Rosario Mauro Catanzaro **Manuela Sforza**

CYBERSECURITY

benvenuti nell'era della pandemia informatica

Corso rapido di sopravvivenza per amministratori, dirigenti, manager e ruoli operativi. Cos'è la cybersecurity e perché è una componente fondamentale del business.

Focus

Sanità
Pubblica Amministrazione
Aziende private

RMC Editore

Cybersecurity
benvenuti nell'era della pandemia informatica
Corso rapido di sopravvivenza per amministratori, dirigenti, manager e ruoli operativi. Cos'è la cybersecurity e perché è una componente fondamentale del business.

Autori: Rosario Mauro Catanzaro e Manuela Sforza
ISBN: 979-12-210-1337-5

Progetto grafico curato da Capolettera Studio di Miriana Maugeri

Editore: Rosario Mauro Catanzaro con il marchio “RMC Editore”

Sito web: www.cyberdefenceitalia.com

Finito di stampare nel mese di novembre 2022 da Graffietti Stampati S.n.c. nello stabilimento di Montefiascone (VT) S.S. Umbro Casentinese Km 4,500.

I edizione novembre 2022

Indice

Introduzione

A chi è indirizzato questo libro

Questo libro, destinato sia a ruoli manageriali che operativi, ha lo scopo di fornire un supporto strategico alle amministrazioni che, ormai, si trovano di fronte alla necessità indifferibile di affrontare un problema nuovo, almeno nella sua dimensione, e complesso nella sua risoluzione, **la *cybersecurity* o *sicurezza informatica*, termine che ormai troviamo comunemente utilizzato anche nella sua italica nomenclatura *cybersicurezza*.**

Com'è organizzato

Nel testo, la materia viene affrontata gradualmente, sia a livello strategico che operativo, cercando di evitare, quando possibile, inutili tecnicismi. Il libro è, quindi, una cerniera tra il mondo strategico (governance) e quello operativo che, nella cybersecurity, si integrano e compenetrano.

I contenuti vengono suddivisi in 4 aree:

A. *La cybersecurity come fattore strategico del business*
Sezione 1 – Perché la Cybersecurity

   Si cerca di fornire, con approccio divulgativo, una visuale completa e aggiornata sulla materia, tenendo conto dei rinnovati **aspetti di mercato**, nonché di quelli **politici, strategici e tattici**. Viene, inoltre, analizzato e definito il **concetto moderno della cybersecurity**, nonché la sua importanza strategica per il business.

B. *Progettazione e management della cybersecurity*
Sezione 2 – Il Framework Nazionale per la Cybersecurity e la Data Protection

   Viene analizzato e descritto il **Framework Nazionale per la Cybersecurity e la Data Protection**, nonché il suo flusso di applicazione, che prende in input il Rischio aziendale. L'area non vuole essere un manuale, ma uno strumento per com-

prendere l'importanza di un **modello gestionale specifico di progettazione e governance**, anche alla luce delle sempre più stringenti richieste normative.

C. *Gli strumenti della cybersecurity*
Sezione 3 – Cybersecurity operativa

Vengono descritte, con un approccio accessibile anche ai non addetti, le **tecniche e gli strumenti operativi** della cybersecurity. In modo particolare, viene affrontato il tema dell'hardening dei sistemi, rappresentati i principali acronimi e processi della cybersicurezza, analizzate le tematiche relative al Security Operation Center.

D. *Parte specialistica*
Sezione 4 – Sanità
Sezione 5 – Pubblica Amministrazione
Sezione 6 – Modelli di metodologia operativa
Sezione 7 – Riferimenti normativi

Vengono analizzati argomenti, modelli, metodologie e normative specifiche per la **Sanità**, la **Pubblica Amministrazione** e le **aziende private**.

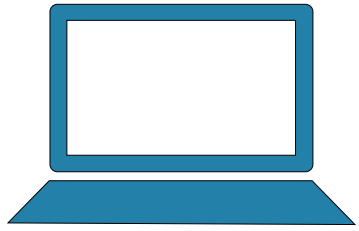
Il website degli autori

La cybersicurezza è un argomento in continua evoluzione, che richiede un maggiore dettaglio di un libro stampato, nonché un costante aggiornamento.

