analisi della realtà specifica dell'azienda, dal tipo di business che conduce al tipo di attività implementata fino alle caratteristiche dell'infrastruttura IT. Gli aspetti critici da tenere in considerazione possono essere, per esempio: il mercato di riferimento, la peculiarità dell'infrastruttura IT, il tipo di informazione trattato, le policy di cybersecurity e le misure di prevenzione e protezione poste in atto, e così via.
A fronte di tutte queste variabili si deve tenere in considerazione che l'assicurazione deve operare come strumento di tutela del bilancio aziendale, intervenendo a copertura dei rischi anche in funzione del risk appetite e risk tolerance. Inoltre si devono considerare i benefici derivanti da ulteriori azioni di prevenzione e protezione, per cui il costo da sostenere per aumentare i livelli di sicurezza può diventare insostenibile se comparato ai benefici connessi. La società deve pertanto stabilire oltre quale soglia sia maggiormente conveniente un trasferimento al mercato assicurativo del rischio residuo e, nel contempo, valutare il trade-off ottimale tra il prezzo della copertura assicurativa e il livello di esposizione residua al rischio.

3.2 Il mercato assicurativo

Il mercato assicurativo delle polizze cyber risk oggi è in rapida evoluzione e offre la possibilità di creare tutele ad hoc per il cliente, adeguandosi al rischio cyber cui è esposta l'azienda, a seguito di un importante processo di analisi e valutazione. Questo tipo di mercato è maggiormente sviluppato nei paesi dell'America settentrionale e anglosassoni, dove questo tipo di problematiche vengono studiate da circa una decina d'anni. Il mercato assicurativo italiano, seppur in evoluzione, si trova ancora in una fase embrionale perché, come sempre in questo tipo di mercato, la risposta a un rischio si attua nel momento in cui tale rischio diviene conosciuto e valutabile.
Il mercato degli assicuratori presenta due approcci da cui derivano due tipologie di indennizzo differenti:

- First Party Damages: comprende tutti i danni sofferti dall'azienda colpita da un particolare evento cyber;
- Third Party Damages: ovvero la responsabilità dell'azienda assicurata per la violazione dei dati di terzi di cui è in possesso.

Nella prima tipologia vengono inclusi l'indennizzo per spese come la messa in sicurezza informatica, il ripristino dei dati persi, i costi legali per far fronte ad un indagine dell'autorità preposta al controllo, la perdita di profitto legata al blocco dell'attività della società assicurata e, inoltre, la frode informatica subita dall'azienda e conseguenti danni a terzi.
Il secondo approccio è speculare e indennizza la richiesta danni avanzata da terzi per violazione dei dati in possesso della società, con l'aggiunta delle spese addizionali per il recupero dei dati, dei danni all'immagine della società assicurata e delle spese legali per fronteggiare una richiesta di risarcimento o di indagine nel caso in cui vi sia una perdita di dati terzi verso l'esterno.
La differenza tra i due approcci risarcitori trova riscontro in due momenti diversi di attivazione della copertura. Nel caso della metodologia first party, l'elemento che fa scattare la copertura è la rilevazione del danno all'azienda assicurata, sia esso danno materiale, immateriale o patrimoniale. Nel secondo

caso invece ciò che fa scattare la copertura è la richiesta di risarcimento danni avanzata da terzi in conseguenza della violazione di dati di terzi detenuti dall'assicurato.

3.3 Valutazione ed elaborazione del cyber risk

I metodi per l'analisi del rischio applicati sugli asset esposti nell'organizzazione sono di due tipi [25]:

- Quantitativo, che usa due elementi base, ovvero la probabilità del verificarsi di un evento e la perdita nella quale si può incorrere.
- Qualitativo, in cui si classifica la magnitudo di un possibile impatto di una minaccia come alto, medio o basso e non attraverso valori numerici. Questo metodo valuta tutti i potenziali impatti, utilizzando diversi elementi come minacce, vulnerabilità e controlli che sono tra di loro interconnessi.

3.3.1 Metodi quantitativi

Il valore del rischio può essere presentato con l'uso di un qualsiasi tipo di scala o direttamente come predizione delle perdite finanziarie connesse a un tipo di rischio, in un determinato periodo.
Solo occasionalmente succede che il team che conduce il processo di valutazione del rischio abbia a disposizione i dati necessari per la realizzazione di accurati task, senza la presenza di errori. Inoltre, per qualche risorsa nell'organizzazione, l'ammontare delle perdite è difficile da stabilire. Una semplice valutazione del rischio è presentata come segue:

$$R = P \times W \wedge P = F \times V$$

dove:

- R valore del rischio;

- P probabilità o il numero di occorrenze di un incidente che causa la perdita di valore in un definito periodo;
- W valore della perdita, predizione della perdita media a seguito di un singolo incidente;
- F frequenza delle minacce;
- V vulnerabilità di un'informazione di sistema per una data minaccia.

Risulta che la valutazione del rischio è spesso rappresentata come valore della potenziale perdita, la quale si basa sulla definizione di tre concetti fondamentali:

1. Valore della risorsa, per il corretto funzionamento dell'impresa;
2. Frequenza di una minaccia, definita come il numero di occorrenze;
3. Vulnerabilità del sistema IT per una minaccia, ovvero la misurazione della probabilità di accadimento di una perdita a seguito del verificarsi dell'evento.

Nel 1979 la National Bureau of Standards pubblica il suo Federal Information Processing Standars (FIPS) 65, Guideline for Automatic Data Processing Risk Analysis [16]. Questo documento ha fissato lo standard di valutazione del rischio per i centri di elaborazione dati di grandi dimensioni ed ha anche proposto una nuova metrica di misurazione dei rischi computer-related: Annual Loss Expectancy (ALE).

$$ALE = \sum_{i=1}^{n} I(O_i)F_i \tag{3.1}$$

dove:

- $\{O_1, O_2, \ldots, O_n\}$ l'insieme degli effetti negativi;
- $I(O_i)$ la perdita (in dollari) dato un evento i;

- F_i la frequenza di un evento i.

Molti modelli di valutazione del rischio IT sono basati sul metodo appena descritto, adatti alle esigenze concrete ed esistenti in una determinata organizzazione. Una derivazione è il modello ISRAM [14], il quale usa i risultati di due questionari separati e indipendenti per analizzare i security risk in un'organizzazione. Il metodo propone quindi di pesare le risposte delle persone intervistate in cui la probabilità e l'impatto sono date dalla media di questi valori. Il flow diagram di ISRAM è composto da sette fasi:

1. Consapevolezza dei problemi di sicurezza dell'informazione;
2. Lista di tutti i fattori che determinano la probabilità dell'occorrenza di violazione di sicurezza e assegnazione di un peso per ogni fattore;
3. Convertire i fattori in questionari, designare le risposte per ogni domanda e assegnare un valore numerico alla risposta scelta;
4. Preparare la risk table per le probabilità dell'occorrenza di violazione di sicurezza;
5. Applicare la formula 3.2 e ottenere un singolo valore di rischio;
6. Valutazione dei risultati.

Quindi, l'indice di rischio è dato dalla formula:

$$Risk = \left(\frac{\sum_{m}[T_1(\sum_{i} w_i p_i)]}{m} \right) \left(\frac{\sum_{n}[T_2(\sum_{j} w_j p_j)]}{n} \right) \tag{3.2}$$

dove:

- i il numero di domande per il survey sulla probabilità delle occorrenze, determinato al passo-2;
- j il numero di domande per il survey sulle conseguenze delle occorrenze, determinato al passo-2;

- m il numero di partecipanti che hanno risposto al survey sulla probabilità delle occorrenze, che viene definito al passo-5;

- n il numero di partecipanti che hanno risposto al survey sulle conseguenze dell'occorrenza; che viene definito al passo-5;

- p_i, p_j il valore numerico della risposta scelta per la domanda i e rispettivamente j, determinato al passo-3;

- T_1 la tabella di rischio per il survey sulla probabilità dell'occorrenza, costruita al passo-4;

- T_2 la tabella di rischio per il survey sulle conseguenze dell'occorrenza, costruita al passo-4;

- *Risk* singolo valore numerico che rappresenta il rischio, ottenuto al passo-6.

Un altro esempio di metodo quantitativo è quello del International Security Technology, Inc. (ICT) che ha sviluppato CORA [3]. Si basa sull'utilizzo di dati raccolti che riguardano le minacce di attività e beni per calcolarne le conseguenze. Si tratta di un metodo in cui i parametri sono specificati nella quantitative risks e dove la perdita è espressa in termini di quantitative finance. CORA utilizza un processo composto da due fasi per supportare la gestione del rischio, calcolando SOL e ALE per ogni minaccia identificata. Le perdite totali per l'organizzazione sono stimate per ogni minaccia, di conseguenza questo valore viene moltiplicato per la frequenza delle minacce. Pertanto impiega i seguenti indici:

- ALE = conseguenza x frequenza, il cui risultato uguale a $\sum n$ dove n è il numero di SOL relativo;
- SOL = perdita potenziale (caso peggiore in valuta monetaria) x vulnerabilità.

