Effetti dell'implementazione di sistemi di gestione della sicurezza delle informazioni sulla sicurezza informatica aziendale reale e percepita

By

Alessandro Franchi

Supervised by

Prof. Salvatore Fava Ph.D.

A DISSERTATION

Presented to the Department of Business Administration
program at Selinus University

Faculty of Business & Media
in fulfillment of the requirements
for the degree of
Doctor of Philosophy

2020

Con la presente dichiaro di essere l'unico autore di questa tesi e del sottostante progetto di ricerca e che il suo contenuto è solo il risultato delle letture e delle ricerche da me eseguite.

Alessandro Franchi

Sommario

Lista delle abbreviazioni usate

Nel testo sono state utilizzate delle abbreviazioni e delle sigle al fine di semplificare la lettura e l'articolazione della struttura dei paragrafi. Sono state adottate, dove possibile, abbreviazioni accettate dalla maggior parte della letteratura. Di seguito viene mostrato l'elenco.

BPM	Business Process Management
BSC	Balanced Scorecard
CIO	Chief Information Officer
GDPR	General Data Protection Regulation
COBIT	Control Objectives for Information and related Technology
IEC	The International Electrotechnical Commission
IOT	Internet of Things
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	The International Organization for Standardization
ISTAT	Istituto Italiano di Statistica
ICT	Information and Communication Technology
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
SGI	Sistema di Gestione delle Informazioni

Abstract

Lo sviluppo dell'Information Technology è sempre più pervasivo nei processi di business delle aziende moderne. Il ruolo aziendale dell'IT è molto cambiato nel corso di pochi anni, oggi esso non rappresenta più un aspetto meramente tecnico ma diviene, soprattutto, un fattore competitivo, capace di contribuire alla generazione del valore per l'azienda. Questo è vero sia nella situazione in cui vi sia la presenza di una infrastruttura IT interna all'azienda, sia in caso di un contesto in cui essa viene invece considerata una *commodity*, e di conseguenza solitamente esternalizzata attraverso servizi c.d. *cloud*.

Il crescere dei processi di digitalizzazione e dei servizi erogati su piattaforme digitali ha posto all'attenzione di tecnici e manager il problema della sicurezza delle informazioni, concetto da analizzare e gestire attraverso le sue tre dimensioni essenziali di integrità, disponibilità e riservatezza.

La sicurezza, come insieme di tecniche e procedure per la salvaguardia del patrimonio informativo aziendale, rappresenta quindi un fattore strategico che in primis, è di competenza del management.

L'adozione di best practice, di sistemi di gestione dell'IT e l'utilizzo della formazione tecnologica, hanno un ruolo importante su due aspetti importanti del mondo digitale: a) la sicurezza informatica reale, intesa come strutture e processi a difesa delle informazioni e della capacità dell'IT di generare valore, e b) la sicurezza percepita, come consapevolezza.

Nella ricerca si dimostra, a seguito di un'indagine basata su delle analisi qualitative, l'esistenza di legami che, a seguito dell'implementazione di sistemi di gestione e best practice, hanno un effetto positivo sia sulla sicurezza IT reale, sia su quella percepita dal management dell'azienda.

1 Introduzione

1.1 Obiettivo della ricerca

L'obiettivo della presente ricerca è di valutare l'effetto sulla sicurezza IT, reale e percepita, dell'introduzione in azienda di sistemi di gestione della sicurezza delle informazioni, di altre best practice gestionali orientate al governo dei sistemi informativi o dell'organizzazione, sulla sicurezza informatica.

Si è scelto di considerare, tra i sistemi di cui vuole valutare l'effetto dell'introduzione in azienda, quelli più diffusi e riconosciuti per il loro impatto sul ciclo della sicurezza informativa aziendale, in particolare:

a) l'implementazione della norma ISO 27001;
b) l'adozione di best practice COBIT;
c) l'adozione di best practice ITIL;
d) la valutazione e la governance dei processi di sicurezza IT tramite metodologie associabili al modello della Balanced Scorecard;
e) le misure organizzate di formazione in ambito IT, erogate agli utilizzatori finali.

Nell'ambito del presente lavoro, la sicurezza informatica viene scomposta in due dimensioni di analisi, quella che nell'ambito di questa ricerca viene chiamata *sicurezza informatica percepita*, ovvero quella che viene indotta dal presupposto dell'avere adottato un impianto di regole o di best practice formalmente in uso e quella che viene chiamata *sicurezza informatica reale*, associata a indicatori oggettivi del livello di sicurezza IT, impostati in azienda e derivanti in questo caso prevalentemente da metriche tecnologiche.

1.2 Background

Già negli anni Ottanta veniva riconosciuto dalla letteratura il notevole impatto dei sistemi informativi in azienda e il conseguente potenziale di trasformazione dirompente sul business; veniva inoltre identificato il venire meno della vecchia concezione della struttura IT come semplice attore del data processing e si cercava di descrivere l'impatto di queste tecnologie sulla struttura organizzativa, sul personale e sullo sviluppo tecnologico (Lee, 1988). Inoltre, nel saggio di Norman (1995) relativo agli *artefatti cognitivi* (Capitolo 2.2) già si prospettava un'era di forte espansione informativa nonché il potenziale proliferare di informazioni in quantità tale da essere di difficile gestione, spesso di dubbia qualità e di scarsa rilevanza. In tal senso si prevedeva, inoltre, la necessità di *agenti intelligenti*, addetti alla selezione e gestione della sovrabbondanza informativa; questi agenti sono descritti anche nel lavoro di Negroponte (1996) e oggi, dopo oltre vent'anni, è abbastanza facile assimilarli ai già noti sistemi di intelligenza artificiale c.d. *debole*. Occorre rilevare che le prospettive di evoluzione di aziende digitali, telelavoro, outsourcing digitale (es. Demaire & Hitt, 2000) erano evidenti sia a livello tecnologico sia a livello sociale e organizzativo, ed erano inoltre chiare le implicazioni manageriali dell'Information Technology in ordine alle trasformazioni che oggi chiamiamo *digitalizzazione*. Già Segars e Hendrickson (2000) identificavano per le aziende efficienti il requisito di avere un allineamento della *core value proposition* della funzione IT con quella dell'azienda. Con lo sviluppo dell'Information Technology, la corsa alla digitalizzazione ha poi portato a una crescita esponenziale nella generazione e nell'uso di dati; già nel 2012 venivano generati nell'arco di in un giorno una mole di dati superiore a quanti ce ne fossero sull'intera rete Internet vent'anni prima (McAfee & Brynjolfsson, 2012) con un tasso di crescita stimato che prevedeva il raddoppio ogni 40 mesi.

Negli anni Novanta, con lo sviluppo della rete Internet comincia a emergere anche il potenziale dirompente delle tecnologie web sui modelli di business (es. Franchi, 1997; Negroponte, 1996); il quadro era quindi completo, con il potenziale delle tecnologie IT in continuo sviluppo e disponibile a chiunque attraverso le reti di telecomunicazioni.

Ciò che non è stato invece chiaro ed evidente fin da subito erano i possibili scenari delle implicazioni legate alla sicurezza del mondo digitale o perlomeno alla mancanza di una attenta valutazione di tutte le dimensioni che la riguardano: integrità, continuità e riservatezza. L'evoluzione dell'*e-commerce* ha ulteriormente sottolineato l'esigenza di un approccio integrato alla sicurezza IT (Dutta & McCrohan, 2002). La connotazione criminale dello sfruttamento delle carenze esistenti nelle varie aree della sicurezza informatica ha trasformato anche nel mondo del crimine le informazioni in merce di scambio, generando interessi economici legali e illegali attraverso il traffico di informazioni, attraverso la possibilità di danneggiare la concorrenza e con i benefici derivanti da altri infiniti tipi di reati, dal furto di identità, furto di dati e ricatti, per fare degli esempi.
Un'ulteriore fonte di espansione dei rischi per i dati digitali è legata alla progressiva diffusione di apparati, e non più solo computer, anch'essi collegati in rete, il c.d. modo della *Internet of Things* (IOT) che amplifica ulteriormente il problema della sicurezza IT e della privacy (es. Corradini, 2017), col risultato di moltiplicare gli effetti del *cyber crime* e della mancanza di sicurezza IT, come espresso anche in Basin e Capkun (2012).

Per definire quindi il background della ricerca, occorre focalizzare i seguenti punti:

a) L'Information Technology è oggi fondamentale e parte integrante del business, (Cap. 2.1, 2.2, 2.3), non solo in senso tecnologico ma anche in senso organizzativo e di *value generation*, costituisce inoltre un vantaggio competitivo per il business.
b) La sicurezza IT, di conseguenza, è un fattore di estrema importanza per il business (Cap. 2.4) e, come accaduto per le tecnologie IT stesse, non può essere più solo un problema tecnico ma rappresenta soprattutto un problema di gestione manageriale. La sicurezza, come ormai generalmente accettato, è un processo continuo.
c) Esistono numerosi sistemi di gestione e di best practice (Cap. 2.5, 2.6, 2.7, 2.8, 2.9) che si curano anche della sicurezza IT negli aspetti tecnologici, manageriali e sociali.

d) Le aziende adottano, o non adottano, diversi di questi sistemi e metodologie per favorire la sicurezza, e lo fanno anche in modalità diverse da realtà a realtà, con diverso spessore e profondità tecnologica o organizzativa.

1.3 Significatività dello studio

La gestione della sicurezza IT secondo paradigmi moderni e completi è arrivata in ritardo rispetto a quanto riesce a esprimere l'evoluzione tecnologica. Inoltre, solo in seguito allo sviluppo delle reti e delle tecnologie web e la conseguente nascita delle problematiche associate all*'hacking*, la sicurezza è stata interpretata in tutti e tre i pilastri che la definiscono. Un aspetto da considerare, infatti, è che, inizialmente, la sicurezza IT è stata vista solo come un problema da affrontare con il supporto tecnologico, e solo in seguito è stato integrata la dimensione umana con gli studi sul *social engineering* e sugli aspetti psicologici e comportamentali. Mentre da un lato si sono evoluti ed evolvono diversi sistemi tecnologici di protezione, dall'altro non esistono approcci organizzativi unici e completamente sicuri. Tra le best practice disponibili ci sono diverse opzioni, diversamente implementabili e potenzialmente criticabili.

Nell'ottica di avere in un prossimo futuro aziende sempre più sicure *by design*, occorre comprendere la sicurezza IT non solo da un punto di vista meramente tecnologico ma è necessario integrarla con una visione manageriale dotata di due aspetti che sono:

a) come queste metodologie, sistemi e best practice impattano sulla sicurezza reale, se hanno aspetti di comunanza e intercambiabilità, e la valutazione del loro livello di efficienza sistemica complessiva;
b) come questi sistemi impattano, a livello di percezione, sull'attitudine del management verso la sicurezza IT. La questione non è da poco in termini sociologici, possiamo infatti riassumerla con l'esempio semplificatore seguente: se *mi sento più sicuro alla guida di un'auto che reputo sicura perché questa è una delle caratteristiche riconosciute del brand, sono maggiormente al sicuro da incidenti d'auto*?

1.4 Presupposti e limiti

Il presupposto sottostante allo studio è che le tecnologie legate all'Information Technology e utilizzate a supporto dei processi di business sono trasversali su diverse dimensioni di analisi, quali ad esempio i settori dove operano le imprese e la loro distribuzione geografica. Come emerge dall'analisi della letteratura (Capitolo 2) questi presupposti sono validati grazie alla crescente globalizzazione sia delle imprese sia delle tecnologie informatiche, nonché da un processo di standardizzazione e commoditizzazione del settore ICT grazie a fattori come:

a) sviluppo delle tecnologie del web e diffusione capillare delle connessioni Internet a banda larga e delle connessioni di tipo mobile;
b) orientamento progressivo delle applicazioni verso l'adozione di piattaforme e tecnologie di tipo web;
c) progressivo outsourcing dell'IT delle aziende verso soluzioni cloud.

Uno dei limiti individuabili nella ricerca è legato alla composizione del campione di aziende coinvolte che è legato prevalentemente ad aziende Italiane con una presenza attiva sul web. Si può parzialmente rispondere a questi limiti considerando alcuni aspetti:

a) il campione su cui si è lavorato è sufficientemente descrittivo della popolazione avendo un confronto molto simile a quanto presentato dalle statistiche nazionali dell'Istituto Italiano di Statistica;
b) la diffusione delle tecnologie IT ha omogeneità in molta parte del monto industrializzato, si veda ad es. Jorgenson and Vu (2016) oppure Ciriani and Perin (2017).

Una ulteriore limitazione può essere individuata nello strumento del questionario che, per ragioni legate alla gestione di dati di tipo personale e riservato e per evitare problematiche relativa alla normativa (GDPR) è stato condotto in forma anonima. Sulla somministrazione del questionario si è

fatta attenzione a usare canali specifici (Capitolo 3) e, relativamente ai risultati, si è posta comunque assoluta attenzione nella verifica della congruità dell'impianto della risposta.

1.5 Risultati attesi

I risultati attesi da questa ricerca sono collegati alle *Research Question* espresse nel Cap. 3.6.1 e riassunte poi dalle conseguenti ipotesi del Cap. 3.6.2. L'obiettivo è di dimostrare l'esistenza di un legame tra l'adozione di un sistema di gestione della sicurezza IT e/o delle best practice in qualche modo collegate alla gestione del patrimonio informativo aziendale, e l'eventuale senso di consapevolezza relativamente alla sicurezza della struttura informatica dell'azienda.

Relativamente all'adozione delle stesse metodologie ci si aspetta anche un impatto più reale e oggettivo, in particolare risultante in un minore numero di incidenti in questa area, ad esempio.

L'altro set di risultati attesi riguarda l'esistenza di un legame tra le ore di formazione erogate in ambito Information Technology e le stesse due dimensioni prima evidenziate, la percezione della sicurezza, indagata sul personale manageriale, e il legame inverso con il numero di incidenti collegabili all'Information Technology.

2 Analisi della letteratura

2.1 Introduzione

L'informatica, le sue teorie e i suoi strumenti tecnologici hanno un ruolo estremamente pervasivo in azienda e, nelle realtà modernamente organizzate, essa fornisce un supporto indispensabile alla gestione dei processi di business. Gli aspetti legati all'allineamento della struttura informativa al business aziendale, alla sicurezza delle informazioni aziendali, e alle strategie di governance delle infrastrutture tecnologiche, non sono più dei meri aspetti tecnici ma sono diventati a tutti gli effetti dei fattori strategici e, come tali, devono essere di competenza del management (es. Reynolds & Yetton, 2015). Quello cui si è assistito con l'evoluzione dell'Information Technology, infatti, è un cambio di paradigma per quanto concerne i sistemi informativi aziendali, che perdono di importanza come fattore di tipo esclusivamente tecnologico e rappresentano sempre più:

a) dei sistemi a supporto dei processi aziendali,
b) una struttura di controllo della sicurezza del patrimonio aziendale, e
c) una parte significativa delle leve aziendali che contribuiscono alla generazione del valore.

Questi aspetti sono evidenziati, ad esempio, in De Haes et al. (2013) e in Van Grembergen et De Haes (2009). L'analisi della letteratura segue il filo logico necessario alla comprensione del flusso della ricerca. Vengono innanzitutto analizzati alcuni aspetti formali della scienza informatica in generale, in particolare quei riferimenti che legano la concezione di artefatto cognitivo, utile al potenziamento delle capacità intellettive umane (Norman, 1995), con gli strumenti offerti dall'IT; segue una classificazione delle strutture dati attraverso il modello DIKW e la formalizzazione degli aspetti legati al valore e alla trasformazione delle informazioni. Segue un'analisi sugli aspetti di sicurezza informatica che saranno alla base delle quattro ipotesi di ricerca oggetto di valutazione.

Sono poi valutati quei sistemi di gestione, best practice e attività coinvolti nella ricerca come fattori correlati alla sicurezza informativa aziendale e la sua percezione.

2.2 Informatica come artefatto cognitivo

Secondo Norman (1995), l'uomo nella sua recente evoluzione non ha conosciuto né un particolare incremento della forza fisica, né un significativo incremento della sua intelligenza intrinseca, intesa come capacità intellettiva propria. A cosa si deve dunque collegare l'enorme sviluppo dell'umanità, nel percorso che l'ha portata dalle caverne alla costruzione dei grattacieli e da un linguaggio di rumori alle equazioni differenziali? L'uomo ha potenziato la sua *forza* attraverso degli strumenti, ad esempio attraverso una leva, un martello, la ruota e le macchine di varia natura che ha costruito e sviluppato. L'uomo riesce oggi a produrre e governare quantità enormi di energia e di forza motrice, spostando navi da migliaia di tonnellate o razzi interplanetari. Lo stesso paragone può essere fatto, oltre che per la forza, anche per l'*intelligenza*. L'uomo ha potenziato la sua intelligenza allo stesso modo di come ha saputo potenziare la sua forza fisica, attraverso cioè la realizzazione e l'utilizzo di strumenti atti a potenziare la sua intelligenza intrinseca. Norman (1995) chiama questi strumenti *artefatti cognitivi*. Se da un lato però vengono inventati strumenti che potenziano la nostra intelligenza, dall'altro il rischio è che la tecnologia usata per la creazione di questi artefatti possa essere superiore alla capacità di comprensione che si può avere di essi (Norman, 1995), questo è uno dei rischi, peraltro sempre più evidenti, che emergono con l'utilizzo delle c.d. *intelligenze artificiali* che si stanno affermando oggi sulla scena tecnologica.

Due esempi di artefatto cognitivo di eccezionale portata e che hanno caratterizzato in passato momenti importanti legati all'evoluzione dell'intelligenza umana, e che spesso non appaiono così evidenti sono, ad esempio, la scrittura e il calcolo.

La scrittura, in particolare quella basata su un alfabeto come nel caso dei greci e dei latini, ha permesso la memorizzazione e la trasmissione precisa di nozioni e concetti che in precedenza potevano essere tramandati in maniera imperfetta solo in forma orale, con tutti i problemi collegati

alla memoria limitata degli usseri umani e agli errori distorsivi legati al fatto di tramandare una nozione in forma orale. La scrittura ha permesso di codificare e trasferire in maniera precisa nozioni, istruzioni, racconti, il diritto, e poi la filosofia, la storia, i principi delle scienze e i dettagli delle varie scoperte scientifiche. Per una cultura basata su una tradizione orale tutto questo è invece sostanzialmente impossibile. L'uso di parole astratte, slegate da una raffigurazione pittografica come potevano essere le forme di scrittura non alfabetiche, ha permesso lo sviluppo di concetti evoluti, complessi e trasmissibili con estrema precisione. Con l'uso di scritture alfabetiche, o in generale forme simboliche specifiche, se includiamo nel concetto di scrittura anche uno spartito musicale, un'equazione, o il codice di un software, si arriva a una rappresentazione concisa e specifica del concetto.

Il calcolo, in particolare quello basato sui sistemi di numerazione posizionale, come quello di derivazione c.d. araba, ha permesso il potenziamento delle capacità di elaborazione del cervello umano. I sistemi di numerazione non posizionali sono in parte legati a una forma di conteggio primitiva, con la necessità di creare nuovi simboli al crescere del numero rappresentato, si pensi ad esempio ai numeri romani. I sistemi posizionali, che abbiano dieci simboli oppure due o sedici come accade nell'informatica, permettono la rappresentazione di quantità infinitamente grandi o piccole con un numero limitato di cifre differenti e, una volta apprese le regole, consentono una notevole semplificazione del calcolo matematico.

Proseguendo nella disamina dei sistemi atti a potenziare le capacità intellettive, ovvero gli artefatti cognitivi secondo Norman (1995), possiamo inquadrare le stesse tecnologie dell'informazione come dei sistemi di artefatti cognitivi a supporto della nostra intelligenza e del nostro sviluppo. Una ulteriore ragione per cui si pone, in questo studio, l'accento sul modello degli artefatti cognitivi sta nel fatto che i modelli di best practice che verranno affrontati nel seguito del capitolo due, uniti agli standard di gestione della qualità e dei processi, sono a tutti gli effetti degli artefatti culturali (es. Iden & Eikebrokk, 2014), che rappresentano quindi strumenti al servizio dell'obiettivo del potenziamento delle capacità intrinseche della mente umana.

2.3 Il ruolo strategico di dati e informazioni in azienda.

Secondo la visione proposta dalla microeconomia, l'azienda viene rappresentata come una *black-box* dotata di fattori di input e di output. Il legame tra questi fattori può essere descritto attraverso dei modelli matematici, come ad esempio le funzioni di produzione (es. Varian, 1992). In aggiunta alle dottrine classiche e considerando aspetti strategici e gestionali del governo dell'azienda, occorre considerare che i legami che sono stati prospettati tra fattori di input e di output, sono influenzati anche da una molteplicità di forze interne ed esterne all'azienda, come ad esempio evidenziato nel modello competitivo delle cinque forze di Porter (Porter, 2008). Ciò che emerge da queste teorie, in ogni caso, è che il governo d'azienda non può prescindere da aspetti quantitativi, ne consegue pertanto che il management si trova nella necessità di avere dei modelli di analisi e di simulazione della realtà basati su informazioni la cui complessità è progressivamente crescente. Se in passato veniva considerato sufficiente, ai fini della gestione e della comprensione dell'azienda, il c.d. modello della contabilità generale, che confluiva nel bilancio aziendale composto di conto economico e stato patrimoniale, oggi ciò non è più sufficiente. Quello che serve, in un contesto di incertezza e dinamica crescenti dell'ambiente competitivo, è modellare i processi con tutte le informazioni rilevanti, in termini gestionali, disponibili all'interno e all'esterno dell'azienda. Come affermato da Kaplan e Norton (2004) "Non si può gestire ciò che non si può misurare". Ecco quindi che gli strumenti per la gestione delle informazioni aziendali e della loro sicurezza sono degli elementi strategici, un potenziale vantaggio competitivo e, comunque, un problema che in primis è di pertinenza del management dell'azienda e, a scendere, dei tecnici incaricati della loro gestione.