Ti invitiamo, quindi, ad iscriverti gratuitamente al nostro website www.cyberdefenceitalia.com, sul quale potrai trovare numerosi **materiali tecnici**, **approfondimenti** e **update**.

Per effettuare l'accesso:

- registrati compilando l'apposito form;
- accedi ai materiali di approfondimento;
- ricevi aggiornamenti e partecipa alle nostre attività.



www.cyberdefenceitalia.com

1 Perchè la cybersecurity

La cybersicurezza: 5 dogmi e 9 conseguenze

1

Prima di iniziare, permettetemi di definire il *corpo dei dogmi* che troverete in questo scritto. Ovviamente non in senso religioso, ma solo nel senso puramente scientifico, vale a dire postulati che hanno il mero scopo di porre le basi per ciò che dimostreremo, enunciati di cui si ipotizza la verità, un punto di partenza per creare una teoria coerente.

1. **Dogma del business:** la cybersecurity è una componente strategica del business: nel mondo moderno non esiste business senza cybersecurity.

   Conseguenza 1: non si può ragionare in termini di ROI (ritorno sull'investimento), quando si parla di sicurezza informatica.

   Conseguenza 2: non è un tema di sola pertinenza dell'IT. É un problema che deve riguardare tutta l'alta direzione e il management e, naturalmente, deve esserne pienamente coinvolto anche il personale operativo.

2. **Dogma della scienza:** la cybersecurity non è un insieme casuale di misure di sicurezza, ma un sistema organizzato in modo scientifico che, prendendo in input un'analisi intersoggettiva dei rischi presentati da un'azienda, determina adeguate misure di sicurezza e, attraverso un progetto ben definito, attua le procedure gestionali e le misure operative necessarie.

   Conseguenza 3: non esistono "miracoli" o "piattaforme miracolose" per la sicurezza informatica. Non esistono aziende di cybersecurity che hanno l'ingrediente segreto o l'accesso alla fonte dell'immortalità. Esistono bravi professionisti (pochi) e avventurieri (tanti): bisogna essere capaci di distinguerli. Questo è uno degli scopi del libro.

Conseguenza 4: non si può pensare di ottenere un buon livello di sicurezza informatica implementando occasionalmente un software o un hardware. La cybersecurity è un processo ben definito, che richiede step successivi, e che va affrontata dal management in maniera sistematica ed efficace.

3. **Dogma della resilienza:** non esiste in cybersecurity l'immunità agli attacchi. Un'azienda, piuttosto, può lavorare per incrementare la sua resilienza.

   Conseguenza 5: visto che, prima o poi, un attacco potrebbe aver successo, al fine di alleggerire le sue responsabilità, il management deve poter dimostrare l'adeguatezza del security model adottato. Questo significa porre in atto adeguate procedure organizzative e gestionali di cybersecurity: senza gestione non è possibile misurare il successo delle azioni implementate e ciò che non è misurato non è gestibile (o quantomeno è estremamente difficoltoso farlo).

   Conseguenza 6: è fondamentale avere un piano ben definito e orchestrato da una precisa metodologia, come quella del FNCS - *Framework Nazionale per la Cybersecurity e la Data Protection*, per sapere cosa fare prima, durante e dopo un attacco, proprio perché un incidente può sempre accadere, qualunque misura di sicurezza si adotti.

4. **Dogma dell'organizzazione criminale:** gli attacchi, nella norma, sono sferrati da organizzazioni criminali internazionali e molto ben organizzate che lavorano in proprio o, spesso, effettuano servizi "per conto terzi".

   Conseguenza 7: a minacce serie bisogna rispondere in maniera seria e organizzata. Ci sono interi squadroni di criminali informatici organizzati in maniera coordinata e tecnologicamente avanzata. Di norma, gli attacchi non vengono eseguiti da "geni del male" solitari o "hacker geniali".

5. **Dogma finale:** la cybersecurity non è un bottone che accende o spegne la luce. É un atteggiamento, un processo che permea il business e l'operatività aziendale.