3.3.2 Metodi qualitativi

L'approccio qualitativo non fa uso di valutazioni monetarie degli asset e non necessita di quantificare la frequenza con cui si verificano degli attacchi al sistema, vale a dire che non si verifica il problema di dover utilizzare delle misure oggettive e indipendenti per le valutazioni [12]. La valutazione del rischio associato agli asset viene infatti effettuata in maniera soggettiva e sulla base di interviste a coloro che lavorano direttamente con ogni risorsa. Queste persone sono chiamate a fornire un proprio parere su gli asset, le minacce, il livello di rischio e tutte le altre grandezze che il team di assessment deve analizzare. Il giudizio su ognuna di esse viene espresso utilizzando delle scale del tipo basso-medio-alto, oppure attraverso dei valori compresi nell'intervallo [1,5]. Una volta raccolte le informazioni necessarie il team di assessment utilizza degli strumenti per trarre le proprie conclusioni sulla situazione del sistema. Uno degli strumenti più comuni è la matrice di rischio, la quale permette di individuare le situazioni di rischio relative ad un certo asset e riesce a determinare se è necessario intervenire o meno a mitigare il rischio individuato.
Esistono molti metodi qualitativi; a seguire verranno brevemente discussi: FMEA/FMECA, NIST 800-30 e CRAMM.
I metodi FMEA (Failure Mode and Effects Analysis) e FMECA (Failure Mode and Effects Criticality Analysis) [11] iniziano a diffondersi negli anni Cinquanta del secolo scorso, quando sono stati elaborati ai fini di analisi di affidabilità di armi. Sono stati successivamente utilizzati, fino ai giorni nostri, nell'industria aeronautica, spaziale ed elettronica. L'essenza della FMEA / FMECA è l'analisi di impatto di ogni potenziale difetto sulla funzionalità dell'intero sistema e l'ordine di potenziali difetti in base al livello di severità. Il metodo FMECA introduce inoltre l'analisi del grado di gravità del difetto ed esamina se ha carattere critico per la funzionalità del sistema esaminato. Tali metodi sono molto laboriosi e richiedono la conoscenza e l'esperienza di persone che li sappiano applicare.
La prima revisione del NIST SP 800-30 [18] ha reso la metodologia, in prece-

denza dedicata al processo di gestione del rischio, più focalizzata sulla valutazione dei rischi, anche se temi come la condivisione dei rischi e il mantenimento della valutazione del rischio sono comunque considerati. La revisione non è un approccio globale, ma fornisce una descrizione ad alto livello del processo di valutazione del rischio e propone cataloghi di conoscenze specifiche utili per ogni passo della fase.
Nel 1987 è stato creato dal CCTA (U.K. Government Central Computer and Telecommunications Agency), ora rinominato in Cabinet Office, il metodo CRAMM (CCTA Risk Analysis and Management Methodology), oggi alla sua quinta versione. CRAMM [31] comprende tre fasi, ciascuna supportata da questionari e linee guida. Le prime due fasi sono identificare e analizzare i rischi per il sistema, la terza raccomanda come questi rischi devono essere gestiti. Le tre fasi di CRAMM sono le seguenti:

1. L'istituzione degli obiettivi per la sicurezza:
    - Definire il limite per lo studio;
    - L'identificazione e la valutazione delle attività fisiche che fanno parte del sistema;
    - La determinazione del "valore" dei dati in possesso intervistando gli utenti circa i potenziali impatti di business che potrebbero derivare dalla mancata disponibilità, la distruzione, divulgazione o modifica;
    - Identificare e valorizzare le risorse software che fanno parte del sistema.
2. La valutazione dei rischi per il sistema proposto e dei requisiti per la sicurezza:
    - Identificare e valutare il tipo e il livello di minacce che possono influenzare il sistema;
    - Valutare il grado di vulnerabilità del sistema alle minacce identificate;

- La combinazione di valutazioni delle minacce e vulnerabilità, con valori delle attività per calcolare le misure di rischio.

3. Identificazione e selezione di contromisure che sono relative alle misure di rischi calcolati nella fase 2. CRAMM contiene una libreria molto grande con più di tremila contromisure dettagliate ed organizzate in oltre settanta raggruppamenti logici.

Capitolo 4

Cybersecurity Framework

La prima parte del capitolo descrive il cybersecurity framework realizzato dal National Institute of Standards and Technology (NIST)[1] in ogni sua componente, proseguendo con l'estensione apportata da Centro di Ricerca di Cyber Intelligence and Information Security (CIS) e dal Laboratorio Nazionale di Cyber Security.

4.1 NIST Cybersecurity Framework

Nel febbraio 2014 il NIST pubblica il documento "Framework for Improving Critical Infrastructure Cybersecurity" [17] nel quale si delinea uno standard al fine di proteggere i sistemi e le risorse più importanti per la sicurezza del paese e garantire che tutti i settori critici sostengono un certo livello di cybersecurity. Esso fornisce alle parti interessate un approccio basato sul rischio in grado di determinare la preparazione corrente in ambito cybersecurity, rifacendosi alle esigenze specifiche e le caratteristiche di ciascun settore di business. Nello specifico, offre una sintesi di processi e best practice fondati su criteri standard per la valutazione dei rischi e delle passività derivanti da

[1] Agenzia del governo degli Stati Uniti d'America facente parte del U.S. Department of Commerce, il cui compito è la promozione dell'economia americana attraverso la collaborazione con l'industria al fine di sviluppare standard, tecnologie e metodologie che favoriscano la produzione e il commercio.

minacce cibernetiche. I rischi sono organizzati attorno a cinque attività principali che i team di gestione e di sicurezza IT di un'azienda devono eseguire periodicamente: identificare, proteggere, rilevare, rispondere e recuperare.
Il Framework è suddiviso in tre parti: Core, Implementation Tier e Profile. Il sistema di Function e Category del Framework Core, di fatto, rappresenta il punto d'incontro tra Framework e standard aziendali.

4.1.1 Core

Il Framework Core fornisce una serie di attività da realizzare per ottenere specifici risultati per la sicurezza cibernetica, ed esempio linee guida per il raggiungimento di tali risultati. Il Core non è una checklist di operazioni da eseguire, bensì presenta i risultati chiave della sicurezza cibernetica identificati dall'industria, utili nella gestione del rischio. Gli elementi centrali sono: Functions, Categories, Subcategories e Informative References raffigurati in Figura 4.1.

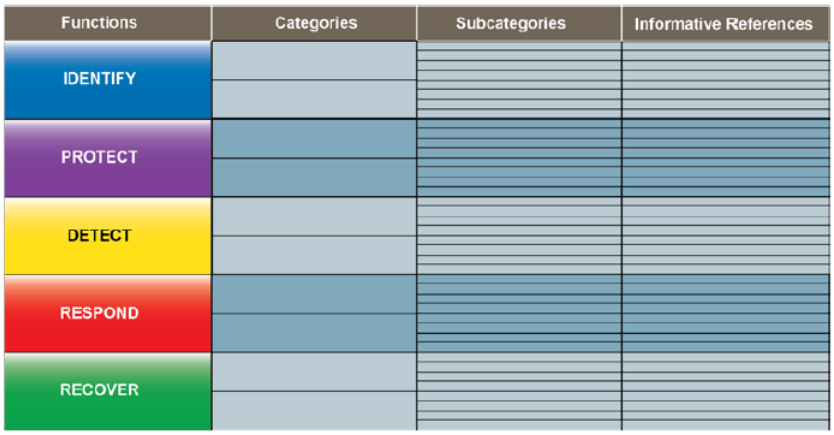


Figura 4.1: Struttura del Framework Core [17].

Functions Organizzano l'attività di base di cybersecurity al livello più alto. Queste funzioni sono Identify, Protect, Detect, Respond e Recover. Esse

aiutano un'organizzazione nella gestione del cyber-rischio per organizzare le informazioni, prendere decisioni, affrontare le minacce e di migliorare imparando da precedenti attività. Le funzioni si allineano anche con le metodologie esistenti per la gestione degli incidenti e contribuiscono a mostrare l'impatto degli investimenti. Ad esempio, gli investimenti in pianificazione ed esercitazione supportano tempestivamente le azioni di risposta e di recupero, con conseguente impatto ridotto per la fornitura di servizi.

Category Sono le suddivisioni di una Function in gruppi di cybersecurity outcome strettamente legati alle esigenze programmatiche e attività particolari. Esempi di Category sono: "Asset Management", "Access Control" e "Detection Processes".

Subcategory Divide ulteriormente una Category in risultati specifici delle attività tecniche e/o di gestione. Esse forniscono una serie di risultati che, seppur non esaustivi, contribuiscono a sostenere il raggiungimento dei risultati in ciascuna categoria. Esempi di sottocategorie sono "I sistemi informativi esterni sono catalogati", "Data-at-rest sono protetti" oppure "Le notifiche da sistemi di rilevamento sono osservate".

Informative Reference Sono sezioni specifiche di norme, linee guida e pratiche comuni tra i settori critici delle infrastrutture che illustrano un metodo per raggiungere i risultati associati ad ogni sottocategoria. Gli Informative Reference presentati nel Core sono esemplificativi e non esaustivi (ISO, SP800-53r4, COBIT-5, SANS20 e altri).

Le cinque Function Di seguito è riportata una breve descrizione delle cinque Function.

Identify Legata alla comprensione del contesto aziendale, degli asset che supportano i processi critici di business e dei relativi rischi associati. Tale comprensione permette infatti a un'organizzazione di definire risorse e

investimenti in linea con la strategia di gestione del rischio e con gli obiettivi aziendali. Le Category all'interno di questa Function sono:

- Asset Management;
- Ambiente di business;
- Governance;
- Valutazione del rischio;
- Strategia di gestione del rischio.