In ambito scientifico, così come pure gestionale o personale, l'analisi dei dati può essere definita come un insieme di procedimenti, trasformazioni, e modellizzazioni degli stessi che permettono di arrivare all'evidenziazione di informazioni utilizzabili per dedurre conclusioni utili al supporto alle decisioni, di qualsiasi tipo esse siano. In generale quindi si applicano *funzioni* sui dati per arrivare a delle informazioni utili per prendere decisioni aziendali. Formalmente:

$$f\colon D \to C \text{ con } f(x) = y, \text{ dove } x \in D \text{ e } y \in C$$

L'insieme D, il dominio della funzione, è l'insieme dei dati noti in azienda sulla base dei quali arrivare a una decisione / azione, che sarà inclusa nell'insieme del codominio C della funzione *f*. Per il nostro ambito di studio si noti che D è l'insieme dei dati che sono noti in azienda, un insieme che potrebbe essere anche incompleto, come accade in un mercato imperfetto, e pertanto, il dominio D è un sottoinsieme del reale dominio esteso U della funzione, che consiste dell'insieme di tutti i dati possibili, anche non noti all'azienda, per il quale la funzione possa essere calcolabile.

$$D \subseteq U$$

Infine, la funzione *f*, la regola di trasformazione, non necessariamente deve essere una funzione biiettiva, sia che si intenda come dominio l'insieme D sia che si intenda il dominio esteso U. Potrebbe pertanto accadere che a partire da due dati diversi si possa giungere alla stessa decisione, oppure potrebbe ugualmente accadere che integrando l'insieme D con i dati mancanti, presenti invece in U, ugualmente le informazioni e le eventuali decisioni non cambino.

La questione non è di poco conto in quanto il processo computazionale, nella vita reale, ha un costo e non è utile elaborare un maggior numero di dati senza aggiungere informazioni al nostro bagaglio informativo C. Si rende opportuno quindi minimizzare l'insieme D, riducendolo a quanto di utile è in grado di generare in termini di conoscenza informativa. In un mondo dove si genera spesso una sovrapproduzione di informazioni diventa questa una condizione essenziale. Si può comprendere che in realtà la funzione *f* ha un numero potenzialmente elevato di parametri, formalmente:

$$f\colon D^n \rightarrow C \text{ con } f(x_1, x_2, x_3, \ldots x_n) = y$$

e, per quanto affermato sul fatto che la funzione non sia necessariamente biiettiva, se ad esempio:

$$f(x_1, x_{2a}, x_3, \ldots x_n) = f(x_1, x_{2b}, x_3, \ldots x_n) = y$$

allora uno tra i dati x_{2a} e x_{2b} non aggiunge nulla al nostro patrimonio informativo.

Caratterizziamo ulteriormente i dati di D^n. Alcuni dei dati sono certi, mentre altri dati potrebbero essere invece aleatori, come quando ad esempio occorre valutare *rischi* o eventi non certi. Tale

aleatorietà potrebbe verificarsi con diversi livelli di *probabilità* e in questo caso i modelli informativi dell'azienda devono integrare funzioni di probabilità, uni o multivariata, attingendo modelli e strumenti dal mondo della statistica. Da queste considerazioni originano logiche di simulazione e di governo dell'azienda, perlomeno quelle basate su dati e informazioni.

Per arrivare infine ai modelli di sicurezza e governance delle informazioni, occorre una comprensione della gerarchia di alcuni termini come *dato* e *informazione*, usati a volte erroneamente come sinonimi. A questo scopo ci viene in aiuto un modello gerarchico, il modello DIKW, che esprime la relazione tra i concetti di Dati, Informazioni, Knowledge (Conoscenza) e Wisdom (Saggezza). Il modello, rappresentato nella figura 2.3.1, è una piramide dove si passa progressivamente dal livello dei segnali, ai dati e alle informazioni, con una crescente attribuzione di valore aggiunto e con una strutturazione che richiede trasformazioni sempre meno algoritmiche. L'evoluzione passa dal mondo della gestione dei segnali, tipicamente dominio dell'elettronica, al mondo dell'Information Technology, fino a un livello di competenza che, per ora, è riservato agli umani. L'ambito tra *Knowledge* e *Wisdom* è il confine in cui iniziano ad operare molte delle tecniche di c.d. *intelligenza artificiale debole*, tutte tecniche basate comunque su algoritmi software e programmazione, il che pone queste tecniche, per la tesi di Church, al massimo equipotenti al modello computazione di Turing, in questo senso, quindi, si parla di Intelligenze Artificiali Deboli.

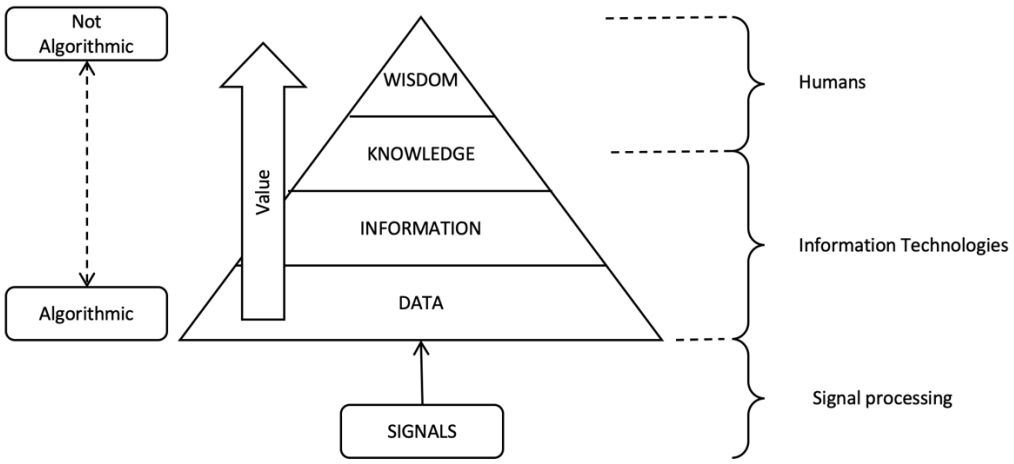

Fig. 2.3.1 – modello DIKW (Adattato da Rowley, 2007)

Le definizioni più frequentemente usate per il modello DIKW, sono, in breve, quelle che possiamo ritrovare ad esempio anche in Rowley (2007), in Pearlson and Saunders (2010) o in Franchi (2017) ovvero:

- *Data* – Una rappresentazione dell'osservazione delle proprietà di un oggetto, di un evento o del loro ambiente.
- *Information* – consiste di dati elaborati ed in grado di fornire risposte a una serie di domande del tipo: chi, cosa, quando, dove, nonché di prendere decisioni.
- *Knowledge* – Permette la trasformazione di informazioni in istruzioni.
- *Wisdom* – Abilità di incrementare l'efficienza. Questo punto, per altro, è la chiave per lo sviluppo delle cosiddette *efficienze adattive* in uso in alcune delle tecniche di intelligenza artificiale.

I sistemi informatici generano, memorizzano e processano dati (Rowley, 2007). L'integrazione dei dati con un modello di analisi, assieme all'attribuzione di uno specifico valore semantico, generano l'informazione necessaria per investigare un comportamento del modello. L'aggiunta di un sistema di feedback significativo, anche parzialmente automatizzato attraverso degli strumenti informatici, genera un primo livello di conoscenza che è capace di indirizzare eventuali problemi evidenziati dal modello.

Per avere una relazione DIKW efficace e in grado di supportare la costruzione di sistemi di analisi appropriati e in grado di generare valore, i dati devono avere alcune caratteristiche. Molte di queste caratteristiche possono essere dedotte, per avere qualche esempio, riferendosi ai lavori di Pearlson and Saunders (2010) o riferendosi a quanto espresso in IRM Association (2011).

In primis i segnali che generano i dati devono essere misurabili ovvero devono costantemente produrre dati coerenti, significativi e corretti. Per quanto condivisibile anche a prima vista, la questione non è ovvia.

Occorre poi arrivare a dei dati con specifiche caratteristiche in termini di disponibilità. Gli attributi di seguito proposti, ad esempio, emergono in Lancaster (2005) e IRM Association (2011). Gli autori identificano tre criteri di base per avere dati efficaci riferendosi a validità, affidabilità e generalizzabilità; inoltre, da un punto di vista più informatico, altri criteri di appropriatezza sono:

- *Timing* – Disponibilità al momento giusto e per i tempi necessari. Non ha senso dover attendere ore per avere la disponibilità di un dato, ad esempio, quando un'azione di feedback deve essere invece presa nel giro di pochi minuti.
- *Formato* – Il formato dati proveniente dai vari sistemi deve essere identificato e rimanere costante o almeno interpretabile, per evitare errori di interpretazione semantica.
- *Correttezza* – I dati devono essere corretti e caratterizzati da un intervallo d'errore conosciuto e, soprattutto, gestito.
- *Frequenza e granularità* – Un sistema di rilevamento, ad esempio, può rilevare i dati ogni secondo, ogni minuto oppure ogni ora, e lo può fare in un unico punto o una molteplicità di punti, in funzione del tipo di feedback richiesto dal processo che vogliamo controllare.
- *Numero appropriato di dimensioni* che caratterizzano il dato – Se una serie di dati è espressa lungo una o più di dimensioni di analisi, confronti tra dati possono essere fatti solo relativamente al minimo numero di dimensioni comuni.
- *Comparabilità* – ad esempio adottando le stesse unità di misura.
- *Significatività* – I dati devono generare informazioni che siano rilevanti per il processo. La questione sembra banale ma non lo è. Le informazioni costano, occorre determinare un set informativo minimo in grado di descrivere appropriatamente il processo evitando l'utilizzo di informazioni inutili o ridondanti.
- *Costo appropriato* – Ottenere dati e informazioni è un processo costoso, come prima menzionato, sia in termini di tempo sia in termini di risorse economiche. Il beneficio che si ottiene dall'analisi deve giustificare il costo per generarla.

Dati e loro trasformazioni diventano gli elementi per il supporto delle decisioni dell'azienda, la loro sicurezza, secondo le classiche tre dimensioni di integrità, continuità e riservatezza (Tsiouras, 2004) diventa quindi compito del management, che deve garantire e ottimizzare opportunamente il valore che ne deriva.

2.4 La sicurezza informatica

Nelle economie digitali, dati e informazioni sono parte dei fattori produttivi dell'azienda e concorrono alla costruzione del suo vantaggio competitivo (Cap. 2.3). La loro gestione, la protezione e l'allineamento della struttura che li governa con la strategia dell'azienda è un importante compito del management aziendale, attraverso policy e strumenti per la sicurezza informatica. I processi relativi alla sicurezza informatica si occupano, sotto gli aspetti che verranno descritti in seguito, della tutela del patrimonio informativo dell'azienda. La sicurezza informatica viene declinata nei suoi tre principali aspetti che sono: integrità, continuità e riservatezza (es. Tsiouras, 2004).

2.4.1 Integrità, continuità e riservatezza

Le prime riflessioni che vengono associate alla sicurezza informatica evocano quel genere di eventi contraddistinti da maggiore notorietà mediatica come *data-breach*, virus, hacker, e violazione di sistemi informatici. La sicurezza viene in realtà suddivisa in tre aree con problematiche specifiche:

Integrità – Riguarda l'inalterabilità del dato nel tempo, i sistemi hardware e software alla base della gestione dei dati devono rispondere, a parità di richiesta, sempre allo stesso modo, il dato non può "deteriorarsi" nel tempo. Mancanza di integrità può aversi, ad esempio, come conseguenza di un guasto hardware o software, di un errore umano, o anche a causa di una violazione di terzi.

Continuità – Riguarda la caratteristica che il dato sia sempre presente a fronte di una richiesta da parte di chi ne ha diritto di accesso, l'indisponibilità può essere conseguente a un guasto sul sistema

di memorizzazione che lo conserva, un guasto sul sistema di comunicazione o a un errore di procedura che lo ha reso indisponibile, ad esempio una cancellazione involontaria, e anche da una violazione di terzi.

Riservatezza – Riguarda la certezza che il dato sia accessibile nel tempo, e quindi in maniera integra e continua, solo alle persone autorizzate a consultarlo. Il principio, illustrato in seguito, è quello della minimizzazione del perimetro di accesso alle informazioni.

La minimizzazione dei problemi di sicurezza su queste tre aree riguardano sia aspetti tecnici sia aspetti procedurali, e quindi aspetti legati ad hardware e software da un lato e aspetti legati al fattore umano dall'altro. Con lo sviluppo della tecnologia, i sistemi hardware e software rappresentano elementi di crescente garanzia qualitativa nei confronti della sicurezza dei dati, pur con la consapevolezza che la crescente complessità dei sistemi rende sempre meno facile eliminare vulnerabilità di tipo tecnologico dagli stessi (Mansir & Morin, 2018). Sempre relativamente all'hardware, occorre rilevare che il crescente livello di connessione tra il mondo IT e il mondo reale, grazie alla pervasività delle tecnologie informatiche, come le tecnologie IOT o i sistemi industriali con tecnologie c.d. 4.0, non farà altro che aumentare il numero e la portata degli attacchi informatici (Basin & Capkun, 2012).

La minaccia alla sicurezza dei dati più difficile da controllare riguarda invece il fattore umano, riconosciuto come l'anello debole della catena della sicurezza IT (Hadnagy, 2011). Il fattore umano, come fonte di pericolo per la sicurezza IT, è legato a diversi aspetti spesso poco controllabili da sistemi di sicurezza hardware e software: ad esempio la disattenzione, la carenza di formazione e tutto l'insieme psicologico di fonti di attacco che vanno sotto il nome di tecniche di *social engineering*.

Mentre gli investimenti in tecnologia, sia in ambito software e sia in ambito hardware, contribuiscono alla riduzione dei rischi IT dal punto di vista tecnologico, per ridurre i rischi legati al fattore umano si ricorre a diverse tecniche:

a) la formazione;
b) la minimizzazione del perimetro informativo accessibile da un utente, tecnica conosciuta anche come principio del *need to know*, ovvero il permettere all'utente l'accesso solo ed esclusivamente alle informazioni minime indispensabili necessarie per svolgere le proprie attività;
c) utilizzo di procedure, regolamenti, adozione di best practice e sistemi di sorveglianza delle attività utente.

L'applicazione di standard e di procedure di sicurezza è ampiamento usato ma ne vengono anche sottolineati alcuni aspetti limitativi (Siponen, 2006) legati al fatto che spesso la focalizzazione degli enti che le adottano è più sull'esistenza stessa dei processi piuttosto che sul reale perseguimento dei risultati.

Da alcune ricerche (es. Khallaf & Majdalawic, 2012) emerge che le performance in IT security sono anche correlate alla presenza in azienda di CIO e manager di area IT con maggiore esperienza e con significative competenze tecniche; se da un lato questo pone in luce il ruolo tecnologico associato alla sicurezza IT, dall'altro occorre ricordare il ruolo trasversale dell'IT sui processi aziendali e pertanto la sicurezza IT non può che essere prima di tutto un problema aziendale, pur se di pertinenza dell'area tecnologica (Peppard, 2007).

La misurazione dell'efficacia degli investimenti in sicurezza IT non è ancora una metodologia consolidata (Cavusoglu, Mishra, and Raghunathan, 2004) ma è diventata oggetto di discussioni, anche controverse, legate allo sviluppo *dell'e-commerce* e comunque alla difficoltà generica di valutazione degli investimenti IT stessi. In sostanza si riconosce la difficoltà nella valutazione e la mancanza di un modello generale, legato secondo alcuni alla mancanza del legame, ad esempio, tra spese in sicurezza IT e profittabilità aziendale (Dutta & McCrohan, 2002).

L'obiettivo della presente ricerca va anche nella direzione di creare alcune condizioni affinché possano essere definiti dei modelli di valutazione sugli investimenti in sicurezza IT, validi sia sotto l'aspetto tecnologico sia, soprattutto, dal punto di vista gestionale.

La misurazione del rischio IT è il cuore di della gestione del rischio in ambito IT (Goble & Bier, 2013), attraverso delle procedure di *risk assessment* che sono tipiche di molte delle best practice oggetto di questa ricerca. Il rischio va quindi identificato, classificato e misurato come premessa della sua gestione.

Si noti che la definizione stessa di rischio implica la non annullabilità dello stesso essendo associato a un concetto di probabilità; occorre pertanto valutare, come avviene ad esempio nella norma ISO27001, se il rischio sia accettabile o meno e, in quest'ultimo caso, identificare le misure per ridurne l'impatto e cercare di renderlo accettabile. L'importanza dei *risk assessment* sta nella loro essenza di report a supporto delle decisioni (Goble & Bier, 2013), passano, come visto, attraverso tre fasi tipiche: a) identificazione del rischio, b) quantificazione e, c) valutazione (es. Charette, 1996), mentre i sistemi di gestione della sicurezza IT passano attraverso le tre fasi di: a) prevenzione, b) scoperta, e c) risposta (Cavusoglu, Mishra, and Raghunathan, 2005).

Infine, occorre considerare un livello ulteriore della dimensione del rischio IT, specialmente alla luce dell'attuale elevata interconnessione di rete tra aziende, fornitori di servizi tecnologici e utilizzatori, identificando un livello di infrastrutture critiche (Warfield, 2012) che vanno protette adeguandole a livelli più accettabili di rischio IT. Questo può essere necessario anche a un eventuale livello sistemico, a supporto dell'economia digitale.

2.5 I sistemi di gestione, il modello ISO 27001.

Lo standard ISO/IEC 27001 definisce i requisiti per costruire un sistema di gestione della sicurezza delle informazioni (ISMS); include diversi aspetti della sicurezza: fisica, logica, e organizzativa. Fa parte di una famiglia di norme più ampia, che spaziano dall'implementazione dei controlli di sicurezza alle tecniche di gestione dei rischi (ISO, 2020). Per alcuni aspetti le logiche di implementazione delle norme della famiglia ISO 27000 richiedono anche dei riferimenti alle norme ISO 31000, relativi alla gestione (generale) del rischio, e alla norma ISO22301, relativa alla continuità operativa di business. Si è scelto di analizzare la certificazione ISO 27001 in ragione della sua capacità di trasformarsi in uno strumento organizzativo, di governance e operativo, restituendo nel contempo una visione reale della sicurezza IT.

Un ISMS è un approccio sistematico per gestire le informazioni sensibili di una azienda al fine di mantenerle sicure. Il sistema applica processi di gestione a persone, processi, e a sistemi tecnologici, e può essere realizzato su imprese di qualsiasi dimensione (ISO, 2020). Ci sono diverse ragioni per adottare un ISMS (es. Calder, 2018), ad esempio ragioni a) Strategiche, per *compliance* governativa o per ragioni strategiche legate alla gestione delle informazioni aziendali; b) ragioni utili ai rapporti con clienti e fornitori; c) controllo dell'utilizzo delle risorse IT aziendali; d) efficienza nella gestione organizzativa.

Il processo di implementazione del sistema di gestione basato sulla norma ISO 27001 è rigoroso e il sistema implementato richiede la redazione di documentazione, organizzativa ed operativa, che si occupa delle procedure di controllo e di audit, degli aspetti di leadership, del sistema di presentazione, delle procedure di management, delle procedure di sistema, delle procedure di supporto e procedure di gestione del rischio.

Dal punto di vista della pura gestione dell'IT aziendale, i vantaggi della certificazione risiedono nella possibilità di uniformarsi a sistemi di lavoro rigorosi, che permettono una gestione organizzata del rischio IT e prevedono un audit di allineamento periodico con lo standard (Calder, 2018).

La certificazione ISO 27001 non ha a oggi una diffusione molto elevata tra le aziende per diverse ragioni:

a) il processo di certificazione richiede dei prerequisiti importanti in termini di apparati, di organizzazione della struttura IT e di procedure di controllo sui flussi di informazioni;
b) il processo di certificazione richiede uno sforzo continuo della struttura IT dell'azienda e un adeguamento a procedure e regole non sempre presenti;
c) il mantenimento della certificazione, basato su periodi triennali con sorveglianze annuali, richiede un impegno costante che non tutte le organizzazioni possono permettersi.

ISO 27001 – Conclusioni

A oggi il principale ente accreditatore italiano, Accredia, ha nella sua banca dati 2402 certificati ISO 27001 (Accredia, 2020); pur non avendo quindi una diffusione elevata a causa dei requisiti e dell'impegno per la sua implementazione, questa certificazione rappresenta un sistema completo per la garanzia della sicurezza delle informazioni. Abbraccia aspetti tecnici, organizzativi e formativi, impostando logiche e metodologie di lavoro efficaci.

2.6 Best practice – ITIL

ITIL, acronimo di *Information Technology Infrastructure Library*, consiste di un insieme di linee guida dedicate alla gestione di servizi IT, è basato su una serie di pubblicazioni, periodicamente rivisitate, che forniscono suggerimenti e indicazioni sull'erogazione di servizi IT, al fine di perseguire un livello adeguato di qualità, di specificare i processi e i mezzi aziendali per supportarli. ITIL fornisce quindi linee guida a entità dotate di infrastrutture informatiche, dando loro direttive per sfruttare al meglio i servizi IT nell'esecuzione della propria missione. Nella sua struttura, ITIL è centrato sul service management, e indica una struttura per il rilascio di servizi basata su processi (Marrone & Kolbe, 2011). Nella sua ultima versione, lo standard ITIL indica i seguenti processi IT

che devono essere previsti: a) *Service Design*, b) *Service Transition*, c) *Service Operation*, e d) *Continual Service Improvement*. Eikkebrok e Iden (2017) sottolineano la crescente attrattività del modello ITIL pur nella presenza di difficoltà e complessità di implementazione.