   Conseguenza 8: bisogna prestare attenzione anche, e soprattutto, agli aspetti **non tecnologici**: le procedure e il personale, nonché il suo coinvolgimento e la sua preparazione, sono la nostra prima barriera di difesa.

   Conseguenza 9: è necessario cambiare totalmente paradigma e passare da un approccio basato sulla segnalazione di eventuali anomalie alla loro prevenzione o individuazione precoce.

2 Gli alieni sono scesi sulla terra e, nel frattempo, due devastanti pandemie e una guerra hanno cambiato il mondo

Se esistono, prima o poi gli alieni si paleseranno. E, dopo una prima fase di sorpresa e incertezza, per tutti noi saranno una normale e quotidiana presenza.

Il recente periodo pandemico è la prova di quanto l'umanità e i suoi comportamenti possano cambiare velocemente adattandosi alle nuove situazioni. Chi, prima del 2020 avrebbe infatti ipotizzato di indossare, anche solo per uscire di casa o andare a lavorare, una mascherina protettiva come in un film catastrofico di Petersen o Romero?

Lo stesso vale per la cybersecurity. Chi avrebbe detto che ci saremmo ritrovati di fronte a una situazione che, se non facciamo nulla, in un momento nel quale siamo ancora in una fase iniziale del problema, sarà, con ogni probabilità, un'onda devastante di Tsunami, capace di travolgere le nostre aziende e la nostra economia come fuscelli?

Si parla già di *pandemia informatica*. E, non volendomi appropriare di questa geniale definizione, sottolineo che non l'ho coniata io, ma l'ho sentita utilizzare, per la prima volta, da Antonio Patuelli, Presidente dell'Associazione Bancaria Italiana.

La cybersecurity è come gli alieni, ci abitueremo e sarà una nostra compagna di vita. Ma c'è una differenza: gli alieni non si sono mai palesati e non sappiamo se esistono, ma le problematiche legate alla cybersecurity, invece si, e in maniera eclatante. Essere pronti ad affrontare i pericoli digitali farà la differenza, per le aziende, tra sopravvivere e perire.

Siamo solo all'inizio della pandemia digitale, che sarà probabilmente più lunga, perniciosa e, per l'economia, una minaccia forse ancor più grande di quella, appena trascorsa, legata al coronavirus.

La cybersecurity è una cosa seria, che **va affrontata ai massimi livelli aziendali** e con precise competenze.

In medicina, lo abbiamo tristemente imparato a nostre spese, non bastano solo i farmaci e i vaccini. Ci sono anche comportamenti da tenere, mascherine da indossare e altre misure di profilassi e igiene. Ma, soprattutto, **bisogna essere preparati**.

Bisogna avere **un piano ben definito che ci guidi nella strategia da adottare e ci indichi le misure da implementare.**

Quello che è stato devastante, nella pandemia Covid-19, è stato proprio il fattore sorpresa. Da anni erano stati dismessi i reparti di virologia e quelli di terapia intensiva, nonché quasi azzerati i relativi budget. A quanto pare, in Italia, non esisteva neanche un piano pandemico aggiornato. Questo è costato file di camion in partenza da Bergamo all'alba (solo per citare uno dei numerosi dolorosissimi episodi di quel periodo) il cui ricordo credo che nessuno di noi potrà mai cancellare, e un impatto economico in confronto al quale una guerra sarebbe stata meno dannosa. Perché la Sanità è stata così trascurata, costringendo poi il personale all'eroismo in corsia, così come nelle case dei pazienti, con mezzi spesso insufficienti e pagando spesso il massimo tributo?

Se tutto ciò non fosse stato sufficiente, chi si aspettava una guerra in Europa che avrebbe totalmente stravolto le nostre certezze?

Adesso ci siamo accorti che una nuova, pericolosissima pandemia, si sta cominciando a diffondere. É vero, non è un virus, ma è la stessa storia. Certamente, non riguarderà un numero di vite umane grande quanto la prima, ma sicuramente per il business sarà almeno altrettanto dannosa. L'esperienza non ci ha insegnato nulla?

Vogliamo ripetere l'esperienza del Covid-19 oppure vogliamo fare in modo che la ns. società superi al meglio questa pericolosissima minaccia?