Protect Associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica. Le Category all'interno di questa Function sono:

- Access Control;
- Awareness and Training; Data Security;
- Information Protection Processes and Procedures;
- Maintenance;
- Protective Technology.

Detect Associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica. Le Category all'interno di questa Function sono:

- Anomalies and Events;
- Security Continuous Monitoring;
- Detection Processes

Respond Legata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato. L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica. Le Category all'interno di questa Function sono:

- Planning;

- Communications;
- Analysis;
- Mitigation;
- Improvements.

Recover Associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente. L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations. Le Category all'interno di questa Function sono:

- Recovery Planning;
- Improvements;
- Communications.

4.1.2 Implementation Tier

Gli implementation Tier inquadrano l'azienda, nel suo complesso, rispetto il rischio cyber e i processi posti in essere per gestirlo. Sono previsti quattro livelli di valutazione, dal più debole al più forte:

1. Parziale. Un modello di gestione del rischio di cybersecurity di una organizzazione è parziale se questo non tiene conto in modo sistematico del rischio cyber o delle minacce ambientali.

2. Informato. Un modello di gestione del rischio cyber di una organizzazione è informato se l'organizzazione ha dei processi interni che tengono conto del rischio cyber, ma questi non sono estesi a tutta l'organizzazione.

3. Ripetibile. Un modello di gestione del rischio cyber di una organizzazione è ripetibile se l'organizzazione aggiorna regolarmente le proprie pratiche di cybersecurity basandosi sull'output del processo di risk management.

4. Adattivo. Un modello di gestione del rischio cyber di una organizzazione è adattivo se l'organizzazione adatta le sue procedure di cybersecurity frequentemente attraverso l'utilizzo delle esperienze passate e degli indicatori di rischio.

4.1.3 Profile

Il Framework Profile è l'allineamento delle Function, Category e Subcategory con le esigenze di business, tolleranza al rischio e le risorse dell'organizzazione. Un Profilo consente alle organizzazioni di stabilire una tabella di marcia per ridurre il rischio di cybersecurity ben allineata con gli obiettivi organizzativi e di settore, considerando i requisiti legali, normativi e best practice. Data la complessità di molte organizzazioni, si può scegliere di avere più profili, in linea con particolari componenti e riconoscere le loro esigenze individuali.
I profili possono essere utilizzati per descrivere lo stato corrente o lo stato di destinazione desiderato di attività di sicurezza informatica specifiche. Il profilo corrente indica i risultati di cybersecurity che sono attualmente raggiunti, invece il profilo di destinazione indica i risultati necessari per raggiungere gli obiettivi di gestione del rischio desiderati.
Un confronto di profili (ad esempio, il profilo attuale e profilo target) può rivelare lacune da colmare, in cui le priorità di mitigazione sono dettate da esigenze di business dell'organizzazione e dei processi di gestione del rischio. Questo approccio basato sul rischio consente a un'organizzazione di valutare le stime delle risorse (ad esempio, il personale, il finanziamento) per raggiungere gli obiettivi di cybersecurity con un'efficienza nei costi, in maniera prioritaria.

4.2 Framework Nazionale

Il Centro di Ricerca Cyber Intelligence and Information Security ed il Consorzio Interuniversitario Nazionale per l'Informatica hanno presentato il

4 febbraio 2016 "Un Framework Nazionale per la Cyber Security" [2], in cui sostanzialmente si è esteso e specializzato quello redatto dal NIST. La volontà è quella di un allineamento a livello internazionale oltre che a livello di sistema paese, in quanto il Framework del NIST propone un quadro d'insieme altamente flessibile diretto principalmente alle infrastrutture critiche, quello italiano si adatta alle caratteristiche del sistema socio-economico che può essere contestualizzato su settori produttivi specifici o su tipologie di aziende con determinate caratteristiche. Può essere considerato il primo documento italiano che definisce la metodologia che un'azienda, a prescindere dalle sue dimensioni, può seguire per rendere più sicura la sua infrastruttura informatica. L'intento è quello di costruire un linguaggio comune per confrontare le pratiche aziendali di prevenzione e contrasto dei rischi cyber, andando ad aiutare un'impresa a organizzare un percorso di gestione del rischio cyber in funzione del suo business, della sua dimensione e di altri elementi caratterizzanti e specifici dell'impresa.
Nel Framework Nazionale sono stati aggiunti tre concetti importanti: livelli di priorità, livelli di maturità e contestualizzazione del Framework.

4.2.1 Livelli di priorità

I livelli di priorità supportano le organizzazioni e le aziende nell'identificazione preliminare delle Subcategory da implementare per ridurre maggiormente i livelli di rischio a cui sono sottoposte, distribuendo gli sforzi per la loro attuazione. L'obiettivo è quello di semplificare l'individuazione delle Subcategory essenziali da implementare e supportare le organizzazioni durante il processo di analisi e gestione del rischio.
La determinazione dei livelli di priorità assegnati alle Subcategory deve essere effettuata sulla base di due specifici criteri:

- Capacità di ridurre il rischio cyber, agendo su uno o più dei fattori chiave per la determinazione, ovvero:

  - esposizione alle minacce, intesa come l'insieme dei fattori che aumentano o diminuiscono la facilità con cui la minaccia stessa può manifestarsi;
  - probabilità di accadimento, ovvero la frequenza con cui una specifica minaccia può verificarsi nel tempo;
  - impatto conseguente sulle Business Operations o sugli Asset aziendali, intesa come l'entità del danno conseguente al verificarsi di una minaccia;

- Semplicità di implementazione delle Subcategory, anche considerando il livello di maturità tecnica e organizzativa tipicamente richiesto per realizzare la specifica azione.

La combinazione dei due criteri ha permesso di definire tre livelli distinti di priorità:

- Alta: interventi che permettono di ridurre sensibilmente uno dei tre fattori chiave del rischio cyber. Questi interventi sono prioritari e per loro natura sono da attuare indipendentemente dalla complessità realizzativa degli stessi;
- Media: interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber e che risultano generalmente anche di semplice implementazione;
- Bassa: interventi che permettono di conseguire una riduzione di uno dei tre fattori chiave del rischio cyber, ma la cui complessità realizzativa è generalmente considerata elevata (ad esempio cambiamenti organizzativi rilevanti e/o modifiche infrastrutturali significative).

4.2.2 Livelli di maturità

I livelli di maturità permettono di fornire una misura della maturità di un processo di sicurezza, di attuazione di una tecnologia specifica o della

quantità di risorse impiegate per l'implementazione di una data Subcategory. I livelli di maturità forniscono un punto di riferimento in base al quale ogni organizzazione può valutare la propria implementazione delle Subcategory e fissare obiettivi e priorità per il loro miglioramento. I livelli devono essere in progressione, dal minore al maggiore. Ogni livello deve prevedere pratiche e controlli incrementali rispetto al livello di maturità inferiore; per alcune Subcategory potrebbe non essere possibile definire livelli di maturità.
Si devono prevedere nella definizione dei livelli di maturità la specificità per Subcategory, dove un'organizzazione potrà avere livelli differenti di maturità per Subcategory differenti e la completezza delle pratiche di sicurezza, in cui il livello di maturità di una Subcategory è al pari con tutte le relative pratiche di sicurezza sono effettuate.
In generale il Framework fornisce solo delle regole per la definizione dei livelli di maturità e di priorità, poiché questi e i relativi controlli sono estremamente caratterizzati dalla natura dell'organizzazione, dal settore in cui opera, dalla struttura e dalla sua dimensione, nonché dal modello di business che segue.

4.2.3 Contestualizzazione del Framework

Adattare il Framework a un settore produttivo o ad una specifica categoria di organizzazioni significa circostanziare il suo core, ovvero selezionare le Function, Category e Subcategory e specificare i livelli di priorità e maturità per le Subcategory selezionate. Fino a questo momento, tutte le nozioni introdotte non considerano il settore produttivo, la tipologia degli impiegati, la dimensione e la dislocazione sul territorio dell'organizzazione. Quando si contestualizza il Framework, tutti o alcuni degli elementi precedentemente descritti devono essere tenuti in considerazione. Il Framework può essere contestualizzato:

- Dalla singola azienda per la gestione del suo programma di cybersecurity;

- Un'associazione di settore produttivo per rendere la contestualizzazione disponibile a tutte le aziende del settore;
- Un regolatore di settore per rendere la contestualizzazione disponibile a tutte le organizzazioni;
- Da un qualsiasi attore che fornisce una contestualizzazione in base a una o più caratteristiche che accomunano delle aziende.

Capitolo 5

Calcolo del rischio nello spazio cibernetico

A fronte dello studio condotto fin'ora, in questo capitolo si propone una riformulazione del rischio adattato al contesto cibernetico. Si tratta quindi della revisione della probabilità di accadimento e della valutazione dell'impatto di un evento.

5.1 Formula del rischio

La formula principale che descrive il rischio:

$$R = P \times I$$

dove R è il rischio dato dalla probabilità P (o frequenza) del verificarsi di un determinato evento per l'impatto I (o danno) che genera l'evento. Tale formula presenta dei limiti nell'applicazione in campo cibernetico.