Si tratta dunque, come per altre proposte, di un framework utile per la governance IT (Iden & Eikebrokk, 2014). Occorre notare che ITIL concerne la delivery di servizi attraverso processi standardizzati, pertanto si richiedono pratiche di Business Process Management (BPM) che, nell'ambito del contesto ITIL riguardano l'implementazione di processi che occorre assicurare che siano in linea con i processi di business (Eikkebrok & Iden, 2017). La letteratura evidenzia, come anticipato, un certo livello di complessità e il requisito di una significativa spinta di orientamento verso il cambiamento (es. Ramakrishnan, 2014; Eikebrokk & Iden, 2017; Iden & Eikebrokk, 2014); questo prefigura il fatto che l'implementazione di linee guida ITIL sia maggiormente perseguito da aziende e realtà più complesse. L'analisi di quanto esposto in ITIL porta comunque verso una valenza generale delle raccomandazioni, applicabili con diversi livelli da ogni tipo di azienda desiderosa di migliorare i propri processi tecnologici.

L'accento sulla governance IT (Iden & Eikebrokk, 2014) pone l'attenzione sulla leadership, le strutture e le relazioni in grado di assicurare che le strategie IT supportino correttamente strategia e obiettivi dell'azienda. L'adozione del framework ITIL è in crescita (Iden & Eikebrokk, 2014), come per altro accade per altri framework legati alla governance IT. La spiegazione risiede nei fatti già emersi per i trend di altri framework, ovvero la necessità di adottare strumenti strutturati per la governance de sistemi informativi, in un contesto che vede una forte crescita dell'IT in termini di complessità, di trasversalità sul business e di fonte di vantaggio competitivo per l'azienda (Ramakrishnan, 2014).

Dal punto di vista del posizionamento tra astrazione e operatività, ITIL si pone a un livello basso di astrazione, molto meno del COBIT, vedi capitolo 2.7, e a un livello abbastanza operativo tra strategia e tattica, ITIL infatti è definito come insieme di linee guida, quindi indicazioni molto vicine all'operatività.

ITIL – Conclusioni

Basandosi sulla letteratura esistente, Iden e Eikebrokk (2013) identificano diversi benefici derivanti dall'implementazione di ITIL, tra cui emergono in misura più frequente il miglioramento dell'orientamento del servizio e la soddisfazione del cliente. Ancora, l'implementazione del framework ITIL, peculiare ma non esclusivo di aziende con maggiore complessità nella gestione dei propri dipartimenti IT, dimostra un elevato potenziale nel miglioramento della *governance* IT (Iden & Eikebrokk, 2014). Il framework, sottendendo anche al processo di IT security management, oltre che indicare l'insieme di linee guida nella gestione dei vari servizi IT, fa si che anche questo insieme di best practice vada collocato tra gli elementi che contribuiscono al miglioramento dell'efficienza e della sicurezza dell'infrastruttura di Information Technology, sia nell'ambito della sicurezza reale, delle procedure, dei processi e delle operazioni, sia nell'ambito di quella percepita dal management aziendale.

2.7 Best Practice – COBIT

COBIT è un framework che consiste di best practice adottabili per la governance dei sistemi informativi delle aziende (COBIT, 2012). I sistemi informativi aziendali sono diventati un sistema cruciale per il supporto, la sostenibilità e la crescita delle aziende (De Haes, Van Grembergen, and Debreceny, 2013), questa importanza ha fatto si che l'IT governance deve essere indirizzata al supporto del business e alla riduzione del rischio correlato all'implementazione e alla gestione dell'IT aziendale (Bowen, Cheung, and Rodhe, 2007; Lin, Guan, and Fang, 2010). Sempre più aziende hanno una dipendenza vitale dalle strutture IT che sono progressivamente sempre più minacciate da pericoli esterni legati alle diverse forme di frodi e pericoli del cyber crime.

Dal punto di vista della strategia aziendale, l'IT ha il potenziale sia per supportare le strategie aziendali esistenti sia per porsi come fonte e origine di nuove (De Haes & al., 2013), l'Information Technology si pone in misura sempre più evidente come primario fattore di successo (*Key Success*

Factor) per le operazioni quotidiane di business, sia come abilitatore di nuovi vantaggi competitivi (Van Grembergen & De Haes, 2009).

Il concetto di IT governance ha ricevuto solo negli ultimi anni una considerevole attenzione accademica introducendo concetti come quello dell'allineamento strategico dell'IT, del contributo alla generazione del valore e della gestione del rischio come insieme dei principali abilitatori della IT governance (De Haes & al., 2013).

Il framework COBIT è stato sviluppato da ISACA (Information Systems Audit and Control Association) una associazione professionale internazionale che si occupa di Information Technology. Il framework prevede un sistema omnicomprensivo per supportare un'azienda nel suo obiettivo di creare una governance e una adeguata gestione dei suoi sistemi IT. L'approccio è di tipo olistico, esso considera l'intero insieme delle responsabilità tecniche e di business dell'area IT (De Haes & al., 2013).

Se consideriamo un posizionamento su due dimensioni di analisi, astrazione e livello di operatività, il posizionamento del framework COBIT può essere considerato a un livello medio di astrazione, inferiore a quanto espresso da sistemi generici di governance, per esempio, e un ampio spettro di operatività che spazia dalla governance dei modelli e dell'organizzazione fino alle tattiche IT (De Haes & al., 2013). Il framework (COBIT, 2012) è costituito attorno a cinque principi: 1) soddisfare i requisiti degli stakeholder, 2) supportare l'intera struttura aziendale, 3) l'adottare un singolo framework, 4) avere un approccio olistico, 5) separare la governance dalla gestione.

L'aspetto interessante del framework COBIT, dal punto di vista di questa ricerca, è che relativamente al punto 1) il sistema si basa su una Balanced Scorecard (Kaplan & Norton, 1996). Un ulteriore aspetto che ne facilita l'adozione risiede nel fatto che il sistema di Balanced Scorecard risulta composto da metriche e processi già definiti a priori, quindi risulta facilitato il confronto tra entità diverse e l'individuazione dettagliata delle responsabilità dei processi attraverso matrici RACI (*Responsible, Accountable, Consulted, Informed*) che individuano coloro che sono coinvolti in diversa misura nell'esecuzione del processo. Il modello per processi COBIT è suddiviso in 4 domini a) pianificazione e organizzazione, b) acquisizione e implementazione, c) delivery e supporto e d)

monitoraggio e valutazione. Il sistema consta di 34 obiettivi di controllo utilizzabili dagli auditor nella verifica della corretta implementazione di un ambiente sicuro per l'IT (es. in Lin & al., 2010).

COBIT – Conclusioni

Il framework COBIT permette un approccio standard, olistico e completo per un sistema di governance dell'IT di una azienda. L'approccio è completo, peraltro, nel suo proporre metodologie che vanno dalla governance vista dall'aspetto più strategico, alla pura operatività IT. Questo aspetto è una diretta derivazione, lo leggiamo nelle parole stesse, dell'adozione interna al framework di un sistema di Balanced Scorecard, uno degli strumenti utili, per l'appunto, alla trasformazione di strategia in operatività, per dirla secondo Kaplan e Norton (1996). Relativamente alla sicurezza ritroviamo metriche e giustificazione al framework nell'ambito dei processi *delivery e support*, processo *DS5 garantire la sicurezza dei sistemi* (COBIT, 2012). La forte tassonomia e uniformità proposta nei processi, dunque, ci fa includere questo framework all'interno di quelli dei quali vogliamo valutare la percezione di sicurezza associata, secondo l'obiettivo della presente ricerca.

2.8 Strumenti di gestione strategica – La Balanced Scorecard

La Balanced Scorecard (BSC) è uno strumento di pianificazione strategica, un sistema di gestione, nonché uno strumento operativo utilizzato per trasformare la strategia dell'azienda in operatività. Sviluppata a partire dagli anni '90 da Kaplan e Norton, la BSC è stata oggetto di un numero rilevante di pubblicazioni, studi e casi aziendali. Dalle origini della sua formulazione, il modello si è evoluto fino a rappresentare oggi un moderno modello strategico, in grado di offrire un supporto efficace alla pianificazione e di supportare la trasformazione di strategia in operatività (Kaplan & Norton, 1996). L'operatività, dal canto suo, genera anche i feedback necessari per correggere il sistema operatività - strategia (Kaplan & Norton, 2005). L'obiettivo di un sistema BSC è quello di costruire un modello efficace per comprendere e gestire le prestazioni dell'azienda e il suo allineamento con

la strategia. Alla base dello sviluppo del modello ci sono (Kaplan & Norton, 2005) anche i seguenti punti chiave:

a) La riduzione dell'eccesso di importanza attribuita in passato alla performance finanziarie delle società. Le prestazioni finanziarie, all'interno del BSC, sono una parte importante della valutazione del business, ma rappresentano solo una delle prospettive considerate (Bieker & Waxenberg, 2002);
b) la creazione di una connessione operativa tra la strategia e la visione, con le attività operative dell'azienda;
c) il miglioramento della comunicazione delle prestazioni organizzative e la riduzione della complessità delle attività di gestione.

La BSC è operativamente basata su un modello a quattro prospettive e di solito è rappresentato usando un'immagine come quella rappresentata in fig. 2.8.1.

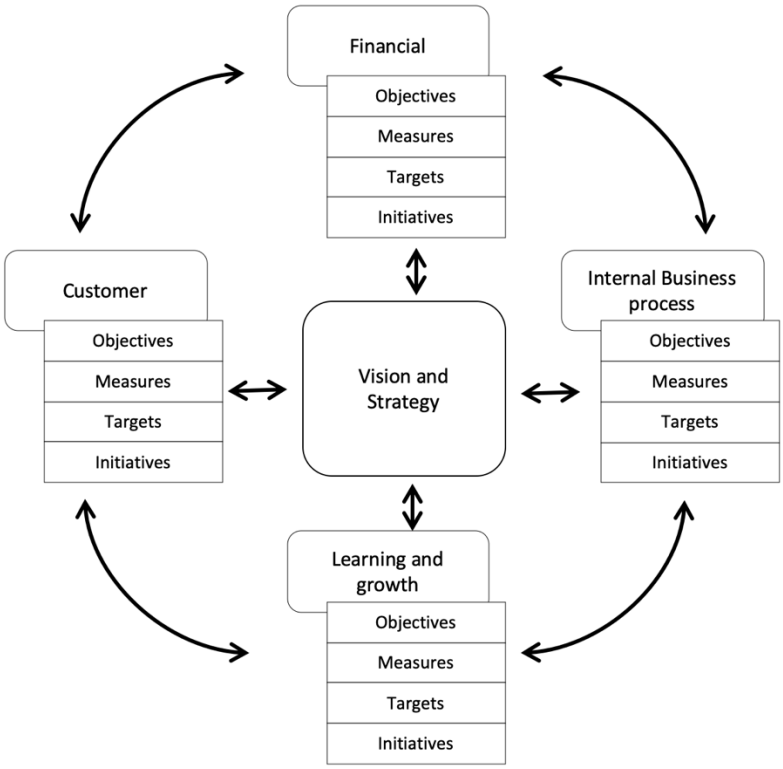

Fig. 2.8.1 – Prospettive BSC – Adattata da Kaplan & Norton, 1996.

La figura ci dice che la strategia è distribuita nelle diverse prospettive dell'azienda. In ogni prospettiva ci sono alcuni obiettivi collegati alla strategia. Per verificare il raggiungimento degli obiettivi ci sono target e misure, generalmente chiamati *Key Performance Indicators* (KPI). A seconda delle misure e della loro deviazione dai target, è possibile avviare iniziative e progetti per ripianificare e reindirizzare gli obiettivi.

Questa metodologia è rappresentata in fig. 2.8.2. Come si può vedere, i diversi elementi della visione e della strategia sono identificati nelle quattro prospettive e sono operativamente rappresentati da obiettivi e misure. Ogni obiettivo ha uno o più target. I target vengono confrontati con le misure reali e, a seconda del risultato del confronto, possono evidenziare il requisito di alcune iniziative correttive, come ad esempio l'avvio di progetti di miglioramento. I feedback, ovvero i risultati di queste azioni correttive, rientrano nella prospettiva per una nuova valutazione dell'efficacia delle azioni intraprese (Kaplan & Norton, 2005; Marr, 2010). Migliore sarà l'attenzione sui singoli processi indipendenti, migliore sarà la traduzione della strategia in operazioni. Ciò sarà a supporto della necessità di adottare un'organizzazione basata sui processi per supportare la tradizionale organizzazione funzionale.

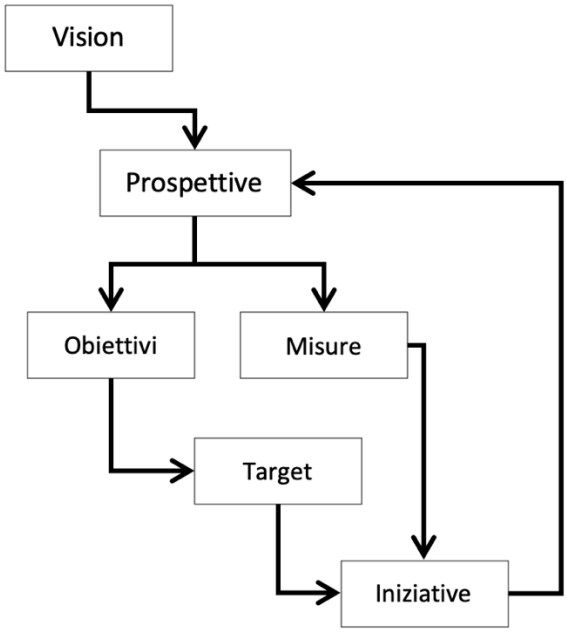

Fig. 2.8.2 – rappresentazione della BSC al lavoro.

La BSC si è evoluta dalla sua essenza originale, ovvero un sistema di prestazioni, in uno strumento strategico (Kaplan & Norton, 2005). Ciò è stato reso possibile grazie ai numerosi contributi sia dei suoi autori originali sia di altri ricercatori. Alcune delle radici del BSC sono state identificate nei sistemi di misurazione delle prestazioni, sviluppati dalla General Electric negli anni Cinquanta, e negli studi francesi relativi al concetto di *Tableau de Bord* (TDB). Alcuni ricercatori hanno anche cercato di identificare le differenze e le somiglianze tra BSC e i concetti alla base del TDB (Bourguignon, Malleret, and Norreklit, 2001). L'evoluzione della BSC nel tempo ha anche fornito risposte efficaci ad alcune critiche sorte sul modello (API, 2012; De Geuser, Mooraj, and Oyon, 2009; Olson & Slater, 2002; Ittner, Larcker, and Meyer, 2003; Norrelik, 2000; Humpreys & Trotman, 2011).

Rilevanza e validità del modello –L'importanza della metodologia BSC occupa una posizione rilevante nelle economie attuali poiché, ad esempio, la complessità e la dinamica dell'ambiente socioeconomico è in crescita e i manager spesso rivelano notevoli difficoltà a gestire questo tipo di ambiente. Altri ricercatori evidenziano l'efficacia della BSC e della sua capacità nel migliorare le prestazioni organizzative, nonché il suo contributo alla creazione di valore per l'azienda (De Geuser, et al., 2009). La BSC è anche riconosciuta come uno "strumento adeguato", in grado di fornire una serie concisa e apprezzata di informazioni ai manager (Mooraj, Oyon, and Hostettler, 1999).

Cultura della misurazione – Uno degli aspetti chiave della BSC è l'introduzione in azienda di una appropriata "cultura della misurazione". Costringere i manager a misurare aiuta a tradurre vaghi concetti o idee ambigue in qualcosa con una definizione precisa (Kaplan & Norton, 2004). Questo crea un linguaggio comune e una conoscenza distribuita nell'azienda, aiutando la traduzione della strategia in operatività. Un altro aspetto importante da menzionare è la validità generale del modello. In letteratura ci sono un numero rilevante di esempi di applicazioni di BSC e in tutte la struttura

portante del modello rimane sempre invariata. Non è necessario modificare i pilastri della BSC in base al settore, all'attività o alla posizione geografica dell'azienda. La validità generale del modello si riferisce anche ai sistemi di BSC applicati ai singoli dipartimenti di un'azienda (Russel, 2004). La BSC manifesta inoltre anche una naturale capacità di integrare aspetti sia quantitativi sia qualitativi, da quest'ultimo punto di vista sembra essere lo strumento ideale da utilizzare per integrare, ad esempio, anche le dimensioni sociale, ambientale e di sostenibilità (Bieker & Waxenberg, 2002).

Balanced Scorecard e Information Technology – Tornando all'uso della BSC all'interno di singoli dipartimenti aziendali vediamo come all'interno del framework COBIT5 è stato definito, ad esempio, un modo strutturato di utilizzare una BSC per la gestione dei processi IT dell'azienda. Le esigenze degli stakeholder aziendali sono quindi tradotte in una strategia che utilizza la BSC aziendale definendo gli obiettivi. Da questi obiettivi è possibile mappare una BSC predefinita per i processi IT, definendo quindi gli obiettivi relativi all'IT. Dal punto di vista puramente operativo e strumentale, un sistema di BSC, come altri modelli con un'implementazione operativa, può ottenere i relativi benefici dal supporto che riceve dai sistemi IT (Pearlson & Saunders, 2010), sia dal punto di vista dell'accessibilità dei dati sia per via delle capacità di elaborazione. La natura del modello, traducendo la strategia in operazioni, definendo obiettivi, identificando misure, fissando obiettivi, confrontando, attivando iniziative, richiede un uso intensivo di tecnologie IT per: a) memorizzare le misure target; b) analizzare misure reali da sistemi transazionali; c) analizzare le deviazioni dagli obiettivi lungo diverse dimensioni dell'analisi, d) riportare le deviazioni alla causa originale con una analisi spesso di tipo multidimensionale; e) misurare gli effetti delle iniziative intraprese per correggere le deviazioni dagli obiettivi, f) supportare analisi più rapide per una quantità significativa di dati, g) comprendere le dimensioni e le cause in cui si è verificato il disallineamento degli obiettivi.

Balanced Scorecard – Conclusioni

La Balanced Scorecard è uno strumento di pianificazione strategica e un sistema di gestione adottabile in misura *universale*, con una comprovata validità nella traduzione della strategia in

operatività. Per ottenere i migliori risultati da un sistema di BSC sono stati identificati alcuni prerequisiti: a) una organizzazione fortemente basata sui processi a supporto dell'organizzazione funzionale tradizionale, b) un approccio di gestione per eccezioni, incentrato sulle misure e sulla gestione degli scostamenti dagli obiettivi; c) supporto da parte dell'IT, per misurare gli indicatori ed esplorare le ragioni delle variazioni e valutare gli effetti delle iniziative di miglioramento; d) la strategia va intesa come un processo continuo.

Dal punto di vista della presente ricerca, il modello moderno della BSC rappresenta una best practice di gestione adeguato anche per l'IT, questo può essere giustificato: a) sia per la declinazione del modello stesso all'interno di altre specifiche best practice, come ad esempio COBIT, b) sia per la possibilità di monitorare l'efficienza del / dei processi di supporto tecnologico e informatico alle aree di business, c) sia, infine, per declinare la strategia di sicurezza IT in una operatività IT *security-oriented*, che integri ad esempio delle metriche di monitoraggio degli indicatori di sicurezza IT.

2.9 La formazione in ambito sicurezza IT

La letteratura riconosce che la formazione in ambito Information Technology è un fattore chiave di successo nelle applicazioni IT e utile nelle azioni a supporto del cambiamento (Soto-Acosta, Martinez-Conesa, et Colomo-Palacios 2010). A fronte di questa identificazione generale, il dibattito si è spostato spesso sul concetto stesso di formazione e la sua efficacia. Ad esempio, ci si è posti il problema dell'efficacia della formazione tradizionale e di come il ruolo dei colleghi possa avere un effetto guida sull'adozione e sull'apprendimento delle tecnologie IT (Gallivan, Spitler, et Koufaris, 2005). L'affermarsi delle tecnologie web ha visto affiancare alla formazione tradizionale anche sistemi di training on line, ovvero di piattaforme di *e-learning*, guidati da alcuni fattori chiave come costo, disponibilità e flessibilità.

Nell'ambito della realizzazione di programmi di formazione sulle procedure di sicurezza in ambito IT, occorre ricordare che prevedere delle sessioni di training sulle procedure e sulle linee guida non

è garanzia del fatto che gli utilizzatori adotteranno poi correttamente le informazioni apprese (Siponen, 2006).

La sicurezza IT, come anticipato, ha una componente tecnologica, basata su hardware e software, la cui efficacia è legata alla qualità dell'hardware, degli algoritmi utilizzati e dal rapporto di forza con eventuali agenti esterni "malevoli", siano essi sistemi automatici o hacker, e una componente umana. Le due componenti concorrono alla robustezza del sistema della sicurezza aziendale e la debolezza di uno dei due decreta la debolezza dell'intero sistema. L'anello debole del sistema sicurezza IT in azienda è rappresentato solitamente dal fattore umano, in quanto sistema che potrebbe non aver ricevuto sufficiente training, oppure potrebbe essere soggetto a disattenzioni o trucchi basati su tecniche di social engineering (Hadnagy, 2011).