Ecco perché la cybersecurity è, e deve essere, uno strumento strategico per le Amministrazioni Pubbliche e le aziende. Non è solo una componente fondamentale del business, vale la loro sopravvivenza.

2 Framework Nazionale per la Cybersecurity e la Data Protection

Italians do it better: i modelli di riferimento e il Framework Nazionale per la Cybersecurity e la Data Protection

20

"Le note sono come il materiale per fare un palazzo, i mattoni sono uguali per tutti i palazzi, ma i palazzi non vengono uguali"[1].
Ennio Morricone

Il Framework

Gli interventi di cybersecurity devono essere, quindi, identificati e modulati adeguatamente applicando un preciso modello di riferimento. Questo ne permette l'intersoggettività interpretativa e la possibilità di poter essere letto e utilizzato da differenti professionisti.

Uno dei framework principali è **Framework Nazionale per la Cybersecurity e la Data Protection**, a cura del CIS-Sapienza/CINI, diventato ormai lo standard di riferimento normativo sia per le aziende pubbliche che private, capace di implementare anche i controlli di modelli o normative specifiche come quelli di AgID e GDPR o, ancora, di schemi di norme e standard di settore come, per esempio, la ISO 27.001, PCI DSS, NIST SP 800-37 v.2, Enisa report – cloud security for healthcare services e così via.

Porre in atto adeguate procedure organizzative e gestionali di cybersecurity vuol dire riuscire a misurare il successo delle azioni implementate. Se non avessimo un Sistema di gestione, non esisterebbe tale misurazione e viceversa.

Devo dire che, almeno in questo caso, *"Italians do it better"* è piuttosto appropriato. Il modello CIS-Sapienza/CINI, infatti, oltre a essere stato elaborato da enti nostrani, estende il corrispondente Framework ideato da NIST integrandone la compliance al GDPR. Il Framework Nazionale, quindi, lega l'aspetto pratico operativo di difesa con la prescrizione normativa, risultandone un grande valore per l'azienda.

L'utilizzo del modello ha numerosi vantaggi per l'ente che, sviluppando la relativa documentazione, vede incrementare la sua capacità operativa e la sua indipendenza dai fornitori.

1 "Ennio", film-documentario di Giuseppe Tornatore, 2021.

L'azienda, inoltre, può dimostrare oggettivamente le misure di sicurezza implementate, sia ai suoi clienti che alle autorità che dovessero richiederne la verifica.

Essenzialmente, **se non si utilizzasse il Framework e la relativa documentazione, l'azienda non sarebbe in grado di dimostrare la sua compliance normativa**, almeno in quella parte che unisce le prescrizioni di sicurezza alla loro applicazione pratica. E di questo ne sarebbe direttamente responsabile il management.

Questo strumento si può usare per qualunque tipologia di organizzazione, da quelle che presentano il rischio più basso alle infrastrutture critiche. **Ovviamente, il documento elaborato non sarà uguale per le prime e per le seconde, anzi, sarà differente per ogni singola azienda, visto che si deve adeguare a ogni specifico livello di rischio aziendale**. Effettueremo, quindi, la nostra analisi dei rischi e saremo capaci di argomentare un certo profilo di riferimento ideale.

La norma ISO 27001 e la cybersecurity

La ISO/IEC 27001 è la norma di riferimento per l'implementazione dei requisiti di un ISMS - *Information Security Management System*. Perché allora ricorrere a un altro, diverso, modello?

La risposta a questa domanda è molto semplice e riguarda sia una questione sostanziale che una formale. Dal punto di vista sostanziale, la norma ISO 27001 è caratterizzata da un'elevata complessità e risulta applicabile solo in contesti fortemente strutturati. Al contrario, la cybersecurity è un requisito fondante di tutte le aziende, anche e soprattutto di quelle non strutturate. In altre parole, tutte le organizzazioni hanno bisogno di un modello adeguato di cybersecurity, non necessariamente modulato sulla ISO 27001.