Dati statistici Il primo problema è l'assenza di dati statistici in grado di determinare la frequenza di un incidente cibernetico. Le informazioni riguardanti una minaccia cibernetica vengono tenute private. Per esempio una compagnia, il più delle volte, tenderà a non rivelare le infrazioni in quanto

possono causare danni secondari importanti, come il danno reputazionale. Prendendo in considerazione il SAS OpRisk Global Data [4], il più grande e accurato repository al mondo di informazioni sulle perdite operative segnalate pubblicamente al di sopra di centomila dollari, che documenta trentaduemila eventi di tutti i settori tra il marzo 1971 e il settembre 2009 di cui circa solo mille relativi allo spazio cibernetico, di fatto non si dispone di un database pubblico completo e consistente sulle violazioni informatiche.

Misure di sicurezza Un altro fattore che incide sulla determinazione delle occorrenze di un attacco è la continua evoluzione delle tecnologie che porta con sé una continua evoluzione delle metodologie di attacco. Cambiando costantemente la tipologia di attacco non si hanno misure di sicurezza e standard in grado di determinare l'effettiva esposizione al rischio dell'organizzazione. Inoltre il livello di sicurezza di un sistema dipende da quello degli altri: un malware può infettare un canale stabilito con un partner dell'organizzazione.

Determinazione dell'impatto Quantificare l'impatto di un attacco informatico é parimenti un'operazione complicata in quanto esso è dato dalla stima dei beni materiali (pc, server, etc.) bensì dalla natura stessa dei beni immateriali, come il know-how e la quantità di informazioni gestite come dati medici e finanziari. In aggiunta anche danni secondari come il danno reputazionale, che riguarda gran parte dell'intero danno, è molto complesso da stimare.

5.2 Sostituzione della probabilità

Per i motivi appena citati si è scelto di sostituire la probabilità P con gli indici di sicurezza S e di esposizione E in modo da ridefinire il rischio cibernetico con la seguente formula:

$$R_C = \bar{S} \times E \times I$$

Dato che all'aumentare del livello di sicurezza diminuisce il fattore di rischio, nella formula si è posto $\bar{S}$ che equivale a $max - S$ dove max è il valore massimo che può assumere l'indice S. In altri termini $\bar{S}$ può essere denominato indice di insicurezza.

Livello di Sicurezza Si basa sulle ventidue attività previste dal Framework for Improving Critical Infrastructure Cybersecurity [17], le quali vengono associate ad un determinato livello di maturità in base al contesto in cui operano come spiegato nella Sezione 4.2.2.
Tali attività sono state riorganizzate in quattro categorie: Identificazione, Protezione, Rilevazione e Resilienza; di fatto si sono unite le due category Respond e Recover mantenendo invariate le altre. Per ogni categoria sono state selezionate le subcategory, nonché le informative reference relative, in base al livello di priorità con le quali devono essere implementate; nello specifico si è mantenuto quello industriale italiano ovvero della piccola e media impresa. Ogni subcategory ha una livello di priorità $L_P = \{basso, medio, alto\}$. Il peso totale della singola categoria è dato dalla somma di ogni singola attività in essa, in modo tale da avere quindi la seguente equazione:

$$S = \frac{\alpha ID + \beta PR + \gamma RI + \delta RE}{\alpha + \beta + \gamma + \delta}$$

dove α, β, γ e δ sono i rispettivi pesi totali delle priorità di ogni categoria: ID, PR, RI e RE. Ogni categoria è data dalla somma delle singole subcategory selezionate (es. $ID = \{id_1, id_2, \ldots\}$) per il loro livello di maturità $L_M = \{basso, medio, alto\}$ con le quali sono implementate nell'organizzazione.

Esposizione Riguarda l'identificazione dei fattori interni ed esterni che interessano l'esposizione al rischio. I fattori interni sono quelli legati ai dati detenuti, per cui la tipologia e la quantità a determinare questo fattore. Le principali categorie di dato sono:

- personali: nome, indirizzo e altre informazioni che consento l'identificazione di una persona;

- medici, per esempio cartelle cliniche;
- finanziari: dettagli bancari e finanziari (numero di conto, carte di credito, etc.).

Invece i fattori esterni sono alcune caratteristiche dell'organizzazione direttamente collegate con le tipologie di attacco. Queste caratteristiche sono:

- il settore in cui opera;
- il luogo in cui opera e se ha sedi in più stati;
- la dimensione globale dell'organizzazione (fatturato, dipendenti, etc.).

In conclusione, l'indice E risulta essere equivalente alla media pesata di tutti i fattori presi in considerazione.

5.3 Classi di rischio

Dati il livello di sicurezza e di esposizione si possono identificare quattro classi di rischio:

1. Resistente: (alto livello di sicurezza e bassa esposizione) il caso migliore, in cui il soggetto non si espone al rischio ed ha un sistema sufficientemente maturo;
2. Sensibile: (alto livello di sicurezza e alta esposizione) di ha una certa sensibilità al rischio di un attacco anche se si seguono correttamente le procedure per la gestione della cybersecurity;
3. Inesperto: (basso livello di sicurezza e bassa esposizione) si ha una bassa esposizione al rischio; occorre tuttavia alzare il livello di sicurezza del sistema per evitare incidenti cibernetici;
4. Vulnerabile: (basso livello di sicurezza e alta esposizione) il caso peggiore, in cui l'organizzazione può essere facile bersaglio di attacchi informatici per via dell'alta attrattività.

5.4 Valutazione dell'impatto

Come già introdotto nella Sezione 3.1 i danni ai fattori produttivi nonché gli elementi necessari alla produzione di un bene o all'erogazione di un servizio si distinguono in materiali e immateriali. Entrambe le immobilizzazioni, secondo l'art. 2424 del Codice Civile, sono da indicate nello stato patrimoniale del bilancio d'esercizio. Le immobilizzazioni immateriali sono:

1. costi di impianto e di ampliamento;
2. costi di sviluppo;
3. diritti di brevetto industriale e diritti di utilizzazione delle opere dell'ingegno;
4. concessioni, licenze, marchi e diritti simili;
5. avviamento;
6. immobilizzazioni in corso e acconti;
7. altre.

I primi due punti costituiscono gli oneri pluriennali, ovvero i costi sostenuti dall'impresa per l'acquisizione o la produzione di risorse e condizioni produttive aventi utilità pluriennali, produzione quindi destinata a non esaurirsi in un unico esercizio. I punti 3 e 4 costituiscono i beni immateriali, diritti che assicurano un controllo legale delle risorse e che tutelano l'azienda dallo sfruttamento altrui della medesima risorsa. Tali beni devono essere individualmente identificabili, devono rappresentare diritti giuridicamente tutelati e il loro costo è stimabile con sufficiente attendibilità.
Tra le altre immobilizzazioni immateriali sono inclusi i costi di software, ovvero i costi sostenuti per la produzione interna del software applicativo. Tali costi possono essere imputati al conto economico nel periodo di sostenimento oppure possono essere rilevati inizialmente tra le "altre immobilizzazioni immateriali" se hanno dato luogo a programmi utilizzabili per un certo numero di anni all'interno della società. I costi capitalizzabili comprendono solo i costi diretti (ad esempio gli stipendi ed i costi ad essi connessi del personale che ha lavorato direttamente sul progetto ed il cui lavoro sul progetto è pro-

priamente documentato e gli altri costi esterni). Sono invece esclusi i costi indiretti attribuibili al progetto, quali gli affitti, gli ammortamenti, i costi del personale con funzioni di supervisione ed altre voci simili.
La capitalizzazione dei costi inizia solamente dopo che la società sia ragionevolmente certa del completamento e dell'idoneità all'uso atteso del nuovo software. Se, ad esempio, il progetto ha un obiettivo specifico e si basa su una tecnologia provata (ad esempio, un sistema di contabilità fornitori), la capitalizzazione può iniziare prima, ma comunque non prima che la fase di fattibilità sia completata (cioè quando inizia la fase di progettazione del sistema o il contratto con i terzi è firmato).
L'ammortamento del costo del software non tutelato è effettuato nel prevedibile periodo di utilizzo. Il software di base, essendo strettamente correlato all'hardware, è trattato alla stregua di una componente di un'immobilizzazione materiale [21].
Invece, le immobilizzazioni materiali comprendono:

1. terreni e fabbricati;
2. impianti e macchinari;
3. attrezzature industriali e commerciali;
4. altri beni;
5. immobilizzazioni in corso e acconti.

In questa tipologia di beni rientra tutta l'infrastruttura tecnologica, quindi la parte fisica dello spazio cibernetico.

5.4.1 Stimare il costo del software

Produttività

La valutazione del costo del software dipende dalla produttività dello stesso. Le stime di produttività sono generalmente basate sulla misurazione di determinati attributi del software e poi divise per lo sforzo totale richiesto per lo sviluppo. Le due metriche usate sono di due tipi:

1. Dimensionali: dipendono dalla dimensione di uno o più output legati ad un'attività. La metrica più comunemente usata è data dalle linee di codice prodotte. Altri parametri che possono essere utilizzati sono il numero di istruzioni di codice oggetto e il numero di pagine di documentazione del sistema.

2. Funzionali: dipendono dalle funzionalità complessive del codice. La produttività è espressa nei termini dell'ammontare di funzionalità realizzate in un determinato periodo temporale. Le metriche meglio conosciute sono function points e object points.