Relativamente alla formazione occorre infine tenere presente che diverse delle best practice proposte richiedono una valutazione dell'efficacia formativa, cosa per altro non facile, non trattandosi solo delle valutazioni dei test di verifica di fine corso ma della reale efficacia delle nozioni trasmesse. Nel caso della sicurezza IT tale esigenza è ancora più sentita in quanto elemento integrante del sistema di sicurezza aziendale. Nel senso dell'efficacia dell'azione formativa, al fine dell'organizzazione delle sessioni di training, occorre ricordare la piramide dell'apprendimento, (Tabella 2.9.1) sviluppata dal *National Laboratory Training Institute* negli anni Sessanta e che pone una precisa scala di efficienza nell'apprendimento, in funzione delle tecniche didattiche.

Tabella 2.9.1 – Piramide dell'apprendimento

Efficacia dell'apprendimento	Metodologia di apprendimento.
90%	Insegnare i concetti appresi a qualcun altro
75%	Esercitarsi con i concetti appresi
50%	Discutere in Gruppo i concetti attesi
30%	Guardare una dimostrazione pratica
20%	Guardare un audio visivo
10%	Leggere
5%	Ascoltare una lezione

Fonte: National Laboratory Institute

La formazione in Ambito IT – Conclusioni

La formazione IT dovrebbe contribuire in azienda a una serie molto lunga di obiettivi tra cui vanno ricordati:

a) azzeramento, o minimizzazione, del *digital divide* generazionale, affinché ogni impiegato possa svolgere i propri compiti sfruttando al massimo l'efficienza gli strumenti IT;
b) migliorare l'allineamento tra le competenze disponibili e le competenze richieste dal business;
c) attivare un circolo virtuoso di consapevolezza degli strumenti IT che si traduca non solo in un effetto positivo sull'efficacia dell'attività lavorativa ma anche sul livello di sicurezza del patrimonio informativo aziendale.

La formazione in ambito IT si connota, indipendentemente dalla metodologia di erogazione e dagli strumenti, come fattore essenziale per migliorare l'intera catena della sicurezza del patrimonio informativo dell'azienda. Lo Strumento si pone su un livello più operativo degli altri strumenti analizzati e richiede comunque un aggiornamento e verifica periodici.

2.10 Conclusioni

Nell'ambito dei sistemi di gestione e delle best practice adottate in ambito IT, sono stati individuati alcuni strumenti che possono avere impatto sulla gestione, la percezione e il livello della sicurezza delle informazioni e dei sistemi tecnologici. La ragione del loro sviluppo e del crescente livello di diffusione, come visto, risiedono nel cambio di paradigma della struttura IT delle aziende, che si configura sempre di più come un sistema trasversale all'azienda, che contribuisce alla generazione del valore e che richiede quindi, efficienza, governance, e allineamento con la strategia di business. Tali strumenti, quindi, sono stati selezionati in quanto rappresentano la parte più significativa delle implementazioni con questo tipo di effetto, ideali quindi a identificare e classificare i fenomeni oggetto di indagine. Essi sono:

a) il modello del sistema di gestione ISO 27001,

b) la metodologia ITIL,

c) il framework COBIT,

d) lo strumento della Balanced Scorecard in quanto integra nel sistema dei processi gli aspetti legati alla sicurezza IT aziendale,

e) la formazione in ambito IT, come elemento strutturato e orientato al miglioramento della consapevolezza del rischio IT da parte dell'utente finale.

Tra alcune di queste metodologie esistono dei chiari legami, come ad esempio l'adozione dello strumento della Balanced Scorecard all'interno del framework COBIT, oppure il ruolo della formazione nella prospettiva interna della Balanced Scorecard e nei requisiti della norma ISO27001.

Tabella 2.10.1 – Riassunto delle best practice

Practice
ISO 27001
ITIL
COBIT
Balanced Scorecard
IT training

3 Metodologia

3.1 Introduzione alla progettazione della ricerca

Nella letteratura corrente non sono emerse delle ricerche che specificatamente abbiano l'obiettivo di indagare i campi di interesse della sicurezza reale e percepita in relazione con la presenza di sistemi di gestione specifici dell'area ICT e con attività di training del settore.

Si è cercato di operare rispettando i seguenti passi:

a) Identificazione delle *research questions* e delle ipotesi (Cap. 3.5)
b) Individuazione di una letteratura di riferimento sufficientemente ampia (Cap. 2) in grado di inquadrare non solo gli aspetti direttamente correlati ai fenomeni in analisi ma anche di definire un background sufficientemente robusto, in ragione della trasversalità degli argomenti. Dovendo trattare di IT, IT a supporto dei processi, passaggio da un paradigma che sposta la centralità dell'IT da un tema di tipo tecnologico a uno che lo propone come una delle leve strategiche di business, è stato necessario affrontare una disamina di diverse teorie.
c) Individuazione delle fonti dati primarie e secondarie e raccolta dei dati (Cap 3.3 e 3.4). Le fonti primarie necessarie sono state identificate e ne è stata pianificata la raccolta attraverso la somministrazione di un questionario, per i dati secondari si è fatto riferimento alla completezza e autorevolezza dei dati dell'Istat, Istituto Italiano di Statistica.
d) L'analisi dei dati raccolti (Cap 3.6) è suddivisa in due fasi; la prima fase prevede un'analisi delle singole variabili statistiche associate alle domande del questionario, la seconda prevede una analisi bivariata di combinazioni delle variabili statistiche associate alle domande del questionario. La difficoltà risiede nell'utilizzo di valutazioni di tipo qualitativo dove non è possibile utilizzare la normale metodologia statistica di tipo quantitativo. Per sopperire sono state utilizzate le funzionalità analitiche di un database multidimensionale

sui dati del questionario, associando ogni domanda a una diversa dimensione di analisi. Questo ha permesso, partendo dalle tabelle di contingenza delle distribuzioni bi-variate delle variabili statistiche associate alle domande del questionario, l'individuazione di forme di correlazione qualitativa.

3.2 Target e descrizione della popolazione

Si è scelto di analizzare aziende di tipo industriale o di servizio nelle quali sia presente una qualche forma di utilizzazione di risorse IT. Non sono stati messi particolari filtri sulla struttura al fine di recepire degli indicatori di composizione del campione. Occorre ricordare infatti che:

a) aziende molto piccole tendono ad avere architetture IT molto semplificate e spesso gestite in outsourcing, potrebbero quindi non aver maturato un concetto di sicurezza IT strettamente legato alla continuità, integrità e riservatezza. Esse potrebbero inoltre vedere l'area dei sistemi informativi come una commodity senza una particolare specializzazione, demandata a un fornitore sulla base di specifiche spesso generiche.
b) Aziende piccole tendono ad avere un numero limitato di processi, spesso semplificati e non necessariamente supportati da soluzioni tecnologiche.
c) Infine, come conseguenza dei punti precedenti è ancora più raro avere aziende di questo tipo per le quali si sia scelto qualche forma di certificazione di sicurezza oppure si sia adottato un qualche meccanismo di best practice, scelte che vengono normalmente riconosciute come troppo complesse per le piccole realtà.

Tra le aziende rientranti nel target avverrà poi una selezione, durante l'analisi dei dati, tra quelle che hanno o meno adottato sistemi di gestione della sicurezza formali, come ad esempio quanto espresso nella norma ISO 27001, o altri tipi di best practice come ITIL, COBIT o sistemi di Balanced Scorecard per i quali sia incluso un sistema di valutazione dell'IT. Non è stato posto un vincolo al campione sul numero di addetti in azienda. La ragione risiede nel fatto che dalle statistiche ufficiali

dell'ISTAT (Istat, 2019) l'utilizzo di tecnologie IT è trasversale a tutte le tipologie di azienda anche se ci sono dei legami di dipendenza tra tecnologie (es. adozione di HW, SW, Sistemi di sicurezza ecc.) e la dimensione dell'organico.

In considerazione dello strumento usato per la raccolta dati e le fonti disponibili, il campione risulta omogeneo con la popolazione delle imprese. Il campione analizza 628 fonti su un totale di quattro milioni e mezzo di imprese censite in Italia. Il campione risulta di piccole dimensioni anche se confrontato con le sole trecento ottantamila aziende manifatturiere.

3.2.1 Caratteristiche della popolazione

In questo paragrafo vengono evidenziati alcuni indicatori della diffusione dell'Information Technology e della sicurezza IT nelle aziende italiane, fonte Istat (2019). In questa sezione si procede a un'analisi di quello che può essere considerata una buona approssimazione delle caratteristiche della popolazione oggetto di studio, questo aspetto è giustificato dalla tipologia delle rilevazioni Istat, meglio descritte nel punto 3.3.3.

Tabella 3.2.1 - Indicatori ICT nelle imprese con almeno 10 addetti

Classe di Addetti	Da 10 a 49	Da 50 a 99	Da 100 a 240	Oltre 250
Imprese che impiegano, tra i propri addetti, specialisti ICT (incidenza %) (Complemento a 100 tra parentesi)	11,8 (88,2)	36,2 (63,8)	55 (45)	73,1 (26,9)
Imprese che hanno organizzato nell'anno precedente corsi di formazione per sviluppare o aggiornare le competenze ICT/IT dei propri addetti (incidenza %)	16,7	32	44,9	60,9
Addetti che utilizzano computer almeno una volta la settimana (incidenza % sul totale addetti)	54	52,3	56,9	56,7

Fonte: Istat (2019)

Si nota che al crescere del numero di addetti cresce la percentuale di aziende che impiegano specialisti ICT, dal punto di vista della presente ricerca, l'attenzione si pone piuttosto sull'analisi della parte complementare, ovvero la percentuale di aziende che non impiegano tra i propri addetti specialisti ICT, valori riportati tra parentesi. Le spiegazioni relativamente a queste percentuali risiedono sui seguenti aspetti:

a) ci sono realtà con un numero elevato di addetti che operano in contesti di tipo puramente produttivo, dove l'ICT ha meno peso relativamente alla complessità dei processi supportati, ad esempio unità produttive delocalizzate a bassa intensità di IT;
b) ci sono sempre più aziende che si affidano a personale ICT in outsourcing, specialmente nel caso sub a) e nei casi laddove ci siano pochi dipendenti, situazioni in cui il supporto IT è fortemente standardizzato;
c) molte aziende non specializzate, specialmente nella fascia fino a cinquanta addetti sono realtà per cui l'IT è *commoditizzato*, facilmente gestibile in outsourcing.

Relativamente alla *formazione* dei dipendenti in area ICT si nota lo stesso tipo di comportamento, ovvero si nota il crescere della percentuale di imprese che ha organizzato formazione sulle competenze ICT al crescere del numero di dipendenti. Si considerino questi aspetti:

a) al crescere del numero di addetti crescono il numero dei processi nonché la complessità e la specializzazione dei sistemi IT a supporto, fatto che comporta la necessità di formazione specifica;
b) all'aumentare della dimensione aziendale, cresce il numero di aziende che adottano procedure e best practice orientate alla gestione dell'IT (si veda anche le tabelle 3.2.2 e 3.2.3), per molte delle best practice la formazione degli utilizzatori ha un ruolo importante e spesso obbligatorio;
c) c) aziende con dimensioni maggiori solitamente aderiscono ad associazioni di categoria, quali Assindustria, che richiedono il versamento obbligatorio su un fondo specifico e nominativo per la formazione dei dipendenti, pertanto aziende di grandi dimensioni hanno

maggiore interesse a recuperare questi fondi attraverso l'erogazione di attività di formazione.

Infine, relativamente alla diffusione dell'uso dell'IT in azienda, si nota invece un allineamento delle percentuali di addetti che "utilizzano un PC almeno una volta a settimana" ovvero c'è uniformità tra le varie classi dimensionali. Dal punto di vista della diffusione delle tecnologie IT questo indicatore, suggerito dall'Istat, è un indicatore estremamente di "minimo" per un'azienda moderna, qualsiasi sia la sua dimensione in termini di numero di addetti. Sarebbe interessante indagare quale tipologia di aziende rientra tra quelle, poco meno della metà, in cui non viene raggiunto questo livello di utilizzo, ma questa dimensione di analisi non è per ora disponibile nei database dell'Istat.

Tabella 3.2.2 - Indicatori Sicurezza ICT nelle imprese manifatturiere con almeno 10 addetti

Classe di Addetti	Da 10 a 49	Da 50 a 99	Da 100 a 249	Oltre 250
Imprese che hanno documenti su misure, pratiche e procedure sulla sicurezza ICT (incidenza %)	32,7	55,9	67,3	82,9
Gestione dei diritti di accesso per l'utilizzo di ICT	91,8	98,2	97,7	98,6
Archiviazione, protezione, accesso o trattamento dei dati	95,6	97,3	98,9	97,4
Procedure o regole per prevenire o rispondere a incidenti di sicurezza	66,1	74,3	82,7	83,5
Responsabilità, diritti e doveri delle persone impiegate nel settore dell'ICT (ad es. uso di e-mail, dispositivi mobili, social media, ecc.)	86,1	90,4	91,4	96,2
Formazione delle persone impiegate nell'uso sicuro delle ICT	74,5	78,8	77,8	79,9
Documenti sulla sicurezza ICT definiti o rivisti negli ultimi 12 mesi (incidenza %)	82,5	78,6	77,9	82,9

Documenti sulla sicurezza ICT definiti o rivisti tra 12 e 24 mesi (incidenza %)	14,6	19,0	20,0	14,6
Documenti sulla sicurezza ICT definiti o rivisti più di 2 anni prima (incidenza %)	2,9	2,4	2,1	2,6

Fonte: Istat (2019)

Nella tabella 3.2.2 è possibile vedere alcuni degli indicatori relativi alla sicurezza ICT per la popolazione delle imprese manifatturiere italiane con più di dieci addetti (Istat, 2019). Come si può evincere al crescere del numero degli addetti cresce la *percentuale di aziende che hanno documenti, pratiche e procedure di sicurezza*, si può notare che solo realtà con più di 250 addetti raggiungono una percentuale di oltre l'80%, la lettura al negativo mette in luce che approssimativamente metà delle aziende con meno di 250 addetti non hanno documenti, pratiche e procedure di sicurezza IT (Rispettivamente 67,3%, 44,1% e 32,7%). In considerazione della diffusione delle problematiche di sicurezza IT c'è da segnalare una importante carenza documentale sulla sicurezza informatica, il che significa la presenza di una gestione non organizzata della sicurezza ICT. Parte della spiegazione risiede in quanto già visto in precedenza: la redazione di documenti e policy relativi alla sicurezza e alla gestione dell'IT sono spesso prescritte dall'adozione di best practice di gestione IT e sicurezza, diffuse nelle aziende di dimensioni maggiori. Declinando le varie sotto-voci dell'indicatore emerge che:

a) Esiste una percentuale molto elevata di aziende che, indipendentemente dal numero di addetti, utilizza la gestione dei diritti di accesso per l'utilizzo dell'IT, percentuali sempre molto elevate anche per gli strumenti di archiviazione, protezione, accesso e trattamento ai dati. Si tratta di un livello di sicurezza IT primario, che per altro oggi dovrebbe essere scontato; il raggiungimento di simili percentuali di adozioni è legato prevalentemente ai requisiti minimi richiesti dalle normative obbligatorie preesistenti alla normativa GDPR, che imponevano l'uso di profili utente, password, backup e sistemi antivirus. La tipologia

di soluzione, in un contesto del genere è vissuto come un aspetto tecnologico e meno come un'adozione di policy o processo di gestione.

b) Si notano percentuali elevate, su tutte le fasce di numero addetti, anche relativamente alla presenza di regole per la gestione degli incidenti di sicurezza e alle responsabilità, diritti e doveri degli operatori ICT; anche questi indicatori sono frutto di legislazioni precedenti come ad esempio il *documento programmatico per la sicurezza*, ormai non più obbligatorio.

c) Sufficientemente equi-distribuito risulta anche il tasso di formazione su temi di sicurezza ICT. Anche in questo caso possiamo scomporre l'indicatore in più parti; in questo caso abbiamo, come emerso dall'analisi della letteratura, che comincia ad affermarsi una sensibilità generale per i temi della sicurezza, a prescindere dalle dimensioni aziendali; inoltre la parte più vincolante della normativa, ad esempio quella relativa al GDPR, riguarda tutte le aziende.

d) Interessante infine notare che la maggior parte dei documenti relativi alla sicurezza ICT sono stati definiti o aggiornati negli ultimi dodici mesi, il significato va letto nella direzione che, all'interno di quelle aziende che si occupano in modo corretto della propria sicurezza ICT, dedicano risorse e tempi adeguati allo scopo.

Tabella 3.2.3 - Indicatori Sicurezza ICT nelle imprese manifatturiere con almeno 10 addetti

Classe di Addetti	Da 10 a 49	Da 50 a 99	Da 100 a 249	Oltre 250
Backup dei dati	86,2	92,0	93,0	96,1
Controllo dell'accesso alla rete	65,9	90,6	94,7	95,6
Valutazione del rischio ICT	30,9	54,6	66,4	77,0
Test di sicurezza ICT	31,9	52,4	64,4	80,4
Utilizzo di almeno una misura di sicurezza ICT	95,1	98,5	99,7	99,9
Impresa rende gli addetti consapevoli dei loro obblighi in materia di sicurezza ICT mediante formazione volontaria (incidenza %)	44,1	62,3	69,6	81,4
	25,7	53,9	75,2	90,5

Sicurezza ICT assicurata dal personale interno (incidenza %)				
Impresa ha subito almeno un incidente di sicurezza ICT relativo a indisponibilità dei servizi ICT (incidenza %)	6,8	8,4	14,0	17,4
Impresa ha subito almeno un incidente di sicurezza ICT relativo a distruzione o corruzione di dati (incidenza %)	3,9	5,0	3,6	5,6
Impresa ha subito almeno un incidente di sicurezza ICT relativo a divulgazione di dati riservati (incidenza %)	0,4	1,7	1,8	3,2
Impresa ha subito almeno un incidente di sicurezza ICT (indisponibilità servizi ICT, distruzione o corruzione di dati, divulgazione di dati riservati) (incidenza %)	9,8	12,2	16,0	21,2

Fonte: Istat (2019)

Nella tabella 3.2.3 è possibile analizzare ulteriori indicatori di sicurezza ICT per aziende manifatturiere italiane con più di 10 addetti, suddivisi per classi. In questo caso l'attenzione viene posta su aspetti progressivamente meno tecnologici e più legati a processi tipici del processo di gestione IT, procediamo con alcune considerazioni su questi dati; innanzitutto notiamo il fatto che una percentuale elevata di aziende adotta almeno una misura di sicurezza IT, in considerazione della varietà di strumenti, del numero di adempimenti di sicurezza IT da garantire anche indirettamente, ad esempio con le normative sulla privacy, e del rischio quotidiano associato alla sicurezza IT, dovrebbe stupire di più il fatto che queste percentuali non siano comunque del 100%. Proseguendo nell'analisi:

a) Il backup dei dati fa parte dell'insieme delle procedure di IT security tecnologiche più diffuse, come pure il controllo di accesso alla rete. In aziende di minime dimensioni è possibile che non esista una rete locale con controllo degli accessi, in questo senso si può spiegare la percentuale di minor adozione di questa soluzione di sicurezza in azienda in questa fascia.

b) La valutazione del rischio ICT e i test di sicurezza ICT fanno normalmente parte di procedure e best practice codificate, anche tra quelle illustrate nel capitolo 2. In questo modo va letta la percentuale crescente di adozione di queste pratiche nelle aziende con maggiore numero di addetti e quindi caratterizzate da un maggiore capacità di implementazione e di utilizzo delle best practice menzionate. Si può notare uniformità di distribuzione percentuale tra queste grandezze e quelle legate all'esistenza di documenti specifici sulla gestione della sicurezza e policy della tabella 3.2.2 (prima riga), a conferma della struttura delle best practice che sono state analizzate allo scopo della presente ricerca.
c) Relativamente alla gestione della sicurezza ICT si evidenzia sempre una correlazione immediata tra numero di addetti crescente e l'organizzazione di formazione, lo stesso accade con la percentuale di aziende che assicurano la sicurezza ICT attraverso personale interno.

Nell'ambito delle statistiche legate al numero e alla tipologia di incidenti IT si rilevano quattro casistiche proposte sulla popolazione in studio. I dati non informano sulla natura tecnologica o sociale degli incidenti IT ma possiamo abbozzare una riflessione in questo senso:

a) La percentuale di aziende che hanno subito almeno un incidente di sicurezza ICT relativo alla indisponibilità di servizi è proporzionale al numero di addetti. La tipologia di incidente è legata prevalentemente a guasti di tipo hardware o software, pertanto la correlazione va ricercata nel fatto che le aziende di dimensioni maggiori hanno una maggiore complessità delle infrastrutture IT, un maggior numero di processi di business da supportare e quindi sono oggetto di un maggior numero di guasti e disservizi potenziali.
b) La percentuale di aziende che ha subito almeno un incidente di sicurezza IT relativo a distruzione o corruzione di dati mostra un andamento non correlato al numero di addetti. La spiegazione risiede nella tipologia tecnologica dell'incidente IT e nell'esistenza, nella quasi totalità di aziende analizzate, di sistemi di backup e di controlli di accesso, si vedano in proposito i punti precedenti.

c) Relativamente alle imprese che hanno subito almeno un incidente di sicurezza ICT relativo alla divulgazione di dati riservati si può notare che tale tipologia è trascurabile nelle piccole aziende e comincia ad assumere maggiore rilevanza nelle aziende più grandi, in queste ultime gli asset informativi hanno maggior peso ed esistono diverse tecniche per la fuga di informazioni, anche non basate su aspetti tecnologici.

Conclusioni sulla popolazione

L'adozione di strumenti IT è un fatto diffuso tra tutte le aziende. All'aumentare del numero degli addetti aumenta, in ragione all'aumento correlato della complessità dei processi, anche l'attenzione verso la formazione sui temi della sicurezza ICT e verso l'utilizzo di personale dedicato per la gestione. Le pratiche formali di gestione della sicurezza sono diffuse e anche in questo caso in misura proporzionale al numero di addetti dell'azienda. In generale all'aumento della complessità, approssimata dalle statistiche sul numero di addetti, gli indicatori sull'adozione di tecnologie IT e delle relative metodologie di protezione assumono maggiore importanza.

3.3 Metodologia per la raccolta dei dati

Per rispondere alle ipotesi formulate nella ricerca, è necessario valutare sia dati primari, sia dati secondari. Per la raccolta dei *dati primari* si è scelto di adottare lo strumento del questionario. Il questionario è stato somministrato attraverso la rete Internet, in particolare nell'ambito del network professionale *Linkedin*, indirizzandolo attraverso gruppi e sottogruppi di interesse compatibili e congruenti con il target di analisi desiderato e con la struttura della popolazione (Cap. 3.2). Le risposte sono state sollecitate: a) direttamente, per quanto attiene alla rete diretta, e b) indirettamente, attraverso la pubblicazione segmentata di articoli che spiegavano l'obiettivo della ricerca e invitavano a partecipare alla raccolta dati. Nel corso del periodo della raccolta dei dati, durata complessivamente due mesi, sono stati ripetuti tre solleciti alla compilazione del questionario al fine

di incrementare il numero dei questionari sui quali realizzare l'analisi dei dati. Una parte dei questionari, il dieci percento circa, sono stati raccolti inviando la richiesta alla rete personale di conoscenze professionali accompagnando l'indirizzo web del questionario a una mail di richiesta che spiegava gli obiettivi della ricerca.

Gli obiettivi di analisi della ricerca prevedono la raccolta e l'elaborazione di dati prevalentemente di tipo qualitativo. Per ragioni di uniformità e di semplicità di somministrazione il questionario contempla entrambi i tipi di domande, che sono state disposte seguendo una sequenza logica di compilazione. Il questionario, riportato nel capitolo *Allegato 1*, prevede un numero complessivo di ventisei domande, numero che rappresenta un corretto equilibrio tra lunghezza del questionario e l'atteggiamento volontario del rispondente. Dove possibile le domande di tipo qualitativo sono state strutturate con la metodologia delle scale di Likert (Robertson, 2012).

Gli aspetti di cui si è voluto avere particolare cura nella raccolta sono:

- Indirizzamento del questionario verso il target identificato
- Significatività e completezza delle risposte
- Assoluta garanzia di riservatezza del dato raccolto

3.3.1 Indirizzamento del questionario

Il metodo più semplice per somministrare il questionario a un campione che possa rispecchiare la struttura della popolazione è consistito nel ricorrere a un sottoinsieme sufficientemente vasto nato spontaneamente attorno alla popolazione stessa. In questo caso un social network, *Linkedin*, che per sua natura chiama ad adesione personale di aziende, e le aziende stesse, caratterizzate da un accesso e un utilizzo delle tecnologie IT, ha una completa varietà nel numero di addetti, nei settori e nell'utilizzo e sperimentazione delle tecnologie IT. Pur non rappresentando una soluzione ottimale dal punto di vista scientifico, si tratta della soluzione economicamente e accettabile nell'ambito di una ricerca di questo tipo.

3.3.2 Significatività e completezza delle risposte

Al fine di garantire significatività e completezza delle risposte sono stati eliminati dal dominio di analisi i questionari che mostravano risposte incomplete e quelle che presentavano elementi non giustificabili di evidente contraddizione nei dati.

3.3.3 Assoluta garanzia della riservatezza del dato raccolto

L'aspetto legato alla riservatezza del dato raccolto contempla due elementi. Il primo concerne la necessità di garantire la riservatezza dell'informazione raccolta in quanto tale. Ci sono informazioni aziendali che possono essere considerate a tutti gli effetti pubbliche, come il numero di dipendenti e il fatturato, mentre altre informazioni, come il numero di incidenti IT o le ore di formazione erogate sono considerate riservate o a circolazione limitata da diversi sistemi di gestione delle informazioni. Il secondo aspetto riguarda le informazioni di tipo personale, che sono invece garantite in tutta la Comunità Europea dalla normativa del *General Data Protection Regulation*, più nota col nome di GDPR. La soluzione adottata è stata quella della totale *anonimizzazione* del questionario. L'unico riferimento di tipo personale, presente nel questionario consiste, in misura volontaria, nell'indicazione di un indirizzo e-mail da parte del rispondente, nel caso in cui egli desideri ricevere, come ricompensa per la partecipazione alla raccolta dati, un estratto aggregato dei risultati ottenuti. Questo dato è stato memorizzato su un sistema a parte, slegato da ogni collegamento con la base dati del questionario.

Per la raccolta dei dati secondari si è fatto riferimento a un database pubblico di statistiche relative agli argomenti trattati. Il database utilizzato è quello dell'Istituto Italiano di Statistica, ISTAT, che rende disponibili diversi *dataset* (Istat, 2019) relativi alle imprese, in particolare centinaia di analisi per imprese, su dimensioni geografiche, personale e struttura riguardanti organizzazione, innovazione, Information Technology, fiducia nell'economia, ricerca e sviluppo. La rilevanza della fonte dati ISTAT è legata a due aspetti:

a) i dati sono aggiornati molto frequentemente, la maggior parte delle fonti utilizzate risalgono all'anno precedente;
b) per le imprese nazionali esiste l'obbligo legislativo di risposta ai questionari distribuiti dall'Istat. Nell'ordinamento italiano l'obbligo di risposta è sancito dall'art. 7 del DLG del 6 settembre 1989, n. 322 (norme sul sistema statistico nazionale) che prevede una diversa graduazione di tale obbligo, secondo la natura del rispondente: amministrazioni, enti, organismi pubblici da una parte e soggetti privati dall'altro.

L'uso dei dati secondari è servito per due principali ragioni: a) verificare la congruenza della struttura dati raccolta con i questionari e b) aggiungere elementi di analisi alle implicazioni che sono emerse dall'analisi dei dati primari (Capitolo 3.2).

3.4 Strumenti

Per la raccolta dei dati primari è stato fatto ricorso ad alcuni strumenti software gratuiti e disponibili sulla rete Internet, in particolare lo strumento *Google Forms*, disponibile anche gratuitamente per tutti coloro che utilizzano un account Google e il relativo sistema di archiviazione *Google Drive*. Lo strumento permette di disegnare in maniera molto semplice degli articolati sistemi di raccolta dati, nella forma del questionario, impostando il corretto metodo di compilazione, come ad esempio risposte a scelta multipla, inserimento di valori e flussi di controllo. Una volta testato, il questionario può essere inviato attraverso l'invio diretto o la pubblicazione di un semplice link. Il questionario è riproposto nel capitolo *Allegato 1*.

La raccolta dati avviene in background e in modo asincrono sul sistema di *Google Forms*, tutte le risposte, ovvero l'insieme dei dati grezzi primari, viene progressivamente memorizzata in un documento tabellare, sempre memorizzato all'interno del profilo di Google utilizzato. Una volta completata la raccolta dei questionari, l'insieme dei dati grezzi viene trasferito in un data base locale, dove verrà controllato, validato ed analizzato attraverso una serie di strumenti di calcolo. L'analisi

e la rappresentazione dei dati, in considerazione della quantità e della tipologia di dati da analizzare, è stata fatta con diversi strumenti, in particolare: a) Query su base dati di tipo SQL; b) elaborazioni con lo strumento di analisi dati basato su un database multidimensionale; c) elaborazioni parziali e rappresentazioni realizzate con un foglio elettronico.

3.5 Domande di ricerca e ipotesi

L'obiettivo della presente ricerca è di valutare l'effetto dell'introduzione in azienda di sistemi di gestione della sicurezza delle informazioni, o altre best practice gestionali orientate al governo dei sistemi informativi o dell'organizzazione, sulla sicurezza informatica, reale e percepita. In pratica si indaga il legame tra l'esistenza o meno di questi sistemi di gestione e una serie di indicatori reali della sicurezza IT e una serie di percezioni del management, valutati con un sistema di scale di Likert.

Un fattore chiave, comune a questi sistemi di gestione, riguarda la formazione (Capitolo 2), pertanto una valutazione quantitativa e qualitativa dell'aspetto formativo, essendo tra gli aspetti più facili da indagare per quanto attiene le risorse umane, rappresenta un ulteriore argomento di indagine nella relazione tra la presenza del modello e la sicurezza, reale o percepita, dell'area IT.

3.5.1 Research questions

Q1 – Avere adottato in azienda un sistema di gestione o delle best practice orientate alla sicurezza IT, aumenta la percezione del livello della sicurezza informatica nel management di una azienda?

Q2 – Avere adottato in azienda un sistema di gestione o delle best practice orientate alla sicurezza IT, riduce il numero di incidenti IT?

Q3 – Esiste un legame tra le ore erogate di formazione sulla sicurezza IT al personale aziendale e la percezione della sicurezza IT?

Q4 – Esiste un legame tra le ore di formazione per la sicurezza IT erogate al personale aziendale e il numero di incidenti IT?

Si può notare che Q1 e Q3 prevedono di valutare un legame tra degli aspetti qualitativi; Q2 prevede di valutare un legame tra l'indicatore di presenza del sistema di gestione e il numero di incidenti IT, infine Q4 prevede di valutare un legame tra due variabili quantitative, in questo caso però, per una limitazione legata alla riservatezza dei dati raccolti, si è scelto di lavorare con classi di valori, trasformando di fatto le variabili in strutture qualitative da cui, con la modalità di analisi adottata, si sono comunque estratte le indicazioni cercate.

3.5.2 Research Hypotesys

Lo studio realizzato nella presente ricerca mira a dimostrare le ipotesi seguenti, valide per la tipologia di campione prescelto.

H1 – Adottare un sistema di gestione della sicurezza IT e / o delle best practice in questo ambito comporta una maggiore percezione della sicurezza IT dell'azienda da parte del management.

H2 – Adottare un sistema di gestione della sicurezza IT e / o delle best practice in questo ambito, riduce il numero di incidenti IT in una azienda.

H3 – Esiste un legame tra le ore di formazione IT erogate e la percezione del livello di sicurezza informatica da parte del management.

H4 – Esiste una correlazione inversa tra il numero di incidenti IT e le ore di formazione IT erogate

Si può notare che le idee sottostanti alle ipotesi H1, H2, H3 sono basate su un ipotizzabile principio di attenzione che possiamo descrivere come segue: la consapevolezza di avere dedicato o costruito dei sistemi formalizzati, che siano essi dei sistemi di gestione, delle best practice, della formazione o altre strutture formali sottostanti a un processo, pone questo processo in evidenza alla mente umana

con una connotazione positiva. Come visto nel capitolo 2, la sicurezza IT è un processo. Relativamente all'ipotesi H4, essa trae indicazione da alcuni aspetti importanti della sicurezza informatica, in particolare il ruolo del fattore umano, che risulta essere il punto debole del processo di IT security pertanto lavorare con la formazione non può che apportare beneficio.

3.6 Analisi dei dati

Sono stati raccolti 691 questionari, in seguito a una prima verifica sui contenuti, sono stati eliminati 63 di questi, in quanto presentavano domande incomplete o emergevano delle risposte in evidente contraddizione, come ad esempio un definito numero di incidenti IT contrapposto al fatto che gli incidenti IT non venissero registrati in azienda. Sono stati analizzati i 628 questionari che sono stati considerati validi.

3.6.1 Verifica preliminare dei dati raccolti – Variabili anagrafiche descrittive

Questa prima parte dell'anali relativa ai dati raccolti si occupa della descrizione delle variabili di tipo anagrafico-descrittivo del campione. L'analisi riguarda la distribuzione di frequenza e quindi la *moda statistica* delle riposte considerate valide. La prima variabile anagrafica del questionario riguarda la sede geografica dell'azienda del rispondente, si tratta per l'88,69 % di aziende localizzate in Italia, per il 9,24% localizzate in Europa e il rimanente 2,07% dal resto del mondo (Tabella 3.6.1.1).

Tabella 3.6.1.1 – Provenienza geografica

Area Geografica	n.	%
Italia	557	88,69 %
Altri paesi EU	58	9,24 %
Resto del Mondo	13	2,07 %
	628	100.00 %

Il questionario ha interessato per il 76,91% aziende che producono e / o vendono beni, il rimanente consiste di aziende del settore servizi. Tabella (3.6.1.2). Le voci relative ad "Altro", presenti in

minima parte nella raccolta del questionario, sono state eliminate dall'attività di validazione dei dati descritta in precedenza.

Tabella 3.6.1.2 – Macro-settore

Macro-settore	n.	%
Produzione e Vendita	483	76,91 %
Servizi	145	23,09 %
Altro	/	/
	628	100.00 %

Il 48,09 % delle aziende dei rispondenti hanno un fatturato maggiore di 50 milioni di € mentre il 35,99% hanno più di 100 dipendenti (Tabelle 3.6.1.3 e 3.6.1.4). A causa del tipo di popolazione utilizzata per estrarre il campione, le cui caratteristiche sono state descritte in precedenza, c'è una maggiore presenza di imprese con una dimensione maggiore rispetto alla distribuzione della popolazione nazionale. Dal punto di vista dell'analisi questo può essere considerato un beneficio in quanto vengono auto-escluse tutte quelle micro-realtà che adottano paradigmi di commoditizzazione semplificata dell'IT, descritte nella parte teorica.

Tabella 3.6.1.3 – Fatturato

Fascia di fatturato	n.	%
Meno di 1 Milione di €	45	7,17 %
Da 1 a 10 Milioni di €	88	14,01 %
Da 10 a 50 Milioni di €	193	30,73 %
Oltre 50 Milioni di €	302	48,09 %
	628	100.00 %

Tabella 3.6.1.4 – Numero di addetti

Fascia: numero di addetti	n.	%
Da 1 a 10 dipendenti	44	7,01 %
Da 11 a 25 dipendenti	82	13,06 %
Da 26 a 100 dipendenti	276	43,95 %
Oltre i 100 dipendenti	226	35,99 %
	628	100.00 %

Integrando le due tabelle in una matrice di contingenza che lega classe di dipendenti e la classe di fatturato, otteniamo la seguente tabella 3.6.1.5 che mostra il legame tra le due grandezze, la tabella serve come ulteriore elemento di verifica della coerenza delle risposte, si noti infatti la prevalenza

dei dati sulla diagonale principale, avendo la maggior parte delle aziende, di produzione e vendita, una correlazione di questo tipo tra le due grandezze.

Tabella 3.6.1.5 – Legame fatturato – dipendenti

Dip. \ Fatt.	< 1 M €	1 -10 M€	10-50 M€	>50M€	Totale
1-10	6,4 %	0,6 %			7 %
11-25	0,8 %	6,2 %	6,1 %		13 %
26-100		6,8 %	21,0 %	16,1 %	44 %
>100		0,3 %	3,7 %	32,0 %	36 %
Totale	7 %	14 %	31 %	48 %	100 %

Nella tabella 3.6.1.6 viene mostrata la distribuzione nelle aree di responsabilità dei rispondenti al questionario, si nota la prevalenza di responsabili dell'area IT, per i due terzi, mentre una quota comunque consistente, un terzo, di rispondenti afferisce ad altre aree aziendali. Questo è importante perché andrà a rafforzare l'analisi che mette in relazione aspetti percettivi, svincolati dalle competenze tecniche. La seconda voce più importante è l'area di general management (12,58%) segno della crescente importanza strategica dell'area IT per le aziende.

Tabella 3.6.1.6– Area di responsabilità

Area di responsabilità	n.	%
Amministrazione Finanza e Controllo	40	6,37 %
General Management	79	12,58 %
Information Technology	427	67,99 %
Aree tecniche e logistica	12	1,91 %
Produzione	14	2,23 %
Sales & Marketing	56	8,92 %
	628	100.00 %

Nella tabella 3.6.1.7 viene mostrata la distribuzione di frequenza che mostra in quante delle aziende interessate c'è la presenza di una formale struttura che controlla l'IT della stessa, e che fa capo a un responsabile formale.

Tabella 3.6.1.7 –Presenza di un dipartimento IT

Dipartimento IT	n.	%
Presenza di un dip. IT	588	93,63 %
Assenza di un dip. IT	40	6,37 %
	628	100.00 %

Se incrociamo questa informazione con l'altra dimensione strutturale, ovvero il numero di dipendenti, otteniamo la tabella 3.6.1.8, dove si vede che la maggior parte delle aziende non dotate di un dipartimento IT formale sono quelle con meno di 10 dipendenti. Questa mancanza non implica assenza di strumenti e supporto IT, solitamente in questi casi c'è il ricorso all'outsourcing o all'attività part-time non formalizzata di uno dei dipendenti dell'azienda.

Tabella 3.6.1.8 – Legame dipendenti – Dipartimento IT

Dip. \ IT.	No	Si	Totale
1-10	5,25 %	1,75 %	7,01 %
11-25	1,11 %	11,94 %	13,06 %
26-100		43,95 %	43,95 %
>100		35,99 %	35,99 %
Totale	6,37 %	93,63 %	100,00 %

3.6.2 analisi singole risposte e distribuzioni

In questa sezione vengono analizzate le variabili statistiche del questionario da un punto di vista unidimensionale. Unite alle analisi dei legami effettuate nel prossimo paragrafo 3.6.3 contribuiranno alla conferma delle ipotesi della ricerca. Nelle tabelle che seguono vengono analizzati dei dati qualitativi raccolti con domande del questionario strutturate secondo una scala di Likert. La legenda della scala riportata nelle tabelle è qui di seguito riportata, richiama la notazione inglese:

CA	*Completely agree*	*Completamente d'accordo*
PA	*Partially Agree*	*Parzialmente d'accordo*
NAD	*Neither Agree nor Disagree*	*Né in accordo né in disaccordo*
PD	*Partially Disagree*	*Parzialmente in disaccordo*
CD	*Completely Disagree*	*Completamente in disaccordo*

Q1 - Nel mio lavoro utilizzo in maniera intensa i sistemi informatici

Nella tabella 3.6.2.1 viene riassunta la distribuzione di frequenza relativa alla domanda sull'intensità IT del lavoro del rispondente. Si nota una assoluta prevalenza di risposte da parte di personale che afferma che il proprio lavoro è sicuramente IT intensive. Guardando la scala della risposta si nota una ridottissima percentuale di chi non la pensa in questo modo, segno che l'attività di qualsiasi manager in azienda sia pesantemente caratterizzata dalla presenza e dall'uso di sistemi informatici.

Tabella 3.6.2.1 – Presenza di lavoro *IT-intensive*

	n.	%
1 – CA	538	85,67 %
2 – PA	77	12,26 %
3 – NAD	8	1,27 %
4 – PD	5	0,80 %
5 - CD	0	
	628	100.00 %

Q2 - Senza l'uso di supporto informatico sarebbe difficile svolgere il mio lavoro

Nella tabella 3.6.2.2 viene proposta la distribuzione di frequenza delle risposte relative alla affermazione secondo cui senza l'uso di supporti informatici sarebbe difficile svolgere il proprio lavoro. Per l'87,58 del campione l'affermazione è completamente condivisibile, unita alla percentuale di coloro per cui è almeno parzialmente condivisibile si raggiunge il 97,77 %, per il campione di aziende interessato, dunque, l'IT è un supporto di business praticamente irrinunciabile.

Tabella 3.6.2.2 – Necessità di supporto IT

	n.	%
1 – CA	550	87,58 %
2 – PA	64	10,19 %
3 – NAD	11	1,75 %
4 – PD	3	0,48 %
5 - CD	0	
	628	100.00 %

Q3 - L'azienda in cui lavoro è fortemente informatizzata

Nella tabella 3.6.2.3 viene proposto il giudizio sul livello di informatizzazione dell'azienda. In questo caso il livello di concentrazione sul valore della moda statistica è meno accentuato sul valore

massimo, comunque il 62,90 % del campione ritiene l'azienda essere fortemente informatizzata, i due valori massimi di accettazione raggiungono il 94,43 %

Tabella 3.6.2.3 – Tasso di informatizzazione

	n.	%
1 – CA	395	62,90 %
2 – PA	198	31,53 %
3 – NAD	24	3,82 %
4 – PD	11	1,75 %
5 - CD	0	
	628	100.00 %

Dalle risposte a queste prime tre domande emerge un campione che è sostanzialmente in accordo con le affermazioni che li vedono lavorare in aziende fortemente informatizzate, che il loro lavoro richiede un forte utilizzo di tecnologie IT, senza le quali sarebbe difficile fare il loro lavoro.

Q4 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

Nella tabella 3.6.2.4 viene valutata l'adozione di best practice di gestione IT in azienda. È interessante notare la presenza di una maggiore distribuzione sull'intero campione. Il valore di moda statistica si attesta al 48,57 sull'adozione, mentre per quasi il 33 % non c'è accordo su tale affermazione. L'adozione di questi sistemi, come evidenziato nell'analisi della letteratura, è appannaggio di aziende più strutturate. Questa variabile verrà meglio spiegata nella parte di analisi dei legami bivariati.