Le linee di codice per programmatore-mese (LOC/pm) sono ampiamente usate come metrica per la produttività. Si può calcolare LOC/pm contando il numero totale di linee di codice sorgente, diviso il numero di programmatori-mesi richiesti per completare il progetto.
Questo approccio è stato sviluppato quando la maggior parte della programmazione era in FORTRAN, assembly o COBOL e i programmi erano scritti su schede perforate. Il numero di linee di codice era facile da contare: su ogni scheda era presente uno statement, quindi bastava contare il numero di schede totali. Ora, in linguaggi di programmazione come Java o C++ in cui si possono includere macro che espandono il programma a molte linee di codice o al contrario mettere più istruzioni in un'unica linea, viene meno la semplice relazione tra istruzioni e linee di codice.
Confrontare la produttività dei linguaggi di programmazione può non essere corretto in quanto taluni possono essere molto espressivi ma con un'apparente minore produttività. Questa anomalia è dovuta al fatto che tutte le attività di sviluppo del software sono considerate insieme nel calcolo del tempo di sviluppo, ma la metrica LOC si applica solo al processo di programmazione. Pertanto se un linguaggio richiede più linee di un altro per implementare la stessa funzionalità, la stima di produttività è falsata.
Per sopperire a queste anomalie si può stimare qualche attributo del software, per esempio il numero di funzionalità che sono indipendenti dal linguaggio di programmazione. La produttività è espressa in numero di function

point implementate per persona-mese. Una function point non è una singola caratteristica ma una combinazione di diverse misurazioni o stime come:

- input/output esterni;
- user interaction;
- interfacce esterne;
- file usati dal sistema.

Ognuna di queste ha complessità diversa, quindi come si propone nella unadjusted function-point (UFC), ad ogni elemento di un dato tipo viene associato un peso. Il difetto di questa tecnica risiede nel fatto che dipende dalla complessità del sistema e da chi effettua la valutazione.
In alternativa alle function point ci sono gli object point, che possono essere usati con linguaggi di programmazione per database e di scripting, che non correlati all'approccio object-oriented. Il numero di object point di un programma è la valutazione pesata del:

- numero di schermate che sono visualizzate;
- numero di report che sono prodotti;
- numero di moduli che devono essere sviluppati in linguaggi come Java e C++ a supporto del codice dei linguaggi data-oriented.

Entrambe le tipologie presentano problemi: per esempio se si fanno calcoli solo sulla dimensione si tralascia quella che è la qualità del software come affidabilità e manutenibilità. D'altra parte la produttività del software dipende strettamente dal dominio di applicazione e dalle organizzazioni.
In generale vi è una serie fattori che influenzano la produttività come:

- la conoscenza del dominio applicazione;
- il processo di sviluppo utilizzato;
- la dimensione del progetto(più è grosso più è necessario spendere tempo nella comunicazione sacrificando lo sviluppo);

Tecniche di valutazione

Non c'è un modo semplice ed unico per valutare lo sforzo richiesto per sviluppare un software; a seguire le principali tecniche utilizzate.

- Modellazione algoritmica dei costi: un modello è sviluppato utilizzando le informazioni del costo storico che si riferisce ad alcune metriche software (di solito le sue dimensioni) per il costo del progetto.
- Expert judgement: sono consultati diversi esperti e ognuno stima il costo del progetto. Successivamente tali stime vengono messe a confronto per raggiungere una stima di comune accordo.
- Stima per analogia: l'applicabile quando altri progetti dello stesso dominio di applicazione sono terminati e quindi sono presi come riferimento.
- Parkinson's law: la legge afferma che il lavoro occupa tutto il tempo a disposizione, quindi il costo è determinato dalle risorse disponibili piuttosto che dalla valutazione oggettiva.
- Pricing to win: il costo del software stimato coincide con il budget che il cliente ha a disposizione per il progetto, quindi non dipende dalle funzionalità del software.

Modellazione algoritmica dei costi La modellazione algoritmica dei costi utilizza una formula matematica per prevedere i costi del progetto sulla base di stime della dimensione del progetto, del numero di ingegneri del software e di altri fattori di processo e di prodotto.
Nella sua forma generale questa tecnica può essere formalmente espressa come

$$\text{Costo} = A \times \text{Size}^B \times M$$

dove A è un fattore costante che dipende da pratiche organizzative e dal tipo di software prodotto. La dimensione può essere data dalla valutazione della

dimensione del codice o dalle funzionalità espresse. Il valore dell'esponente B varia da 1 a 1.5. M è un moltiplicatore dato dalla combinazione di processi, prodotti e attributi di sviluppo come la dipendenza di requisiti richiesti e l'esperienza del team di sviluppo. Il fattore esponenziale B indica che i costi non crescono linearmente col crescere delle dimensioni del progetto, in quanto l'aumento della complessità è esponenziale. Questi ultimi due fattori sono soggettivi quindi la stima dipende dal grado di esperienza dell'esperto.
Il COnstructive COst MOdel (COCOMO) è un modello matematico creato da Barry Boehm realizzato attraverso una preliminare raccolta di dati provenienti da un gran numero di progetti. La prima versione risale al 1981, invece la seconda è stata pubblicata nel 2000.
COCOMO 81 era un modello a tre livelli, ciascuno dei quali corrisponde al dettaglio dell'analisi di costo. Con COCOMO II vengono introdotti nuovi approcci di sviluppo software come la prototipazione, lo sviluppo per componenti e l'uso di linguaggi per database. I diversi sottomoduli che fanno parte di COCOMO II sono:

1. Un modello applicazione-composizione. Questo presuppone che i sistemi derivino da componenti riutilizzabili, di scripting o includenti database e che siano progettati per fare delle stime sullo sviluppo del prototipo. La stima della dimensione del software si basa sui application point e su una formula dimensione-produttività che viene utilizzata per quantificare lo sforzo richiesto. Gli application point equivalgono agli object point.

2. Un modello di progettazione iniziale. Questo modello è usato durante le prime fasi della progettazione del sistema dopo che sono stati stabiliti i requisiti. Le stime sono basate sui function point che vengono poi convertiti in numero di linee di codice sorgente. La formula segue quella standard discussa in precedenza con una serie semplificata di sette moltiplicatori.

3. Un modello di riutilizzo. Questo modello è utilizzato per calcolare

lo sforzo richiesto per integrare i componenti riutilizzabili e/o codice di programmi generati automaticamente dalla progettazione o da strumenti di traduzione. Solitamente è usato in combinazione con il modello post-architetturale.

4. Un modello post-architetturale. Una volta che l'architettura del sistema è stata progettata, una stima più precisa della dimensione software può essere effettuata. Anche in questo modello si utilizza la formula standard per la stima dei costi discussi in precedenza. Tuttavia, esso include un più ampio insieme di 17 moltiplicatori che riflettono la capacità del personale e le caratteristiche del prodotto e di progetto.

5.4.2 Quantificare l'informazione

Oltre alla valutazione dell'intera infrastruttura tecnologica (fisica) e quella del software in uso all'interno dell'organizzazione, si devono quantificare i dati in possesso. Fare una stima del valore potenziale delle informazioni che non rientrano nello stato patrimoniale tra le immobilizzazioni immateriali è da considerarsi pratica complessa. I tipi di informazioni sensibili che rientrano in questa categoria sono:

- dati personali, che identificano le informazioni relative alla persona fisica, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altro dato, ivi compreso un numero di riconoscimento personale [1];
- dati medici, cartelle cliniche e altri dati relativi al campo medico-sanitario;
- dati bancari e finanziari, come estremi della carta di credito e coordinate bancarie.

Si tratta quindi di valutare un dato che non è acquistabile sul mercato (legale) ma la cui compromissione causa un danno economico all'organizzazione.

[1] Art. 4 c.1, lettera b, D.Lgs. 196/2003.

Per quanto riguarda tutte le altre informazioni detenute dall'organizzazione qui non elencate, si ipotizza che il valore dell'informazione sia equivalente al danno a seguito dell'interruzione di esercizio. Nel caso di business interruption il danno è pari al reddito originato dalla gestione caratteristica d'impresa che risulta cessante per il mancato svolgimento.
Seguendo lo studio condotto da Algarni et al. [1], in cui si mettono a confronto i principali calcolatori di costi per data breach, i fattori chiave che li accomunano sono riassumibili nei seguenti punti:

- numero totale di record;
- tipo di dato e tipo di business;
- dimensione dell'organizzazione (totale dipendenti, mercato, sedi principali, etc.)
- dove risiedono i dati;
- fattori vari:
  - se si ha subito in precedenza almeno una violazione;
  - complicazioni riguardanti Payment Card Industry;
  - se c'è stato un coinvolgimento in una class action.

Nello specifico studio Ponemon [23] sono stati identificati sedici fattori volti alla determinazione del costo e della probabilità di accadimento:

1. team specializzato nella risposta agli incidenti;
2. ampio utilizzo della crittografia;
3. addestramento dipendenti;
4. partecipazione nella condivisione delle minacce;
5. coinvolgimento nel Business Continuity Management[2];

[2]Processo orientato all'identificazione dei rischi e all'analisi dei potenziali impatti su un'organizzazione nel suo complesso.

6. ampio uso DLP[3];
7. la designazione di un chief information security officer (CISO);
8. coinvolgimento del consiglio;
9. schema per la classificazione dei dati;
10. protezione assicurativa;
11. adozione di una protezione ID;
12. consulenze;
13. perdita o furto dei device;
14. tempestività nella notifica;
15. ampia migrazione su spazi cloud;
16. coinvolgimento di terze parti.

[3]Insieme di tecniche e sistemi che identificano, monitorano e proteggono i dati in uso, in movimento e i e dati a riposo all'interno o all'esterno dell'azienda, con il fine di individuare e prevenire l'uso non autorizzato e la trasmissione di informazioni riservate.