Tabella 3.6.2.4 – Adozione di best practice

	n.	%
1 – CA	305	48,57 %
2 – PA	92	14,65 %
3 – NAD	24	3,82 %
4 – PD	103	16,40 %
5 - CD	104	16,56 %
	628	100.00 %

Q5- La presenza di un sistema di gestione certificato suggerisce un livello adeguato di sicurezza delle informazioni aziendali

Nella tabella 3.6.2.5 viene rappresentata la distribuzione di frequenza relativa alla percezione di sicurezza suggerita dall'adozione di best practice IT. La moda statistica è centrata sul secondo valore di accettazione, PA; nel 94,90 % dei casi è comunque opinione comune che l'adozione di un sistema di gestione certificato per l'IT, o di altre best practice come quelle descritte nel capitolo di analisi della letteratura, possano suggerire un livello adeguato di sicurezza delle informazioni aziendali.

Tabella 3.6.2.5 – percezione di sicurezza

	n.	%
1 – CA	256	40,76 %
2 – PA	340	54,14 %
3 – NAD	7	1,11 %
4 – PD	25	3,98 %
5 - CD		0,0 %
	628	100.00 %

Q6 - L'azienda ha adottato un sistema di gestione delle informazioni con l'obiettivo di aumentare il livello di sicurezza informatica

Nella tabella 3.6.2.6 il legame tra l'adozione del sistema di gestione delle informazioni e l'obiettivo di sicurezza. La moda statistica indica chiaramente questo legame, valore che raggiunge il 97,13 %. La singola risposta in completo disaccordo sembra più un errore di compilazione o di incomprensione della domanda.

Tabella 3.6.2.6 – sistemi di gestione per la sicurezza

	n.	%
1 – CA	436	69,42 %
2 – PA	174	27,71 %
3 – NAD	13	2,07 %
4 – PD	4	0,64 %
5 - CD	1	0,16 %
	628	100.00 %

Q7 - L'adozione di un sistema certificato di gestione della sicurezza delle informazioni ha comportato anche un beneficio di immagine e commerciale

L'idea alla base di questa domanda è che l'aver adottato un sistema di gestione delle informazioni possa essere una leva di tipo promozionale, utile per comunicare un elemento distintivo della propria capacità di gestione del patrimonio informativo. Occorre ricordare infatti che lungo la *catena del valore estesa* (fornitore, azienda, cliente) ci sono molti elementi di intersezione informativa (Porter, 1985). La moda statistica si assesta su un valore di parziale accettazione dell'affermazione, la distribuzione in questo caso è più centrale delle altre viste fino ad ora. La spiegazione risiede probabilmente nel fatto che il passaggio, già citato, dell'Information Technology che si trasforma da un paradigma tecnico a uno manageriale è ancora in corso per molte aziende.

Tabella 3.6.2.7 – benefici di immagine da sicurezza

	n.	%
1 – CA	66	10,51 %
2 – PA	363	57,80 %
3 – NAD	158	25,16 %
4 – PD	41	6,53 %
5 - CD	0	0 %
	628	100.00 %

Q8 - La sicurezza IT è composta da tre fattori: integrità, disponibilità e riservatezza. È compito del management aziendale assicurarsi che le informazioni aziendali siano tutelate in tutti e questi tre ambiti.

Dalla tabella 3.6.2.8 emerge un forte riconoscimento a due aspetti fondamenti, analizzati nella parte di analisi della letteratura e qui confermata: la sicurezza IT non è solo un aspetto legato alle violazioni informatiche più note, ma un concetto a tre dimensioni ben codificato; il secondo aspetto è che il compito della gestione della sicurezza IT spetta a un livello manageriale, proprio perché è chiaro che il valore dell'informazione è parte integrante della generazione del valore di business (Capitolo 2). L'86,46% del campione è orientato su questa opinione.

Tabella 3.6.2.8 – Sicurezza compito del management

	n.	%
1 – CA	394	62,74 %
2 – PA	149	23,73 %
3 – NAD	75	11,94 %
4 – PD	10	1,59 %
5 - CD	0	0 %
	628	100.00 %

Q9 - Le informazioni e i dati aziendali sono estremamente importanti per i risultati della nostra azienda.

L'importanza dei dati aziendali e il loro impatto sui risultati sono pienamente riconosciuti dalla quasi totalità del campione, per il 97,29 %. Vi è quindi uniforme consapevolezza del legame tra informazioni, strutture IT e capacità delle aziende di generare business.

Tabella 3.6.2.9 – Dati importanti per il business

	n.	%
1 – CA	332	52,87 %
2 – PA	279	44,43 %
3 – NAD	17	2,71 %
4 – PD	0	0 %
5 - CD	0	0 %
	628	100.00 %

Q10 - Senza una infrastruttura IT efficiente e sicura non sarebbe per noi possibile fare business

Questo aspetto è legato al filone delle tecnologie e delle informazioni a supporto delle attività del business, e, in maniera congruente alle altre distribuzioni analizzate mette in luce ulteriormente l'opinione secondo cui per l'azienda non sarebbe possibile fare business senza una infrastruttura IT efficiente e sicura (97,39% del campione). C'è un legame importante con la domanda precedente, che verrà approfondita in seguito in maniera congiunta, nella domanda precedente si conferma l'importanza di dati e dell'Information Technology per fare business, in questa si conferma che l'infrastruttura tecnologica per la loro elaborazione è ugualmente essenziale.

Tabella 3.6.2.10 – sicurezza infrastrutture IT

	n.	%
1 – CA	378	60,19 %
2 – PA	237	37,74 %
3 – NAD	13	2,07 %
4 – PD	0	0 %
5 - CD	0	0 %
	628	100.00 %

Q11 - La sicurezza IT è uno dei fattori in cui la nostra azienda investe molto

L'opinione di una parte consistente del campione, quasi l'80%, conviene sul fatto che l'azienda investa molto sul fattore della sicurezza IT. In parte l'opinione che emerge potrebbe anche essere influenzata dalla mole di attività preparatoria e comunicativa legata ad adeguamenti normativi in tema di dati personali, eventuali implicazioni emergeranno nel seguito.

Tabella 3.6.2.11 – Investimenti in sicurezza

	n.	%
1 – CA	297	47,29 %
2 – PA	202	32,17 %
3 – NAD	104	16,56 %
4 – PD	15	2,39 %
5 - CD	10	1,59 %
	628	100.00 %

Q12 - Ritengo che il personale dell'azienda sia adeguatamente preparato al corretto utilizzo dell'informatica

Il business non può beneficiare completamente dell'infrastruttura IT se il personale non è adeguatamente formato all'uso degli strumenti. In generale la formazione IT è oggetto di valutazioni contrastanti (Capitolo 2). L'opinione sull'adeguata formazione IT in azienda da parte del campione mostra valori positivi per oltre il 70 % dei rispondenti.

Tabella 3.6.2.12 – personale preparato all'IT

	n.	%
1 – CA	328	47,29 %
2 – PA	116	32,17 %
3 – NAD	85	16,56 %
4 – PD	76	2,39 %
5 - CD	23	1,59 %
	628	100.00 %

Q13 - Esistono dei servizi IT in uso all'azienda e che devono essere sempre garantiti?

Sulla base dei tassi di informatizzazione, della pervasività e importanza dei servizi IT si giustifica l'opinione che vede l'esistenza, per almeno il 87,43% dei rispondenti, di servizi IT considerati vitali e che devono essere sempre garantiti.

Tabella 3.6.2.13 – Servizi IT garanti

	n.	%
Si	549	87,42 %
No	79	12,58 %
	628	100.00 %

Q14 - Esiste un regolamento IT aziendale formalizzato?

Quando la struttura di un'azienda comincia a diventare complessa, le risorse IT crescono e i processi diventano molto interrelati; il primo strumento per organizzare l'uso degli strumenti IT e garantire un primo livello di sicurezza delle informazioni è l'adozione di un regolamento IT, che ne codifichi l'uso degli strumenti, dei dati e delle informazioni. L'86,62% dei rispondenti dichiara che l'azienda è dotata in un regolamento di questo tipo. Occorre ricordare che questo è spesso previsto sia dalle best practice analizzate, sia da normative e regolamenti, inoltre non è infrequente che i regolamenti aziendali "generici" spesso interiorizzino gli aspetti più generali delle regole previste per L'Information Technology dell'azienda.

Tabella 3.6.2.14 – Esistenza di un regolamento IT

	n.	%
Si	544	86,62 %
No	84	13,38 %
	628	100.00 %

Q15 - Viene eseguita in azienda una analisi periodica dei rischi IT?

Q16 - In azienda vengono registrati gli incidenti IT?

Analizziamo assieme queste due domande. L'analisi dei rischi IT è un elemento fondamentale nella gestione IT, ed è un requisito richiesto da diverse best practice e sistemi di gestione. Occorre considerare due aspetti: il primo, citando Kaplan e Norton (2004), si riferisce al fatto che "non si

può gestire ciò che non si conosce", pertanto l'esistenza di un processo di gestione del rischio ne richiede l'analisi; il secondo è legato al fatto che per sua stessa natura il rischio è un concetto probabilistico e pertanto non si può annullare; le pratiche pertanto suggeriscono metodologie per il trattamento del rischio, classificandone il suo livello di accettabilità e di non accettabilità, cercando infine di definire come sia possibile portare eventuali rischi non accettabili a un livello di accettabilità. Nelle due tabelle 3.6.2.15 e 3.6.2.16 si vede una presenza del 72,93% di analisi dei rischi IT, elemento formale e comunque complesso, e una registrazione degli incidenti IT del 78,50%; operazione più semplice e comunque utile sia dal punto di vista operativo, al fine di conoscere eventuali punti di debolezza della propria struttura, sia dal punto di vista formale, come richiesto da alcune best practice tra quelle analizzate, in primis la ISO27001 o sistemi basati su Balanced Scorecard.

Tabella 3.6.2.15 – analisi dei rischi IT

	n.	%
Si	458	72,93 %
No	144	22,93 %
Non So	26	4,14 %
	628	100.00 %

Tabella 3.6.2.16 – registrazione incidenti IT

	n.	%
Si	493	78,50 %
No	111	17,68 %
Non So	24	3,82 %
	628	100.00 %

Q17 - Quante ore di formazione annue eroga l'azienda su temi di Information Technology?

Il valore modale si attesta in un intervallo di 11-20 ore di formazione su temi IT per persona. Il dato ragguardato vede un valore di circa 1-2 ore mese di training a persona, dato ragionevole e non elevato, in considerazione del fatto che rappresenta un concetto di formazione IT generica, che include anche quella per l'utilizzo di procedure e strumenti di lavoro, non solamente la tradizionale forma di training in aula. A tal proposito, con riferimento alla piramide dell'apprendimento

(Capitolo 2) si sottolinea come le tradizionali lezioni d'aula, a bassa efficacia, sono sempre più spesso accompagnate da sessioni di sperimentazione dei concetti appresi (c.d. *learning by doing*), metodologie frequentemente adottate nei sistemi di finanziamento della formazione aziendale, come accade ad esempio per i piani finanziati da alcune associazioni di categoria come Confindustria.

Tabella 3.6.2.17 – Ore di formazione annue IT

	n.	%
Meno di 10 ore	247	39,33 %
Da 11 a 20 ore	331	52,71 %
Più di 20 h	36	5,73 %
Non So	14	2,23 %
	628	100.00 %

Q18 - Quanti incidenti IT si verificano orientativamente in un anno? Per incidenti IT si intende: perdita, distruzione o inaccessibilità dei dati, dovuti a virus, guasti di apparecchiature, errato intervento umano colposo o volontario, o fuga di dati verso l'esterno.

La tabella 3.6.2.18 mostra la distribuzione di frequenza del numero di incidenti IT, questo dato va analizzato in correlazione con altre variabili (cap. 3.6.3). Una breve considerazione, la moda statistica rilevata è sulla classe di zero incidenti, questa casistica comprende sia realtà per le quali il dato viene registrato, sia realtà che non registrano affatto gli incidenti IT.

Tabella 3.6.2.18 – Numero di incidenti IT

	n.	%
0	277	44,11 %
Da 1 a 5	149	23,73 %
Da 6 a 10	87	13,85 %
Oltre i 10	3	0,48 %
Non So	112	17,83 %
	628	100.00 %

Q19 - Una fuga di informazioni riservate dall'azienda avrebbe gravi ripercussioni sulla vita e sulla reputazione dell'azienda

Nella tabella 3.6.2.19 l'opinione sull'effetto della fuga di informazioni riservate. Si nota la generale consapevolezza su questo aspetto. I manager quindi, per oltre l'84% sono consapevoli e convinti dell'impatto di un *data-breach* sulla reputazione dell'azienda. A questo risultato ha contribuito la discussione degli ultimi anni sulla gestione dei dai dati personali e l'introduzione della relativa normativa GDPR, si veda anche domanda Q20.

Tabella 3.6.2.19 – Ripercussioni fuga informazioni

	n.	%
1 – CA	307	48,89 %
2 – PA	225	35,83 %
3 – NAD	60	9,55 %
4 – PD	36	5,73 %
5 - CD	0	0 %
	628	100.00 %

Q20 - La nostra azienda si è adeguata pienamente alla normativa relativa al GDPR

L'entrata in vigore della normativa sul General Data Protection Regulation è stata proceduta da intense attività di sensibilizzazione. È inoltre emersa la consapevolezza del cambio di paradigma della normativa che è diventata più concreta, con verifiche più rigorose, con sanzioni particolarmente impegnative. La quasi totalità delle aziende ha preso iniziative in proposito, pertanto i rispondenti, con ogni probabilità, hanno sentito di qualcuna di queste iniziative in azienda. È giustificabile quindi che chi sia stato coinvolto in iniziative legate al GDPR consideri l'argomento chiuso.

Tabella 3.6.2.20 – Adeguamento GDPR

	n.	%
1 – CA	343	54,62 %
2 – PA	266	42,36 %
3 – NAD	17	2,71 %
4 – PD	2	0,32 %
5 - CD	0	0 %
	628	100.00 %

3.6.3 Analisi correlate

Trattandosi di una raccolta dati di tipo prevalentemente qualitativo, sono state costruite delle matrici bidimensionali di distribuzione delle frequenze da cui raccogliere le convergenze dati a supporto delle conferme delle ipotesi di ricerca.

Queste matrici in statistica sono note come *matrici di contingenza*; le colonne coi totali di riga e colonna sono le distribuzioni marginali delle variabili rappresentate, da queste sono ricavati i valori relativi rappresentati nelle matrici colorate in funzione della percentuale. l'aspetto interessante ai fini della correlazione è che l'assenza di correlazione si può evincere dal fatto che la frequenza congiunta è pari al prodotto delle frequenze marginali di riga e colonna in quanto la distribuzione è uguale a quelle subordinate. Per le analisi congiunte sviluppate non appare per nessuna matrice la condizione di indipendenza pertanto tutte mostrano dei legami di correlazione.

Come per l'analisi effettuata sulle variabili singole, nelle tabelle che seguono vengono analizzati dei dati qualitativi raccolti con le domande del questionario strutturate secondo una scala di Likert. La legenda della scala, di seguito riportata, richiama la notazione inglese.

CA	*Completely agree*	*Completamente d'accordo*
PA	*Partially Agree*	*Parzialmente d'accordo*
NAD	*Neither Agree nor Disagree*	*Né in accordo né in disaccordo*
PD	*Partially Disagree*	*Parzialmente in disaccordo*
CD	*Completely Disagree*	*Completamente in disaccordo*

In questa sezione verranno messe in relazione tra loro variabili di tipo qualitativo al fine di ottenere le indicazioni necessarie a rispondere alle ipotesi della ricerca. Il modo migliore per trarre conclusioni informative è di utilizzare matrici che legano le distribuzioni delle frequenze delle variabili statistiche in modo di poter individuare aree di correlazione altrimenti non evidenziabili.

Per poter fare questo in maniera agevole è stato realizzato un database multidimensionale con le informazioni raccolte dal questionario.

Un database multidimensionale è tipico dei sistemi di business intelligence, in quanto consentono di esplorare complesse moli di dati da diverse dimensioni di analisi e a diversi livelli di aggregazione.

Come vanno lette le matrici. Il sistema multidimensionale distribuisce le frequenze relative delle due variabili statistiche in analisi; ad esempio data la variabile X, generata dalla combinazione della domanda D1 e D2, il valore x_{ij} della matrice rappresenta la frequenza relativa della combinazione $D1_iD2_j$. Per esemplificare ulteriormente, con riferimento alla tabella 3.6.4.1, la cella con coordinate x = 4-PA e y = 5-PA che contiene il valore 17,99 significa che il 17,99% dei rispondenti alle domande Q4-Q5 hanno risposto PA a Q4 e CA per Q5.

I test di associazione tra variabili categoriali sono poco utilizzati in statistica e portano a risultati poco soddisfacenti perché queste variabili sono caratterizzate da modalità caratterizzate da una forte autonomia semantica, ovvero il grado in cui l'etichetta di una modalità assume significato senza dover ricorrere all'etichetta della variabile. Per questa ragione si tende piuttosto a parlare di attrazione/repulsione fra singole modalità della variabile.

Per questo motivo la parte di evidenza è stata colta con riguardo alla distribuzione delle frequenze relative co-variate, tabella di contingenza, individuando dove sono emersi i maggiori legami congiunti sulla parte della scala di Likert di interesse.

3.6.4 Analisi correlate a supporto dell'ipotesi H1

H1 – Adottare un sistema di gestione della sicurezza IT e / o delle best practice in questo ambito comporta una maggiore percezione della sicurezza IT dell'azienda da parte del management.

Per valutare questa ipotesi sono state correlate le seguenti variabili statistiche:

- (Q4, Q5) (Q11, Q5) (Q4, Q7) (Q4, Q9) (Q4, Q12) (Q4, Q13) (Q6, Q5) (Q20, Q9).

Di seguito le matrici con le distribuzioni co-variate delle frequenze relative degli otto casi presi in esame:

Legame 1

Q4 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

Q5- La presenza di un sistema di gestione certificato suggerisce un livello adeguato di sicurezza delle informazioni aziendali

Tabella 3.6.4.1 – Correlazione Q4-Q5

Q4-Q5	1-CD	2-PD	3-NAD	4-PA	5-CA	TOTAL
1-CD		1,75	0,32	14,17	0,32	17
2-PD		1,75	0,16	14,01	0,48	16
3-NAD		0,16	0,00	2,07	1,59	4
4-PA		0,16	0,48	5,89	8,12	15
5-CA		0,16	0,16	17,99	30,25	49
TOTAL	0	4	1	54	41	100

La moda statistica della distribuzione bivariata ha una frequenza del 30,25% sulla combinazione CA/CA, la sottomatrice 2x2 che esprime un legame forte raccoglie il 62,26 % delle risposte del questionario, quindi possiamo considerare un forte legame tra l'esistenza di best practice di gestione IT e la percezione di un adeguato livello di sicurezza.

Legame 2

Q11 - La sicurezza IT è uno dei fattori in cui la nostra azienda investe molto Completamente d'accordo

Q5- La presenza di un sistema di gestione certificato suggerisce un livello adeguato di sicurezza delle informazioni aziendali

Tabella 3.6.4.2 – Correlazione Q11-Q5

Q11-Q5	1-CD	2-PD	3-NAD	4-PA	5-CA	TOTAL
1-CD		0,00	0,00	1,11	0,48	2
2-PD		0,00	0,00	1,91	0,48	2
3-NAD		0,48	0,16	11,15	4,78	17
4-PA		2,87	0,32	21,66	7,32	32
5-CA		0,64	0,64	18,31	27,71	47
TOTAL	0	4	1	54	41	100

La moda statistica della distribuzione bivariata ha una frequenza del 27,71% sulla combinazione CA/CA, la sottomatrice 2x2 che esprime un legame forte, raccoglie il 75 % delle risposte del questionario.

Possiamo quindi confermare il forte legame tra l'esistenza di investimenti importanti in sicurezza IT e la presenza di un sistema di gestione certificato o l'adozione di best practice. I due tipi di azione non sono aprioristicamente correlati, l'esistenza di un legame segnala un comportamento virtuoso che beneficia della consapevolezza del ruolo dell'IT nelle aziende secondo quanto emerso nell'analisi della letteratura.

Legame 3.

Q4 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

Q7 - L'adozione di un sistema certificato di gestione della sicurezza delle informazioni ha comportato anche un beneficio di immagine e commerciale

Tabella 3.6.4.3 – Correlazione Q4-Q7

Q4-Q7	1-CD	2-PD	3-NAD	4-PA	5-CA	TOTAL
1-CD		2,87	12,42	0,80	0,48	17
2-PD		3,50	12,42	0,16	0,32	16
3-NAD				3,34	0,48	4
4-PA		0,16	0,32	12,74	1,43	15
5-CA				40,76	7,80	49
TOTAL	0	7	25	58	11	100

La moda statistica della distribuzione bivariata ha una frequenza del 40,76% sulla combinazione CA/PA, la sottomatrice 2x2 che esprime un legame forte, raccoglie il 62,74 % delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte tra la presenza di un sistema di gestione certificato o di best practice e l'ottenimento di benefici che vadano oltre l'aspetto della sola sicurezza, come benefici di immagine commerciale o in genere di reputazione.

Con l'emergere dei paradigmi di valorizzazione del ruolo dell'IT nell'economia del business, questo aspetto potrebbe essere meglio sviluppato e valorizzato dalle aziende.

Legame 4

Q4 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

Q9 - Le informazioni e i dati aziendali sono estremamente importanti per i risultati della nostra azienda.

Tabella 3.6.4.4 – Correlazione Q4-Q9

Q4-Q9	1-CD	2-PD	3-NAD	4-PA	5-CA	TOTAL
1-CD			1,27	5,89	9,39	17
2-PD			0,48	6,85	9,08	16
3-NAD				2,07	1,75	4
4-PA			0,16	7,32	7,17	15
5-CA			0,80	22,29	25,48	49
TOTAL	0	0	3	44	53	100

La moda statistica della distribuzione bivariata ha una frequenza del 40,76% sulla combinazione CA/CA, la sottomatrice 2x2 che esprime un legame forte, raccoglie il 62,26% delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte tra la presenza di un sistema di gestione certificato o di best practice e la consapevolezza dell'importanza di dati e informazioni al fine del risultato aziendale.

Legame 5

Q4 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

Q12 - Ritengo che il personale dell'azienda sia adeguatamente preparato al corretto utilizzo dell'informatica

Tabella 3.6.4.5 – Correlazione Q4-Q12

Q4-Q12	1-CD	2-PD	3-NAD	4-PA	5-CA	TOTAL
1-CD	1,43	4,46	5,89	4,62	0,16	17
2-PD	2,07	5,73	6,37	2,07	0,16	16
3-NAD	0,16	1,43	1,11	0,96	0,16	4
4-PA		0,16		2,23	12,26	15
5-CA		0,32	0,16	8,60	39,49	49
TOTAL	4	12	14	18	52	100

La moda statistica della distribuzione bivariata ha una frequenza del 39,49% sulla combinazione CA/CA, la sottomatrice 2x2 che esprime un legame forte, raccoglie il 62,58 % delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte tra la presenza di un sistema di gestione certificato o di best practice e la presenza di personale dell'aziende adeguatamente preparato nelle tecnologie IT.

Legame 6

Q4 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

Q13 - Esistono dei servizi IT in uso all'azienda e che devono essere sempre garantiti?

Tabella 3.6.4.6 – Correlazione Q4-Q13

Q4-Q13	No	Si	TOTAL
1-CD	4,30	12,26	17
2-PD	2,55	13,85	16
3-NAD	0,80	3,03	4
4-PA	1,11	13,54	15
5-CA	3,82	44,75	49
TOTAL	13	87	100

La moda statistica della distribuzione bivariata ha una frequenza del 44,75% sulla combinazione CA/Si, la sottomatrice 1x2 che esprime un legame forte, raccoglie il 58,28% delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte tra la presenza di un sistema di gestione certificato o di best practice e l'idea che ci debbano essere dei servizi IT sempre garantiti. Metodologicamente la questione è corretta, è molto frequente che l'esigenza di avere servizi garantiti faccia emergere la necessità di adottare dei sistemi di practice o di gestione che ne abbiano a carico l'organizzazione in maniera metodologicamente appropriata.

Legame 7

Q6 - L'azienda ha adottato un sistema di gestione delle informazioni con l'obiettivo di aumentare il livello di sicurezza informatica

Q5- La presenza di un sistema di gestione certificato suggerisce un livello adeguato di sicurezza delle informazioni aziendali

Tabella 3.6.4.7 – Correlazione Q6-Q5

Q6-Q5	1-CD	2-PD	3-NAD	4-PA	5-CA	TOTAL
1-CD			1,27	5,89	9,39	17
2-PD			0,48	6,85	9,08	16
3-NAD				2,07	1,75	4
4-PA			0,16	7,32	7,17	15
5-CA			0,80	22,29	25,48	49
TOTAL	0	0	3	44	53	100

La moda statistica della distribuzione bivariata ha una frequenza del 25,48% sulla combinazione CA/CA, la sottomatrice 2x2 che esprime un legame forte, raccoglie il 62,26% delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte tra l'obiettivo di sicurezza legato all'adozione di un sistema di gestione o di best practice e la percezione di sicurezza che ne consegue.

Legame 8

Q9 - Le informazioni e i dati aziendali sono estremamente importanti per i risultati della nostra azienda.

Q20 - La nostra azienda si è adeguata pienamente alla normativa relativa al GDPR

Tabella 3.6.4.8 – Correlazione Q20-Q9

Q20-Q9	1-CD	2-PD	3-NAD	4-PA	5-CA	TOTAL
1-CD						0
2-PD				0,16	0,16	0
3-NAD				1,75	0,96	3
4-PA			1,43	21,18	19,75	42
5-CA			1,27	21,34	32,01	55
TOTAL	0	0	3	44	53	100

La moda statistica della distribuzione bimodale ha una frequenza del 32,01% sulla combinazione CA/CA, la sottomatrice 2x2 che esprime un legame forte, raccoglie il 94,27% delle risposte del questionario. Possiamo quindi assumere un legame decisamente forte tra la consapevolezza dell'importanza delle informazioni aziendali e la *compliance* con la normativa GDPR, anche se questa è legata alla gestione di un sottoinsieme dei dati aziendali, quelli di carattere personale.

3.6.5 Analisi correlate a supporto dell'ipotesi H2

H2 – Adottare un sistema di gestione della sicurezza IT e / o delle best practice in questo ambito, riduce il numero di incidenti IT in una azienda. Per valutare questa ipotesi sono state correlate le seguenti variabili statistiche:

- (Q4, Q18) (Q11, Q18) (Q11, Q13) (Q3, Q18) (Q4, Q14) (Q4, Q15) (Q4, Q16).

Di seguito le matrici con le distribuzioni co-variate delle frequenze relative dei sette casi presi in esame:

Legame 1

Q4 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

Q18 - Quanti incidenti IT si verificano orientativamente in un anno? Per incidenti IT si intende: perdita, distruzione o inaccessibilità dei dati, dovuti a virus, guasti di apparecchiature, errato intervento umano colposo o volontario, o fuga di dati verso l'esterno.

Tabella 3.6.5.1 – Correlazione Q4-Q18

Q4-Q18	0	1	2	3	4	TOTAL
1-CD	0,16	4,46	5,10	0,16	6,69	17
2-PD		4,94	4,94		6,53	16
3-NAD	0,16	0,64	0,80	0,16	2,07	4
4-PA	8,44	4,78	0,64	0,16	0,64	15
5-CA	35,35	8,92	2,39		1,91	49
TOTAL	44,11	23,73	13,85	0,48	17,83	100

La moda statistica della distribuzione bivariata ha una frequenza del 35,35% sulla combinazione CA/0 Incidenti IT, la sottomatrice 2x2 che esprime una correlazione forte, raccoglie il 57,78 % delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte, di tipo inverso, tra la presenza di un sistema di gestione certificato o di best practice e il numero di incidenti IT.

Legame 2

Q11 - La sicurezza IT è uno dei fattori in cui la nostra azienda investe molto

Q18 - Quanti incidenti IT si verificano orientativamente in un anno? Per incidenti IT si intende: perdita, distruzione o inaccessibilità dei dati, dovuti a virus, guasti di apparecchiature, errato intervento umano colposo o volontario, o fuga di dati verso l'esterno.

Tabella 3.6.5.2 – Correlazione Q11-Q18

Q11-Q18	0	1	2	3	4	TOTAL
1-CD	0,16	0,32	0,80		0,32	2
2-PD	0,16	0,32	1,11		0,80	2
3-NAD	2,87	6,05	3,82	0,16	3,66	17
4-PA	5,57	9,08	7,01	0,32	10,19	32
5-CA	35,35	7,96	1,11		2,87	47
TOTAL	44,11	23,73	13,85	0,48	17,83	100

La moda statistica della distribuzione bivariata ha una frequenza del 35,35% sulla combinazione CA/0 Incidenti IT, la sottomatrice 2x2 che esprime un legame forte, raccoglie il 57,96 % delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte (di tipo inverso, chiaramente) tra la percezione che gli investimenti IT in Sicurezza siano importanti per l'azienda e il numero di incidenti IT.

Legame 3

Q11 - La sicurezza IT è uno dei fattori in cui la nostra azienda investe molto

Q13 - Esistono dei servizi IT in uso all'azienda e che devono essere sempre garantiti?

Tabella 3.6.5.3 – Correlazione Q11-Q13

Q11-Q13	No	Si	TOTAL
1-CD	1,27	0,32	2
2-PD	1,27	1,11	2
3-NAD	3,98	12,58	17
4-PA	4,94	27,23	32
5-CA	1,11	46,18	47
TOTAL	12,58	87,42	100

La moda statistica della distribuzione bivariata ha una frequenza del 46,18% sulla combinazione CA/Si, la sottomatrice 1x2 che esprime un legame forte, raccoglie il 73,41% delle risposte del questionario. Possiamo quindi assumere un legame forte tra la percezione che gli investimenti IT in

sicurezza siano importanti per l'azienda e la presenza in azienda di servizi IT che devono essere sempre garantiti.

Legame 4

Q3 - L'azienda in cui lavoro è fortemente informatizzata

Q18 - Quanti incidenti IT si verificano orientativamente in un anno? Per incidenti IT si intende: perdita, distruzione o inaccessibilità dei dati, dovuti a virus, guasti di apparecchiature, errato intervento umano colposo o volontario, o fuga di dati verso l'esterno.

Tabella 3.6.5.4 – Correlazione Q3-Q18

Q3-Q18	0	1	2	3	4	TOTAL
5-CA	30,73	13,69	5,57	0,32	12,58	63
4-PA	12,90	9,08	5,57		3,98	32
3-NAD		0,80	2,23	0,16	0,64	4
2-PD	0,48	0,16	0,48		0,64	2
1-CD						0
TOTAL	44,11	23,73	13,85	0,48	17,83	100

La moda statistica della distribuzione bivariata ha una frequenza del 30,73% sulla combinazione CA/0 Incidenti IT, la sottomatrice 2x2 che esprime un legame forte, raccoglie il 66,40 % delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte tra il livello di informatizzazione che viene percepito dall'azienda e il basso numero di incidenti IT.

Legame 5

Q4 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

Q14 - Esiste un regolamento IT aziendale formalizzato?

Tabella 3.6.5.5 – Correlazione Q4-Q14

Q4-Q14	No	Si	TOTAL
1-CD	5,25	11,31	17
2-PD	3,82	12,58	16
3-NAD	0,96	2,87	4
4-PA	0,80	13,85	15
5-CA	2,55	46,02	49
TOTAL	13,38	86,62	100

La moda statistica della distribuzione bivariata ha una frequenza del 46,02% sulla combinazione CA/Esistenza di un regolamento IT aziendale. La sottomatrice 1x2 che esprime un legame forte, raccoglie il 59,87% delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte tra l'esistenza di un sistema di gestione IT o di best practice e la presenza di un regolamento IT.

Legame 6

Q4 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

Q15 - Viene eseguita in azienda una analisi periodica dei rischi IT?

Tabella 3.6.5.6 – Correlazione Q4-Q15

Q4-Q15	No	Si	Non So	TOTAL
1-CD	9,87	4,62	2,07	17
2-PD	9,71	5,57	1,11	16
3-NAD	1,43	1,75	0,64	4
4-PA	0,16	14,33	0,16	15
5-CA	1,75	46,66	0,16	49
TOTAL	22,93	72,93	4,14	100

La moda statistica della distribuzione bivariata ha una frequenza del 46,66% sulla combinazione CA/Analisi periodica dei rischi IT. La sottomatrice 1x2 che esprime un legame forte, raccoglie il 60,99% delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte tra l'esistenza di un sistema di gestione IT o di best practice e la presenza di un regolamento IT.

Legame 7

Q4 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

Q16 - In azienda vengono registrati gli incidenti IT?

Tabella 3.6.5.7 – Correlazione Q4-Q16

Q4-Q16	No	Si	Non So	TOTAL
1-CD	7,17	7,32	2,07	17
2-PD	6,69	8,92	0,80	16

3-NAD	2,07	1,27	0,48	4
4-PA	0,48	14,01	0,16	15
5-CA	1,27	46,97	0,32	49
TOTAL	17,68	78,50	3,82	100

La moda statistica della distribuzione bivariata ha una frequenza del 46,97% sulla combinazione CA/Registrazione incidenti IT. La sottomatrice 1x2 che esprime un legame forte, raccoglie il 60,98% delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte tra l'esistenza di un sistema di gestione IT o di best practice e la pratica di registrazione degli incidenti IT.

3.6.6 Analisi correlate a supporto dell'ipotesi H3

H3 – Esiste un legame tra le ore di formazione IT erogate e la percezione del livello di sicurezza informatica da parte del management.

Per valutare questa ipotesi sono state correlate le seguenti variabili statistiche:

- (Q17, Q5) (Q17, Q12) (Q17, Q19) (Q1, Q17) (Q17, Q6).

Di seguito le matrici con le distribuzioni co-variate delle frequenze relative dei cinque casi presi in esame:

Legame 1

Q17 - Quante ore di formazione annue eroga l'azienda su temi di Information Technology? (Media annua per persona)

Q5- La presenza di un sistema di gestione certificato suggerisce un livello adeguato di sicurezza delle informazioni aziendali

Tabella 3.6.6.1 – Correlazione Q5-Q17

Q5-Q17	1	2	3	4	TOTAL
1-CD					0
2-PD	3,66	0,32			4
3-NAD	0,48	0,48	0,16		1
4-PA	31,69	19,27	2,07	1,11	54
5-CA	3,50	32,64	3,50	1,11	41
TOTAL	39	53	6	2	100

La moda statistica della distribuzione bivariata ha una frequenza del 32,64% sulla combinazione CA/Ore di formazione. La sottomatrice 2x2 che esprime un legame forte, raccoglie il 87,10% delle risposte del questionario. Possiamo quindi assumere un legame molto forte tra la presenza di una attività di formazione in ambito IT strutturata e la percezione che un sistema di gestione IT sia garanzia di adeguata sicurezza per le informazioni aziendali.

Legame 2

Q17 - Quante ore di formazione annue eroga l'azienda su temi di Information Technology? (Media annua per persona)

Q12 - Ritengo che il personale dell'azienda sia adeguatamente preparato al corretto utilizzo dell'informatica Completamente d'accordo

Tabella 3.6.6.2 – Correlazione Q12-Q17

Q12-Q17	1	2	3	4	TOTAL
1-CD	3,66				4
2-PD	11,78	0,32			12
3-NAD	13,54				14
4-PA	8,28	8,76	1,11	0,32	18
5-CA	2,07	43,63	4,62	1,91	52
TOTAL	39	53	6	2	100

La moda statistica della distribuzione bivariata ha una frequenza del 43,63% sulla combinazione CA/fascia 2 delle Ore di formazione. La sottomatrice 2x2 che esprime un legame forte, raccoglie il 62,74% delle risposte del questionario. Possiamo quindi assumere un legame sufficientemente forte tra la presenza di una attività di formazione in ambito IT strutturata e la percezione di una adeguata formazzine IT del personale dell'aziende.

Legame 3

Q17 - Quante ore di formazione annue eroga l'azienda su temi di Information Technology? (Media annua per persona)

Q19 - Una fuga di informazioni riservate dall'azienda avrebbe gravi ripercussioni sulla vita e sulla reputazione dell'azienda.

Tabella 3.6.6.3 – Correlazione Q19-Q17

Q19-Q17	1	2	3	4	TOTAL
1-CD	0,00	0,00	0,00	0,00	0
2-PD	2,23	3,34	0,16	0,00	6
3-NAD	4,94	3,98	0,32	0,32	10
4-PA	18,95	14,65	1,43	0,80	36
5-CA	13,22	30,73	3,82	1,11	49
TOTAL	39	53	6	2	100

La moda statistica della distribuzione bivariata ha una frequenza del 30,732% sulla combinazione CA/fascia 2 delle Ore di formazione. La sottomatrice 2x2 che esprime un legame forte, raccoglie il 77,55% delle risposte del questionario. Possiamo quindi assumere un legame forte tra la presenza di una attività di formazione in ambito IT strutturata e la percezione che una fuga di informazioni riservate possa avere ripercussioni negative sulla reputazione dell'azienda.

Legame 4

Q1 - Nel mio lavoro utilizzo in maniera intensa i sistemi informatici

Q17 - Quante ore di formazione annue eroga l'azienda su temi di Information Technology? (Media annua per persona)

Tabella 3.6.6.4 – Correlazione Q1-Q17

Q1-Q17	1	2	3	4	TOTAL
1-CD					0
2-PD	0,32	0,48			1
3-NAD	0,64	0,64			1
4-PA	5,10	6,05	0,80	0,32	12
5-CA	33,28	45,54	4,94	1,91	86
TOTAL	39	53	6	2	100

La moda statistica della distribuzione bivariata ha una frequenza del 45,54% sulla combinazione CA/fascia 2 delle Ore di formazione. La sottomatrice 2x2 che esprime una correlazione forte, raccoglie il 89,97% delle risposte del questionario. Possiamo quindi assumere un legame molto forte tra un tipo di lavoro molto IT – intensive e la presenza di una attività di formazione in ambito IT.

Legame 5

Q17 - Quante ore di formazione annue eroga l'azienda su temi di Information Technology? (Media annua per persona)

Q6 - L'azienda ha adottato un sistema di gestione delle informazioni con l'obiettivo di aumentare il livello di sicurezza informatica

Tabella 3.6.6.5 – Correlazione Q6-Q17

Q6-Q17	1	2	3	4	TOTAL
1-CD	0,16	0,00	0,00	0,00	0
2-PD	0,32	0,32	0,00	0,00	1
3-NAD	2,07	0,00	0,00	0,00	2
4-PA	13,54	12,26	0,80	1,11	28
5-CA	23,25	40,13	4,94	1,11	69
TOTAL	39	53	6	2	100

La moda statistica della distribuzione bivariata ha una frequenza del 40,13% sulla combinazione CA/fascia 2 delle Ore di formazione. La sottomatrice 2x2 che esprime un legame forte, raccoglie il 89,17% delle risposte del questionario. Possiamo quindi assumere un legame molto forte tra la presenza di una attività di formazione in ambito IT strutturata e la l'idea che l'adozione di sistemi di best practice sia legato all'incremento della sicurezza IT.

3.6.7 Analisi correlate a supporto dell'ipotesi H4

H4 – Esiste una correlazione inversa tra il numero di incidenti IT e le ore di formazione IT erogate.

Per valutare questa ipotesi sono state correlate le seguenti variabili statistiche:

- (Q17, Q18) (Q17, Q2) (Q17, Q3).

Di seguito le matrici con le distribuzioni co-variate delle frequenze relative dei cinque casi presi in esame:

Legame 1

Q17 - Quante ore di formazione annue eroga l'azienda su temi di Information Technology? (Media annua per persona)

Q18 - Quanti incidenti IT si verificano orientativamente in un anno? Per incidenti IT si intende: perdita, distruzione o inaccessibilità dei dati, dovuti a virus, guasti di apparecchiature, errato intervento umano colposo o volontario, o fuga di dati verso l'esterno.

Tabella 3.6.7.1 – Correlazione Q17-Q18

Q17-Q18	0	1	2	3	4	TOTAL
1	1,11	10,83	11,15	0,48	15,76	39
2	36,94	11,46	2,71		1,59	53
3	4,46	0,80			0,48	6
4	1,59	0,64				2
TOTAL	44	24	14	0	18	100

La moda statistica della distribuzione bivariata ha una frequenza del 36,94% sulla combinazione 0 Incidenti IT/fascia 2 delle Ore di formazione. La sottomatrice 2x2 che esprime un legame forte, raccoglie il 60,35% delle risposte del questionario. Possiamo quindi assumere un legame, inverso

ovviamente, sufficientemente forte tra la presenza di una attività di formazione in ambito IT strutturata e il verificarsi di incidenti IT.

Legame 2

Q17 - Quante ore di formazione annue eroga l'azienda su temi di Information Technology? (Media annua per persona)

Q2 - Senza l'uso di supporto informatico sarebbe difficile svolgere il mio lavoro

Tabella 3.6.7.2 – Correlazione Q2-Q17

Q2-Q17	1	2	3	4	TOTAL
1-CD					0
2-PD	0,32	0,16			0
3-NAD	0,64	1,11			2
4-PA	3,82	5,25	0,64	0,48	10
5-CA	34,55	46,18	5,10	1,75	88
TOTAL	39	53	6	2	100

La moda statistica della distribuzione bivariata ha una frequenza del 46,18% sulla combinazione CA/fascia 2 delle Ore di formazione. La sottomatrice 2x2 che esprime un legame forte, raccoglie il 89,81% delle risposte del questionario. Possiamo quindi assumere un legame molto forte tra la presenza di una attività di formazione in ambito IT strutturata e la l'idea possa essere molto difficile svolgere la propria attività senza un adeguato supporto informatico.

Legame 3

Q17 - Quante ore di formazione annue eroga l'azienda su temi di Information Technology? (Media annua per persona)

Q3 - L'azienda in cui lavoro è fortemente informatizzata

Tabella 3.6.7.3 – Correlazione Q17-Q3

Q17 – Q3	1	2	3	4	TOTAL
1-CD					0
2-PD	0,64	1,11			2
3-NAD	2,07	1,75			4
4-PA	13,54	15,29	1,91	0,80	32
5-CA	23,09	34,55	3,82	1,43	63
TOTAL	39	53	6	2	100

La moda statistica della distribuzione bivariata ha una frequenza del 34,55% sulla combinazione CA/fascia 2 delle Ore di formazione. La sottomatrice 2x2 che esprime un legame forte, raccoglie il 86,46% delle risposte del questionario. Possiamo quindi assumere un legame molto forte tra la presenza di una attività di formazione in ambito IT strutturata e la l'idea che l'azienda abbia un forte livello di informatizzazione.

4 Risultati

4.1 Analisi dei risultati

Di seguito il riepilogo dell'analisi dell'attrazione tra singole modalità, generate dalle tabelle di contingenza delle variabili indicate.