Capitolo 6

Formalizzazione dello strumento di valutazione

In conclusione, dopo la completa esposizione del problema con la conseguente proposta teorica riportata nel capitolo precedente, in questo capitolo vengono descritti quali strumenti sono stati realizzati.

6.1 Realizzazione del modello

Gli strumenti necessari per l'implementazione di un modello ai fini della valutazione del cyber-rischio sono:

- un database dei profili che identifica la classe di rischio di appartenenza;
- un database di tutti gli incidenti informatici ai fini della realizzazione di una collezione storica.

I profili e gli incidenti devono essere messi in correlazione per poter bilanciare costantemente variabili e pesi appartenenti al modello matematico.

Questionario

Si è quindi realizzato un questionario (appendice A) al cui termine viene fornita:

- un'indicazione grafica del proprio livello di sicurezza e una classificazione in base all'esposizione al rischio;
- un report in cui si evidenziano le principali problematiche e le azioni da implementare (appendice B) per una efficace strategia di gestione del cyber-rischio.

La compilazione del questionario è rivolta ai responsabili dell'area IT dell'organizzazione e serve a popolare il database dei profili. Il questionario è diviso in due parti:

1. Profilo generale, in cui si raccolgono i dati di carattere generale già elencati nella Sezione 5.2. Solo una parte di questi sono usati per determinare l'indice di esposizione, ovvero:
   (a) settore e luogo in cui opera;
   (b) quantità di dati processati.

   I pesi dei fattori del punto (a) sono determinati dalle percentuali riportate nel rapporto Clusit [7], mentre il fattore (b) cresce linearmente in base alla quantità di dati.
2. Quattro fasi della gestione del rischio (identificazione, protezione, rilevamento e resilienza). Come è stato specificato nella Sezione 5.2, ogni fase è determinata dalla somma delle singole attività i cui pesi fanno riferimento al contesto piccola-media impresa approntati nel Framework Nazionale [2].

Tale strumento (Figura 6.1) è raggiungibile all'indirizzo http://130.136.143.32/ e svolge una duplice funzione di:

- un'autovalutazione da parte dell'entità che decide di compilare il questionario dando una prima valutazione di rischio cibernetico;
- una registrazione in forma anonima di come le entità sono organizzate nelle varie aree di gestione del rischio a fini statistici.

Figura 6.1: Cyber Risk Assessment Tool (home page).

6.2 Classificazione degli incidenti

Capire l'impatto dell'incidente è fondamentale nella valutazione della sua gravità e nella messa a fuoco delle aree coinvolte nel controllo della cybersecurity. Inoltre, un impatto può diventare una richiesta d'indennizzo assicurativo se un prodotto in questione è stato acquistato e copre questo tipo di perdita.
Classificare l'impatto ha lo scopo principale di costruire una banca dati che includa anche le perdite subite a seguito di un incidente informatico. Quindi è importante utilizzare queste categorie per registrare tutti gli impatti che interessano gli incidenti informatici, anche quelli non coperti da assicurazione, in modo d'acquisire una migliore comprensione del rischio e del suo impatto. Le categorie individuate convergono con il Cyber Exposure Data Schema (v0.9) dell'Università di Cambridge [6].

- Business Interruption:

  - Perdita di profitti a causa dell'indisponibilità del proprio sistema tecnologico o dei dati, originata da un evento informatico, non necessariamente a fini malevoli.
  - Perdita di profitti a causa dell'indisponibilità del sistema IT di terzi, nonché fornitori e servizi esterni.

- Cyber estorsione: l'ammontare dei costi a seguito della gestione di un'estorsione, compresa la cifra del riscatto.

- Costi di indagine e di ripristino: costi diretti sostenuti nell'indagine e nella chiusura di un incidente al fine di minimizzare le perdite (applicabile a tutte le categorie di eventi).

- Costi legali: copre i servizi forensi, tecnici o legali necessari per rispondere alle richieste di informazioni governative relative a un attacco informatico. Fornisce copertura per sanzioni, costi di difesa legale, indagini o altri atti normativi a seguito della violazione della legge sulla privacy e per altre spese imposte da enti regolatori e associazioni di settore.

- Danno ambientale: risarcimento a seguito della fuoriuscita di prodotti tossici e/o inquinanti scaturita da un cyber-evento.

- Danno beni materiali: perdita dei propri beni materiali a seguito di un cyber attacco.

- Danno reputazionale: compensazione della perdita di profitto a causa della riduzione di mercato/clienti dopo la comunicazione di avvenuta violazione all'interno dell'organizzazione.

- Diffamazione e denigrazione: costi di compensazione dovuti all'uso improprio dei mezzi di comunicazione con conseguente diffamazione o calunnia di terzi, tra cui web page defacement, nonché violazione del copyright e della proprietà intellettuale.

- Frode o furto finanziario: la perdita finanziaria subita da un'organizzazione a causa di frode o furto di denaro, titoli o altri beni per un attacco informatico.

- Furto della proprietà intellettuale: perdita del valore di una proprietà intellettuale espressa in termini di profitto della quota di mercato.

- Morte e lesioni personali: responsabilità per morte e lesioni personali di terzi a seguito di un cyber attacco.

- Network failure: responsabilità di terzi derivante da determinati eventi di cybersecurity che si verificano all'interno della rete informatica dell'organizzazione o che passano attraverso di essa al fine di attaccarne una terza.

- Perdita di dati e/o software: costi per il ripristino del software e/o dati persi, rubati, distrutti, danneggiati o criptati.

- Prodotti e operazioni: passività di terzi che derivano dai propri prodotti e operazioni difettose a causa di un cyber evento. Altri casi specifici:

  - Errori e omissioni tecniche;
  - Errori e omissioni di servizi professionali.

- Responsabili e superiori: costi per il risarcimento contro i superiori e i responsabili del business per abuso di fiducia o violazione dei doveri derivanti da incidenti informatici. Possono provenire da una presunta cattiva condotta o dal fallimento di un'azione svolta nel migliore interesse per la società, per i suoi dipendenti e per i suoi azionisti.

- Violazione della privacy: costi di indagine e risposta alla violazione dei dati.

6.3 Bilanciamento del modello

Una volta organizzati i due database, il passo successivo è metterli in correlazione. Quindi si ha:

- da una parte, un insieme di profili con i relativi indici di sicurezza e di esposizione, che nel loro insieme rappresentano il livello medio di gestione del cyber-rischio;
- dall'altra, tutti gli eventi informatici che caratterizzano la scena, mettendo in evidenza la quantità e la tipologia di quest'ultimi.

Lo scenario ideale prevede la registrazione del profilo di ogni organizzazione che ha affrontato un incidente informatico; gli stessi profili posso evolvere nel tempo e sono mantenuti come storico. La dipendenza tra le due basi di dati serve:

- per affinare l'indice di sicurezza e di esposizione, riconsiderando i singoli pesi dei vari fattori in relazione alla tipologia e alla quantità degli eventi che colpiscono le organizzazioni;
- nel caso lo strumento fosse utilizzato da una compagnia assicurativa. E quindi, nello specifico:
  - la classificazione degli eventi dovrebbe essere accompagnata anche dalle richieste avanzate dalle singole organizzazioni per le coperture assicurative;
  - nel complesso si avrebbero gli strumenti necessari per un accurato calcolo del premio.

In conclusione si può affermare che tale strumento potrebbe essere usato, oltre che dalle singole organizzazioni come strumento di prima valutazione del cyber-rischio, anche da una compagnia assicurativa in quanto consentirebbe la stipulazione delle polizze e contemporaneamente la raccolta del maggior

quantitativo possibile di dati sia relativi al cliente che alle scelte dell'assuntore. In questo modo, negli anni, si creerebbe una vera e propria base di dati interna su cui calibrare il modello.

Appendice A

Questionario

Profilo Generale

1. In che settore opera l'azienda?[1]

    - Governativo, Militare, LEA o Intelligence
    - Online Services e Cloud (webmail, social network, eCommerce, etc)
    - Intrattenimento e News (siti d'informazione, piattaforme di gaming, blogging, etc)
    - Ricerca e Istruzione
    - Banche e Servizi Finanziari
    - Fornitore di Software e/o Hardware
    - Ricettività (organizzazioni alberghiere, ristoranti, recidence e collettività)
    - Organizzazioni e ONG
    - Sanità
    - Infrastrutture Critiche
    - Telecomunicazioni
    - GDO e Retail
    - Goverment Contractors e Consulenze

[1]Settori definiti nel Rapporto Clusit 2016 sulla sicurezza ICT in Italia.

- Altro

2. In che Stato si trovano le sedi principali dell'azienda?
3. Ha sedi in più Stati?
4. Società terze hanno accesso alle sedi?
5. Qual è il fatturato annuale (milioni di euro)?
   - 0 - 2 / 2 - 10 / 10 - 50 / 50 - 500 / Oltre 500
6. Quanto consta l'organico dell'azienda?
   - 0 - 9 / 10 - 49 / 50 - 249 / 250 - 1000 / Oltre 1000
7. Quanti dati personali gestisce[2]?
   - Nessun dato / Solo quelli dei dipendenti / 0 - 5000 / 5.000 - 25.000 / 25.000 - 100.000 / 100.000 - 1 mln / Oltre 1 mln
8. Quanti dati medici gestisce (cartelle mediche)?
   - Nessun dato / Solo quelli dei dipendenti / 0 - 5000 / 5.000 - 25.000 / 25.000 - 100.000 / 100.000 - 1 mln / Oltre 1 mln
9. Quanti dati finanziari gestisce? (carte di credito, dettagli bancari, etc)
   - Nessun dato / Solo quelli dei dipendenti / 0 - 5000 / 5.000 - 25.000 / 25.000 - 100.000 / 100.000 - 1 mln / Oltre 1 mln

Identificazione

1. Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione?
   - Si, avviene in modalità perlopiù manuale secondo un processo definito e controllato
   - Si, in modalità completamente automatica dove si cura l'intero ciclo di vita dell'asset
   - No

[2]Personally Identifiable Information, NIST SP 800-122.