Tabella 4.1.1

Legame	Var.1	Modalità Var.1	Var.2	Modalità Var.2	Freq.	Legame
H1 – 1	Q4	PA-CA	Q5	PA-CA	62,26 %	MF
H1 – 2	Q11	PA-CA	Q5	PA-CA	75,00 %	F
H1 – 3	Q4	PA-CA	Q7	PA-CA	62,74 %	MF
H1 – 4	Q4	PA-CA	Q9	PA-CA	62,26 %	MF
H1 – 5	Q4	PA-CA	Q12	PA-CA	62,58 %	MF
H1 – 6	Q4	PA-CA	Q13	Si	58,28 %	M
H1 – 7	Q6	PA-CA	Q5	PA-CA	62,26 %	MF
H1 – 8	Q9	PA-CA	Q20	PA-CA	94,27 %	F
H2 – 1	Q4	PA-CA	Q18	0-1	57,48 %	M
H2 – 2	Q11	PA-CA	Q18	0-1	57,96 %	M
H2 – 3	Q11	PA-CA	Q13	Si	73,41 %	MF
H2 – 4	Q3	PA-CA	Q18	0-1	66,40 %	MF
H2 – 5	Q4	PA-CA	Q14	Si	59,87 %	M
H2 – 6	Q4	PA-CA	Q15	Si	60,99 %	MF
H2 – 7	Q4	PA-CA	Q16	Si	60,98 %	MF
H3 – 1	Q5	PA-CA	Q17	1-2	87,10 %	F
H3 – 2	Q12	PA-CA	Q17	1-2	62,74 %	MF
H3 – 3	Q19	PA-CA	Q17	1-2	77,55 %	F
H3 – 4	Q1	PA-CA	Q17	1-2	89,97 %	F
H3 – 5	Q6	PA-CA	Q17	1-2	89,17 %	F
H4 – 1	Q17	1-2	Q18	0-1	60,35 %	MF
H4 – 2	Q2	PA-CA	Q17	1-2	89,81 %	F
H4 – 3	Q3	PA-CA	Q17	1-2	86,46 %	F

Var.1	Variabile 1 rappresentata nella matrice di contingenza
Modalità Var.1	Elenco delle modalità della variabile Var.1 usate per l'attrazione
Var.2	Variabile 2 rappresentata nella matrice di contingenza
Modalità Var.2	Elenco delle modalità della variabile Var.1 usate per l'attrazione
Freq.	Frequenza delle modalità combinate
Legame	50-60 Legame Medio (Si tratta di valori convenzionali)

60-75	Legame Medio Forte
>75	Legame Forte

Sulla base dei dati della popolazione, delle elaborazioni fatte sul campione di dati raccolto tramite la somministrazione di un questionario, emergono le conferme alle ipotesi fatte nell'ambito del disegno della ricerca:

H1 Tutte le otto matrici della frequenza bivariata tra variabili statistiche qualitative scelte per confermare l'ipotesi H1, esprimono elevati livelli di correlazione (Forte e Medio Forte e Medio) pertanto è possibile affermare che (H1) – *Adottare un sistema di gestione della sicurezza IT e / o delle best practice in questo ambito comporta una maggiore percezione della sicurezza IT dell'azienda da parte del management*.

H2 Tutte le sette matrici di frequenza bivariata tra variabili statistiche qualitative scelte per confermare l'ipotesi H2, esprimono significativi livelli di correlazione (Medio e Medio Forte) pertanto è possibile affermare che (H2) *Adottare un sistema di gestione della sicurezza IT e / o delle best practice in questo ambito, contribuisce a ridurre il numero di incidenti IT in una azienda*.

H3 Tutte le cinque matrici di frequenza bivariata tra variabili statistiche qualitative scelte per confermare l'ipotesi H3, esprimono elevati livelli di correlazione (Forte e Medio Forte) pertanto è possibile affermare che (H3) *Esiste un legame tra le ore di formazione IT erogate e la percezione del livello di sicurezza informatica da parte del management.*

H4 Tutte le tre matrici di frequenza bivariata tra variabili statistiche qualitative scelte per confermare l'ipotesi H4, esprimono elevati livelli di correlazione (Forte e Medio Forte)

pertanto è possibile affermare che (H4) *Esiste una correlazione inversa tra il numero di incidenti IT e le ore di formazione IT erogate.*

4.2 Conclusioni

In un'era in cui c'è una spinta alla digitalizzazione senza precedenti, sia nella vita comune sia nel mondo delle imprese, il ruolo delle tecnologie informatiche è sempre più centrale sia a livello infrastrutturale sia in termini di vantaggio competitivo e di generazione del valore.

Il cambio di paradigma relativo all'ICT implica una importante attenzione alla sicurezza dei dati e informazioni. Questo passaggio passa anche attraverso l'adozione di best practice o di sistemi di gestione per i quali, l'indagine effettuata, conferma il loro positivo effetto nell'ambito della sicurezza ICT, sia che si parli di sicurezza effettiva, basata su metriche e misurazioni oggetti, sia che si parli di sicurezza ICT di tipo "percepito". Lo stesso effetto positivo sulla sicurezza ICT, declinata nelle due modalità già descritte, si manifesta anche con l'adozione di programmi di formazione in area ICT.

5 Discussione

5.1 Riassunto

Il lavoro di ricerca si è basato sull'analisi qualitativa basata dei dati primari raccolti da un questionario di 26 domande, somministrato on-line a un campione di aziende per la maggior parte Italiane e prevalentemente operanti nel settore della produzione e vendita di beni.

L'analisi ha comportato tre fasi:

a) individuazione delle caratteristiche tecnologiche della popolazione delle aziende, questa fase è stata supportata basandosi sui dati dei questionari obbligatori, somministrati periodicamente dall'Istituto Italiano di Statistica, alle imprese italiane e resi disponibili pubblicamente dall'istituto;
b) analisi uni-variata delle variabili statistiche associate alle domande del questionario somministrato nel corso della presente ricerca;
c) analisi co-variata, per coppie, delle variabili statistiche associate alle domande del questionario somministrato nel corso della presente ricerca, selezionate in modo da supportare le affermazioni espresse nelle quattro ipotesi di ricerca. Trattandosi di variabili statistiche qualitative, le forme di correlazione sono state dedotte dalle matrici di distribuzione, ovvero le tabelle di contingenza, e dalle frequenze relative, generate attraverso un sistema di analisi di dati basato su un database di tipo multidimensionale programmato per questo tipo di analisi. Le quattro ipotesi sono state tutte confermate portando alle conclusioni già espresse nel capitolo relativo alle conclusioni.

5.2 Limitazioni

L'obiettivo della ricerca era cercare una possibile conferma dell'esistenza di legami che potessero condurre a giustificare le ipotesi espresse in sede di progettazione. Questo risultato, confermato, apre la possibilità di un nuovo e più ampio insieme di obiettivi di ricerca che, in primis, superi alcune limitazioni di ordine matematico e statistico associato all'utilizzo di variabili qualitative.

Il passaggio a una raccolta dati di tipo quantitativo porterà a maggiori benefici sulla costruzione dei legami qui evidenziati, il tutto però richiederà una maggiore complessità della raccolta dei dati e, soprattutto della loro validazione; in un contesto del genere lo strumento del questionario sarebbe probabilmente meno indicato e sarebbe opportuno operare una raccolta diversa dei dati primari, con un impegno temporale estremamente più lungo, con costi decisamente maggiori e con problematiche da risolvere nell'ambito della riservatezza delle informazioni raccolte.

5.3 Raccomandazioni per ricerche future

L'obiettivo della presente ricerca va anche nella direzione di creare alcune condizioni affinché possano potenzialmente emergere ed essere definiti dei modelli di valutazione sugli investimenti in sicurezza IT. Si ritiene importante cogliere il messaggio confermato nella parte teorica del presente lavoro, ovvero il paradigma che vede il ruolo centrale dell'IT come:

a) elemento di supporto ai processi lungo la catena del valore;

b) elemento di contribuzione alla generazione del valore stesso;

c) elemento di distinzione e di vantaggio competitivo;

d) infrastruttura IT e relativa sicurezza come ambito di competenza del management.

Da questi presupposti si possono imbastire eventuali ricerche sul processo della sicurezza IT che possano uscire dall'ambito puramente tecnologico.

Allegato 1 - Questionario

Di seguito viene riportato il questionario proposto in rete secondo quanto esposto nella parte metodologica. Lo strumento utilizzato fa parte degli strumenti gratuiti forniti da Google e prende il nome di *Google Forms* ©. Vengono riportate le domande proposte, esposte in formato testuale.

Avviso: questo survey fa parte di un progetto di ricerca per una tesi di Ph.D relativa alle percezioni della sicurezza IT nelle aziende con certe caratteristiche. L'ambito è puramente di business & strategy. Il questionario è anonimo e non raccoglie nessun riferimento né dell'azienda, né del rispondente, o alcuno dei suoi dati che possano essere considerati riservati o personali. I Dati verranno usati in modo aggregato all'interno della ricerca.

1 - Dove ha sede l'azienda in cui lavori

- Italia
- Unione Europea Resto del Mondo
- Macro-settore in cui opera l'azienda

2 - Fascia di fatturato

- Inferiore a 1 Milione di €
- Tra 1 e 10 Milioni di €
- Tra 10 e 50 Milioni di €
- Più di 50 Milioni di €

3 - Macro-settore in cui opera l'azienda

- Produzione e/o vendita
- Servizi
- Altro

4 - Numero di dipendenti

- Meno di 10
- da 11 a 25
- da 26 a 100
- Oltre 100

5 - Area di responsabilità del rispondente

- Direzione generale
- Amministrazione, Finanza e Controllo
- Vendite, Marketing
- Acquisti,
- Logistica, Magazzino
- Aree tecniche

- Produzione
- Information Technology

6 - In azienda esiste una struttura che si occupa dell'IT e che fa capo un responsabile formale?

- Si
- No

7 - Nel mio lavoro utilizzo in maniera intensa i sistemi informatici

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

8 - Senza l'uso di supporto informatico sarebbe diffcile svolgere il mio lavoro

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

9 - L'azienda in cui lavoro è fortemente informatizzata

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

10 - L'azienda in cui lavoro adotta un sistema di gestione certificato (es. ISO 27001) o un sistema di best practice (es. ITIL, COBIT) per gestire la sicurezza dei sistemi e/o i processi IT

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

11- La presenza di un sistema di gestione certificato suggerisce un livello adeguato di sicurezza delle informazioni aziendali

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

12 - L'azienda ha adottato un sistema di gestione delle informazioni con l'obiettivo di aumentare il livello di sicurezza informatica

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

13 - L'adozione di un sistema certificato di gestione della sicurezza delle informazioni ha comportato anche un beneficio di immagine e commerciale

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

14 - La sicurezza IT è composta da tre fattori: Integrità, disponibilità e riservatezza. E' compito del management aziendale assicurarsi che le informazioni aziendali siano tutelate in tu i e questi tre ambiti

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

15 - Le informazioni e i dati aziendali sono estremamente importanti per i risultati della nostra azienda.

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

16 - Senza una infrastruttura IT efficiente e sicura non sarebbe per noi possibile fare business

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

17 - La sicurezza IT è uno dei fattori in cui la nostra azienda investe molto Completamente d'accordo

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

18 - Ritengo che il personale dell'azienda sia adeguatamente preparato al corretto utilizzo dell'informatica Completamente d'accordo

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

19 - Esistono dei servizi IT in uso all'azienda e che devono essere sempre garantiti?

- Si
- No
- Non So

20 - Esiste un regolamento IT aziendale formalizzato?

- Si
- No
- Non So

21 - Viene eseguita in azienda una analisi periodica dei rischi IT?

- Si
- No
- Non So

22 - In azienda vengono registrati gli incidenti IT?

- Si
- No
- Non So

23 - Quante ore di formazione annue eroga l'azienda su temi di Information Technology? (Media annua per persona)

- Meno di 10 ore annue
- Tra 10 e 20 ore annue
- Più di 20 ore annue
- Non lo so

24 - Quanti incidenti IT si verificano orientativamente in un anno? Per incidenti IT si intende: perdita, distruzione o inaccessibilità dei dati, dovuti a virus, guasti di apparecchiature, errato intervento umano colposo o volontario, o fuga di dati verso l'esterno.

- Nessun incidente IT nell'ultimo anno
- Da 1 a 5 incidenti IT nell'ultimo anno
- Da 6 a 10 incidenti IT nell'ultimo anno
- Più di dieci incidenti IT nell'ultimo anno
- Non lo so

25 - Una fuga di informazioni riservate dall'azienda avrebbe gravi ripercussioni sulla vita e sulla reputazione dell'azienda.

- Completamente d'accordo

- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

26 - La nostra azienda si è adeguata pienamente alla normativa relativa al GDPR

- Completamente d'accordo
- Parzialmente d'accordo
- Né in accordo né in disaccordo
- Parzialmente in disaccordo
- Completamente in disaccordo

Bibliografia

Accredia, Ente Italiano di Accreditamento, (2020). Retrieved from https://www.accredia.it/banche-dati/ consultato a febbraio 2020.

Basin, D., Capkun, S. (2012). Privacy and security, the research value of publishing attacks. *Communications of the ACM. 55*(11), 22-24.

Bieker, T., Waxemberg, B. (2002). *Sustainability balanced scorecard and business ethics*. Contribution to the 10th International Conference of the Greening of Industry Network, Goteborg.

Bourguignon, A., Malleret, V., Norreklit, H. (2001). *Balanced scorecard versus French tableau de bord: beyond dispute, a cultural and ideological perspective*", Working Papers hal-00597021, HAL.

Bowen, P., Cheung, M., Rohde, F., (2007). *Enhancing IT governance Practices: a model and case study of an organization's effort.*, International Journal of Accounting Information Systems, *8*(3), 191-221.

Calder, A. (2018). *Implementing Information Security based on ISO 27001/ISO 27002*. Van Haren Publishing.

Cavusoglu, H., Mishra, B., Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information systems research. 16*(1), 28-46.

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM. 47*(7), 87-92.

Charette, R.N., (1996). The Mechanics of managing IT risk. *Journal of Information Technology. 11*, 373-378.

Ciriani, S., Perin, P. (2017), Trends in Global ICT Trade. *DigiWorld Economic Journal*, *107*, 17-47.

COBIT5 framework (2012). www.isaca.org [consultato 11 febbraio 2020]

Corradini, A. (2017). *Internet delle cose. Dati, sicurezza e reputazione*. Franco Angeli.

De Geuser, F., Mooraj, S., Oyon, M. (2009). Does the balanced scorecard add value? Empirical evidence on its effect on performance. *European Accounting Review*, *18*(1), 93-122.

Demaire, S.M., Hitt, M.A. (2000). Strategic implications of the information age. Journal of Labour Research. *XXI*(3), 419-429.

Dutta, A., McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*. *45*(1), 67-87.

Eikebrokk, R., Iden, J. (2017). Strategizing IT service management through ITIL implementation: model and empirical test. *Total Quality Management*. *28*(3), 238-265.

Franchi, A., (2017). *Reporting per l'azienda, Fondamenti per l'analisi con la business intelligence.* Amazon Media EU S.à r.l.

Franchi, A. (1997). *Reti telematiche e opportunità per le imprese – Uno studio sulle innovazioni aziendali per il mercato globale*. A cura di AREA Science Park, Trieste.

Gallivan, M.J., Spitler, V.K., Koufaris, M. (2005). Does Information Technology Training Really Matter? A Social Information Processing Analysis of Coworkers' Influence on IT Usage in the Workplace, *Journal of Management Information Systems*, *22*(1), 153-192.

Goble, R., Bier, V.M. (2013). Risk assessment can be a game-changing information technology – but too often it isn't. *Risk Analysis. 33*(11), 1942-1950.

Hadnagy, C. (2011). *Social Engineering – The art of human hacking.* Wiley Publishing, Indianapolis, IN

Humpreys, K.A., Trotman, T.K. (2011). The Balanced Scorecard: The effect of Strategy Information on Performance evaluation judgments. *Journal of management accounting research*. *23*, 81-98.

Iden, J., Eikebrokk, R. (2014). Using the ITIL process reference model for realizing IT governance: An empirical investigation. *Information Systems Management*. *31*, 37-58.

Iden, J., Eikebrokk, R. (2013). Implementing IT Service Management: A systematic literature review. *International Journal of Information Management*. *33*(3), 512-523.

IRM Association, (2011). *Enterprise information systems- Concepts, methodologies, tools and applications*. Business Science Reference, Hershey, NY.

ISO, International Standard Organization (2020) ISO/IEC 27001 Information Security Management. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

ISTAT Istituto Italiano di Statistica (2019). *Banche dati sui censimenti permanenti delle imprese*. dati.istat.it, consultato 2 marzo 2020.

Ittner, C.D., Larcker, D.F., Meyer, M.W., (2003). Subjectivity and the weighting of performance measures: evidence from a balanced scorecard. *The Accounting Review*, *78*(3), pp.725-758.

Jorgenson D., Vu K. (2016). The ICT revolution, world economic growth, and policy issues; *Telecommunications Policy*; *40*(5), 383-397.

Kaplan, R.S., Norton, D.P. (2005). Using the Balanced Scorecard as a strategic management system. *Harvard Business Review*.

Kaplan, R.S., Norton, D.P. (2004). Strategy maps. Converting intangible assets into tangible results. *Harvard Business School Press*.

Kaplan, R.S., Norton, D.P. (1996). Linking the balanced scorecard to strategy. *California Management Review*, *39*(1) Fall 1996.

Khallaf, A., Majdalawieh, M. (2012). Investigating the impact of CIO competencies on IT security performance of the US federal government agencies. *Information Systems Management. 29*, 55-78.

Lancaster, G. (2005). *Research methods in management - A concise introduction to research in management and in business consultancy*. Elsevier.

Lee, D.R. (1988). The evolution of information systems and technologies. *SAM, Advanced Management Journal*. Summer 1988.

Lin, F., Guan, L., Fang, W. (2010). Critical factors affecting the evaluation of information control systems with the COBIT framework. *Emerging Markets Finance & Trade*, *46*(1), 42-55.

Mansir, J., Morin, P. (2018). Poor network hygiene threatens IT security. *Business NH Magazine. Sept 2018, 16-17.*

Marr, B., (2010). What is a modern balanced scorecard? *Management White paper by Advanced Performance Institute*.

Marrone, M., Kolbe, L.M. (2011). Impact of IT service management frameworks on the IT organization. *Business & Information Systems Engineering*, *3*(1), 224-247

McAfee, A., Brynjolfsson, E. (2012). Big Data: the management revolution. *Harvard Business Review*, Oct 2012. 1-9.

Mooraj, S., Oyon, D., Hostettler, D. (1999). The Balanced Scorecard: a Necessary Good or an Unnecessary Evil? *European Management Journal*, *17*(5), Ott.1999.

Negroponte, N. (1996). *Being Digital.* New York, NT, Vintage editor.

Norman, D.A. (1995). *Le cose che ci fanno intelligenti - Il posto della tecnologia nel mondo dell'uomo.* Milano*,* Feltrinelli*.*

Norreklit, H. (2000). *The Balance on the balanced scorecard – A critical analysis of some of its assumptions*. Management Accounting Research, 11, 65-98.

Olson, E.M., Slater, S.F. (2002). The Balanced Scorecard, competitive strategy and performance, *Kelly school of business, Indiana University*.

Pearlson, K.E., Saunders, C.S. (2010). *Managing and Using information systems – a strategic approach*". 4th edition. Hohn Wiley & Sons Inc.

Peppard, J. (2007). The conundrum of IT management. *European Journal of Information Systems*. *16*, 336-345,

Porter, M.E. (2008). The five competitive forces that shape strategy (Reprint*). Harvard Business Review*, Jan. 2008.

Porter, M.E. (1985). *Competitive Advantage*. The Free Press. New York.

Ramakrishnan, A. (2014). Benefits of adopting Information Technology Infrastructure Library (ITIL). *Journal of Management Research*. *14*(3), 159-168.

Reynolds, P., Yetton, P. (2015). Aligning business and IT strategies in multi-business organizations. Journal of Information Technology. *30*, 101–118.

Robertson, J. (2012). Likert-type scales, statistical methods, and effect sizes. *Communications of the ACM*. *55*(5).

Rowley, J., (2007). The wisdom hierarchy: representing of the DIKW hierarchy. *Journal of Information Science*. *33*, 163-180.

Russel, R.H. (2004). The State of IT and business alignment - 2003. *Balanced scorecard collaborative*, Jan.-Feb. 2004.

Segars, A.H., Hendrikson, A.R. (2000). Value, Knowledge, and the human equation: evolution of the information technology function in modern organizations. *Journal of Labour Research*, *XXI*(3), 432-445.

Siponen, M. (2006). Information security standards focus on the existence of process, not its contents. *Communication of the ACM. 49*(8), 97-100.

Soto-Acosta, P., Martinez-Conesa, I., Colomo-Palacios, R. (2010). An Empirical Analysis of the Relationship Between IT Training Sources and IT Value. *Information Systems Management*, *27*(3), 274-283.

Tsiouras, I. (2004). *La sicurezza dell'informzione – Dal sistema di gestione alla sicurezza dei sistemi informatici. Le Norme BS 7799-2 e ISO/IEC 15408 (Common Criteria)*. Milano, Franco Angeli.

Van Gremberger, W., De Haes, S. (2009). *Enterprise governance of Information Technology: achieving strategic alignment and value*. New York, NY:Springer.

Varian, H.R. (1992). *Microeconomic Analysis*, Norton & Company, Inc.

Warfield, D. (2012). Critical infrastructures: IT security and threats from private sector ownership. *Information security journal. 21*, 127-136.

Pagina vuota finale