2. Sono censite le piattaforme e le applicazioni software in uso e nell'organizzazione?
    - Si, avviene in modalità perlopiù manuale secondo un processo definito e controllato
    - Si, in modalità completamente automatica dove si cura l'intero ciclo di vita dell'asset
    - No
3. I flussi di dati e le comunicazioni inerenti l'organizzazione sono identificati?
    - Si / Parzialmente / No
4. Le risorse hanno priorità in base alla loro classificazione (e.g. confidenzialità, integrità, disponibilità), criticità e valore per il business dell'organizzazione?
    - Si / Parzialmente / No
5. Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)?
    - Si, vi è un referente per la cybersecurity e un disciplinare tecnico per l'utilizzo consono delle informazioni e degli strumenti informatici da parte di tutte le parti interessate
    - Si, esiste un documento di politica aziendale per la cybersecurity che definisce ruoli e responsabilità.
    - No
6. Quali delle seguenti sono identificate e rese note?
    - Priorità per quanto riguarda la missione, gli obiettivi e le attività dell'organizzazione
    - Interdipendenze e funzioni fondamentali per la fornitura di servizi critici
    - I requisiti di resilienza a supporto della fornitura di servizi critici

7. Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione sono compresi e utilizzati nella gestione del rischio di cybersecurity?
    - È identificata e resa nota una policy di sicurezza delle informazioni
    - Ruoli e responsabilità inerenti la sicurezza delle informazioni sono coordinati ed allineati con i ruoli interni ed i partner esterni?
    - I requisiti legali in materia di cybersecurity, con l'inclusione degli obblighi riguardanti la privacy e le libertà civili, sono compresi e gestiti
    - 4 La governance ed i processi di risk mangement includono la gestione dei rischi legati alla alla cybersecurity
8. L'impresa comprende il rischio di cybersecurity inerente l'operatività dell'organizzazione, gli asset e gli individui? Quali delle seguenti vengono identificate e documentate?
    - Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione
    - Le possibili minacce sia interne che esterne
    - I potenziali impatti sul business e le relative probabilità di accadimento
9. Le priorità, i requisiti dell'organizzazione e la tolleranza al rischio sono definiti e utilizzati per supportare le decisioni sul rischio operazionale?
    - Si / Parzialmente / No

Protezione

1. L'accesso agli asset ed alle relative risorse è limitato al personale, ai processi, ai dispositivi, alle attività ed alle transazioni effettivamente autorizzate?
    - Le identità digitali e le credenziali di accesso per gli utenti e per i dispositivi autorizzati sono amministrate

- L'accesso fisico alle risorse è protetto e amministrato
- L'accesso remoto alle risorse è amministrato
- Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e delle separazioni delle funzioni
- L'integrità di rete è protetta anche applicando la segregazione di rete dove appropriata.

2. Il personale è formato in materia di cybersecurity e riceve un'adeguata preparazione, coerente con le politiche, le procedure e gli accordi esistenti, per svolgere correttamente i compiti e le responsabilità legate alla sicurezza delle informazioni?

   - Tutti gli utenti sono informati ed addestrati
   - Gli utenti privilegiati comprendono ruoli e responsabilità
   - Tutte le terze parti (e.g. fornitori, clienti, partner) comprendono ruoli e responsabilità
   - I dirigenti ed i vertici aziendali comprendono ruoli e responsabilità
   - Il personale addetto alla sicurezza fisica e delle informazioni comprende i ruoli e le responsabilità

3. I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenza e la disponibilità delle informazioni?

   - Si / Parzialmente / No

4. Sono attuate e adeguate nel tempo politiche di sicurezza, processi e procedure per gestire la protezione dei sistemi informativi e degli assets?

   - Sono definite e gestite delle pratiche di riferimento per la configurazione dei sistemi IT e di controllo industriale
   - Viene implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle)
   - Sono attivi processi di controllo della modifica delle configurazioni

- I backup delle informazioni sono eseguiti, amministrati e verificati periodicamente
- Sono rispettate le policy ed i regolamenti relativi agli ambienti fisici in cui operano le risorse dell'organizzazione
- I dati sono distrutti in conformità con le policy
- Sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro
- Viene sviluppato e implementato un piano di gestione delle vulnerabilità

5. La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti?
   - Si / Parzialmente / No
6. Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi?
   - Esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi
   - I supporti di memorizzazione sono protetti ed il loro uso è ristretto in accordo alle policy
   - L'accesso alle risorse e ai sistemi è limitato secondo il principio di minima funzionalità
   - Le reti di comunicazione e controllo sono protette

Rilevazione

1. Le attività anomale sono rilevate e il loro impatto potenziale viene analizzato?
   - Si, esistono procedure atte a rilevare eventi anomali e determinare il superamento delle soglie di allerta

- Si, ma non viene stimato il loro impatto
- No

2. I sistemi informativi e gli asset sono monitorati periodicamente per identificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione?
   - Viene svolto il monitoraggio degli spazi fisici per rilevare potenziali eventi di cybersecurity
   - Viene svolto il monitoraggio del personale per rilevare potenziali eventi di cybersecurity
   - Viene svolto monitoraggio ai fini dell'identificazione di codice malevolo
   - Viene svolto il monitoraggio delle attività dei attività dei service provider esterni per rilevare potenziali eventi di cybersecurity
   - Viene svolto il monitoraggio per rilevare il personale, connessioni, dispositivi o software non autorizzati
   - Vengono svolte scansioni per l'identificazione di vulnerabilità
3. Sono adottati, mantenuti e verificati nel tempo i processi e le procedure di monitoraggio per una tempestiva e adeguata comprensione degli eventi?
   - Si / Parzalmente / No

Resilieza (Risposta e Ripristino)

1. Esiste un piano di ripristino e questo viene eseguito durante o dopo un incidente?
   - Si / No
2. Nel caso esista un piano di ripristino:
   - Le attività di ripristino sono migliorate incorporando le lezioni passate da attività precedenti di monitoraggio e risposta

- Sono coordinate con le parti interne ed esterne, per includere eventuale supporto da parte degli organi di legge o dalle forze dell'ordine

3. Vengono condotte analisi per assicurare un'adeguata risposta e supporto alle attività di ripristino?
   - Si / Parzialmente / No
4. Vengono eseguite procedure atte a contenere l'impatto e mitigare gli effetti di un incidente?
   - Si, la risposta agli incidenti di cybersecurity avviene attraverso una formale procedura aziendale costantemente aggiornata
   - Si, il processo di gestione degli incidenti prevede la registrazione dell'incidente e che attività vengono svolte per la gestione di quest'ultimo
   - No
5. Esiste un piano di risposta e viene eseguito durante o dopo un evento?
   - Si / No
6. Nel caso esista un piano di risposta:
   - Le strategie di recupero sono aggiornate e tengono in considerazione le esperienze passate
   - Sono coordinate con le parti interne ed esterne

Appendice B

Best Practices

A seguire una breve guida, ripresa parzialmente dal "2015 Italian Cyber Security Report - Un Framework Nazionale per la Cyber Security" [2], sulle attività essenziali per il contrasto al rischio cibernetico.

Identificazione

- Identificazione degli asset: È indispensabile pertanto disporre di un inventario di tutti gli asset rappresentati dalle informazioni, applicazioni, sistemi e apparati informatici presenti all'interno dell'azienda. Registrare attributi importanti, come ad esempio la posizione fisica, il proprietario, la funzione di riferimento, le dipendenze, ecc. risulta funzionale alle attività di governo e gestione della cybersecurity.

- Assegnazione Responsabilità: È fondamentale che tutto il personale sia consapevole dei ruoli e delle responsabilità di sicurezza, correlate allo svolgimento della attività lavorative. Ai vertici aziendali, nelle figure dell'amministratore delegato, del consiglio di amministrazione, della dirigenza e più in generale alla "proprietà", è assegnato il ruolo chiave di definizione delle priorità e di assegnazione delle risorse associate alle iniziative di cybersecurity.

- Conformità a Leggi e Regolamenti: L'organizzazione ha l'obbligo di conoscere e ottemperare alle leggi e ai regolamenti applicabili al proprio contesto, soprattutto in relazione ai mercati in cui essa opera e alla tipologia di servizi informatici fruiti e/o erogati.

Protezione

- Protezione perimetrale: Le reti di computer di un organizzazione, collegate a Internet o interconnesse con altre reti, devono essere protette da attaccanti volti ad avere accesso ai sistemi, computer e alle informazioni ivi contenute. Un dispositivo di sicurezza di rete come il firewall, posizionato sul perimetro della rete, è in grado di proteggere la stessa contro le minacce cyber basilari - attacchi che richiedono capacità e tecniche limitate, e che conseguentemente risultano largamente diffusi - limitando il traffico di rete in entrata e in uscita alle sole connessioni autorizzate.

- Controllo Accessi: Modalità di controllo accessi devono essere stabilite per limitare l'accesso alle informazioni, applicazioni, sistemi, reti e in generale dispositivi informatici aziendali da parte di tutti le tipologie di utenti. L'obiettivo è garantire che solo gli utenti effettivamente autorizzati possano accedere a tali sistemi o dati, assicurando il livello di privilegio minimo necessario a esercitare le proprie funzioni.

- Configurazione Sicura dei Sistemi: Spesso le credenziali amministrative, o in generale le configurazioni impostate dal produttore, sono pubbliche o insicure e potrebbero essere usate per ottenere l'accesso non autorizzato ai sistemi di un'azienda e alle informazioni in questi contenute. Applicando alcuni semplici accorgimenti di sicurezza durante la configurazione di nuovi computer o sistemi informatici è possibile ridurre considerevolmente i rischi e le probabilità che un attacco informatico vada a buon fine.

- Aggiornamento dei Sistemi: I software presenti su tutti i computer e più in generale sui sistemi informatici possono contenere difetti ed errori, genericamente conosciuti come "vulnerabilità". Queste rappresentano degli elementi di debolezza intrinseci, sfruttabili da individui o gruppi di attaccanti, come anche da malware o altri programmi malevoli. Le vulnerabilità, dal momento della loro scoperta, fino al momento in cui sono eventualmente sfruttate, devono essere individuate e gestite attraverso opportune contromisure, come ad esempio l'installazione degli aggiornamenti rilasciati dai produttori software, proprio per risolvere una o più vulnerabilità.

- Formazione di Base del Personale: Gli utenti delle aziende che interagiscono con i sistemi informatici rappresentano la principale fonte di rischio cyber. I comportamenti non consoni o errati possono vanificare le più sofisticate misure di sicurezza adottate da un'azienda. Per migliorare la consapevolezza degli utenti nell'utilizzo consono degli strumenti informatici e delle informazioni, l'organizzazione deve prevedere specifici programmi di sensibilizzazione e formazione, volti a migliore la percezione dei rischi cyber e a promuovere l'utilizzo di comportamenti appropriati.

- Backup e Restore: Il controllo primario da attuare è rappresentato dal salvataggio delle informazioni di business e delle configurazioni dei sistemi, su supporti dedicati, da impiegare in caso di disastri, guasti o errori umani, favorendo il ripristino della normale operatività.

Rilevazione

- Protezione da Malware: I sistemi informativi sono comunemente esposti a software malevoli, denominati malware, soprattutto se connessi a internet. La compromissione attraverso malware può avvenire mediante diverse modalità, quali l'apertura di una e-mail infetta, la navigazione

su siti compromessi, l'apertura di file su dispositivi locali o contenuti su memorie di massa esterne (come Storage USB). Soluzioni di protezione specifiche devono essere adottate per monitorare, individuare e rimuovere il software malevolo.

Resilienza

- Risposta agli Incidenti di Sicurezza: Nei casi in cui le misure di sicurezza non siano in grado o risultino limitatamente efficaci nella prevenzione di eventi avversi di sicurezza (es. compromissione di un sistema, accesso non autorizzato alle informazioni), l'organizzazione deve avere la capacità di rispondere rapidamente ed efficacemente a un potenziale incidente di sicurezza, riducendo gli impatti e limitando la possibilità di occorrenze future.

Bibliografia

[1] Algarni A. M., Malaiya Y., *A Consolidated Approach for Estimation of Data Security Breach Costs*, 2016 2nd International Conference on Information Management (ICIM 2016)–IEEE, EI May 7-8, 2016.

[2] Baldoni R., Montanari L., *Un Framework Nazionale per la Cyber Security*, 2015 Italian Cyber Security Report, Febbraio 2016. http://www.cybersecurityframework.it/sites/default/files/CSR2015_web.pdf.

[3] Behnia A., Rashid R. A., Chaudhry J. A., *A Survey of Information Security Risk Analysis Methods*, Smart Computing Review vol. 2 no. 1, February 2012.

[4] Biener C., Elig M., Wirfs J. H., *Insurability of Cyber Risk: An Emperical Analysis*, Working Papers on Risk Management and Insurance no. 151, January 2015.

[5] Cacciamani C., *Rischi Puri e Valore di Impresa*, Bagnaria Arsa, Edizioni Goliardiche, 2010.

[6] Cambridge Centre for Risk Studies, *Cyber Exposure Data Schema (v0.9)*, 2016. http://cambridgeriskframework.com/downloads.

[7] CLUSIT, *Rapporto Clusit 2016 sulla Sicurezza ICT in Italia*, Security Summit, 15-17 Marzo 2016.

[8] Daboni L., *Lezioni di tecnica attuariale delle assicurazioni contro i danni*, Lint Editoriale, 1993.

[9] Decreto del presidente del Consiglio dei ministri, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, 24 gennaio 2013. http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.

[10] Ferrara L., *Risk management & control: identificazione, misurazione e gestione del rischio*, Contabilità finanza e controllo: mensile di pratica aziendale, (10), 2000, pp. 1017-1023.

[11] Failure Mode and Effect Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA). http://www.weibull.com/basics/fmea.htm.

[12] Jacobs M., *Risk Analysis: Tying It All Together*. SANS Institute, As part of GIAC practical repository, 2003.

[13] Käärik M., *Non-Life Insurance Mathematics*, Aine maht 6 EAP, Tartu Ülikool, 2013.

[14] Karabacak B., Sogukpinar I., *ISRAM: Information security risk analysis method*, Computer & Security 24: 147-159, 2005.

[15] McFarland C., Paget F., Samani R., *L'economia sommersa dei dati - Il mercato delle informazioni digitali rubate*, McAfee Labs di Intel Security Group, 2015.

[16] National Bureau of Standards, *Guideline for Automatic Data Processing Risk Analysis*, FIPS PUB 65, August 1979. http://www.femtosecond.com/Documents/FIPS65.pdf.

[17] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, v1.0, 12 February 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[18] National Institute of Standards and Technology, *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1, September 2012. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[19] National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST Special Publication 800-122, April 2010. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

[20] National Security Presidential Directives 54/Homeland Security Presidential Directive 23, *Cybersecurity Policy*, 8 January 2008. http://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[21] Organismo Italiano di Contabilità, *Immobilizzazioni Immateriali*, Gennaio 2015. http://www.fondazioneoic.eu/wp-content/uploads/downloads/2015/01/OIC-24-Immobilizzazioni-immateriali.pdf.

[22] Pignolo P., *La Gestione e la Ritenzione del Rischio d'Impresa*, 9, Milano, FrancoAngeli, 2011.

[23] Ponemon Institute, *2016 Cost of Data Breach Study: Global Analysis*, Ponemon Institute Research Report, June 2016.

[24] Ponemon Institute, *2016 Cost of Data Breach Study: Italy*, Ponemon Institute Research Report, June 2016.

[25] Rot A., *IT Risk Assessment: Quantitative and Qualitative Approach*, Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, San Francisco, October 22-24, 2008.

[26] Sistema di informazione per la sicurezza della Repubblica, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, Dicembre 2013. http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf.

[27] Sistema di informazione per la sicurezza della Repubblica, *Piano nazionale per la protezione cibernetica e la sicurezza informatica*, Dicembre 2013. http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/piano-nazionale-cyber_0.pdf.

[28] Sommerville I., *Software Engineering*, Pearson, 9 edition, Mar 2010.

[29] United States Government Accountability Office, *Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, GAO-08-536 Report to Congressional Requesters, May 2008. http://www.gao.gov/new.items/d08536.pdf.

[30] Wüthrich M. V., *Non-Life Insurance: Mathematics & Statistics*, version April 14, 2016.

[31] Yazar Z., *A qualitative risk analysis and management tool – CRAMM*, SANS Institute InfoSec Reading Room, GSEC, Version 1.3, 2002. https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83.

[32] Young V. R., *Premium Principles*, Reproduced from the Encyclopedia of Actuarial Science, John Wiley & Sons Ltd, 2004.

Ringraziamenti

Desidero innanzitutto ringraziare il mio relatore, prof. Danilo Montesi, per avermi condotto in questo progetto e avermi dato ampia fiducia nello svolgimento del lavoro.
Un altro ringraziamento sentito va al dott. Flavio Bertini, correlatore della tesi, per l'incredibile disponibilità e il costante supporto.
Meritano un pensiero speciale tutti quelli che a loro modo hanno portato un proprio contributo nella realizzazione di questa tesi, in particolare il mio caro amico Andrea che mi ha dato energia e utili indicazioni all'inizio di questo progetto.
Questo lavoro va a chiudere due anni speciali, punto di arrivo e di nuovo inizio, nel quale ho avuto modo di conoscere persone eccezionali. Quindi, grazie davvero ai miei compagni di corso soprattutto a Riccardo con cui ho condiviso tutto di questa esperienza, anche questo giorno di laurea.
Senza le persone accanto, che ti ascoltano e ti consigliano, difficilmente avrei centrato gli stessi obiettivi. Per questo voglio ringraziare i miei genitori, per quello che sono e per quello che mi hanno permesso di fare, devo tutto a loro. Un ringraziamento particolare a Linda per avermi incondizionatamente sostenuto, sempre al mio fianco lungo questo cammino.
Grazie a tutti gli amici e alle persone che fanno parte della mia vita.