Dal punto di vista formale inoltre, troppo spesso il possesso della "Certificazione ISO 27001", focalizzandosi prevalentemente su evidenze documentali, più che un vero indicatore di cybersicurezza, ha rappresentato, per le aziende, un "lasciapassare" per

dimostrare burocraticamente il possesso di requisiti e, di conseguenza, un comodo alibi per non subire audit di seconda parte e per non affrontare quelle lacune sostanziali che, dalla cronaca quotidiana degli attacchi finalizzati, non è più possibile ignorare.

Occorre quindi un modello di cybersecurity che sia in grado di realizzare una *governance strategica dei processi della sicurezza delle informazioni*, da un lato, inquadrandone le nuove dimensioni costitutive, come quelle di *data protection*, dall'altro, attraverso un'attività di *project management*, declinando il piano strategico generale e astratto in quello operativo, concreto, tecnico e misurabile.

Essenzialmente, il Framework è composto da una corposa serie di controlli divisi in cinque macroaree o funzioni: **Identify, Protect, Detect, Respond** e **Recover**. Le funzioni sono la rappresentazione logica del ciclo di vita di **qualsiasi processo finalizzato alla sicurezza delle informazioni**. Per questo motivo, implementare i controlli su ogni area tematica, crea un Sistema di gestione della cybersecurity trasversale all'organizzazione, in grado di metterne al sicuro i flussi di trattamento.

Un'ultima osservazione. Questo libro non ha lo scopo di fornire indicazioni di dettaglio sull'utilizzo operativo del Framework. Un manager non ha la necessità, a meno che lo desideri, di scendere nei particolari, ma deve conoscerne le generalità e i principi. Nel caso, ci sarà sempre tempo per approfondire, ma, intanto, possiamo condividerne significato, modalità operative e magari dare indicazioni sugli errori da evitare:

1. **Il Framework è semplicemente un modello**

   É un template teorico, espresso in termini generali che contiene tutte le *macroaree* in tema di sicurezza. Questo significa che, per utilizzarlo e applicarlo, è **necessario l'intervento di una figura professionale**, il *Cybersecurity Manager*, che sia capace di "cucirlo" sull'azienda, come fosse un'opera

sartoriale, innestando due azioni fondamentali e ad alto valore aggiunto:

a. da un lato, la *contestualizzazione*, cioè la selezione, tra tutte le misure possibili, dei controlli *adeguati* allo specifico profilo di rischio;

b. dall'altro, la *traduzione* dei requisiti generali, espressi con termini divulgativi e vicini al linguaggio comune, *in istruzioni operative* e molto tecniche.

In questo modo, il Cybersecurity Manager, riducendo al minimo la discrezionalità degli operativi, tutela il dirigente della business unit che lo coinvolge perché, assumendosi chiaramente la responsabilità dell'adeguatezza dell'istruzione impartita e del suo monitoraggio, risolve il "cortocircuito" tipico delle pericolose deleghe alla gestione della sicurezza a profili operativi, che ovviamente, oltre a non essere figure esperte di analisi dei rischi, non possono e non devono occuparsi contemporaneamente, come abbiamo già analizzato in precedenza, dell'aspetto strategico e di quello attuativo.

2. **Il Framework non può essere applicato pedissequamente**

É fondamentale analizzare dettagliatamente il rischio che presentano i nostri sistemi: solo così potremo attuare adeguate misure di sicurezza. Non solo, non è neanche possibile implementarlo pedissequamente. Come vedremo, è compito dell'analista, in base all'analisi dei rischi e alle specificità aziendali, scegliere quali controlli applicare e come quantificare, in base a dati oggettivi, le opportune misure di sicurezza.

Tanti anni fa un amico mi ha insegnato che *"è meglio essere vicini alla luce che sicuramente al buio"*. Ho sempre tenuto conto di questa preziosa considerazione nella mia vita. Probabilmente usare il Framework ci posiziona vicino alla fonte luminosa, o forse lo diventa esso stesso. Utilizziamolo per illuminare il nostro percorso piuttosto che andare avanti alla cieca.

Il Framework e gli OSE - *Operatori di Servizi Essenziali*

Agli OSE appartengono le aziende private e le Amministrazioni Pubbliche che erogano quei servizi individuati dalla Presidenza del Consiglio dei ministri, e che partecipano in modo mandatorio all'architettura critica del Paese, facendo parte del Perimetro Cibernetico Nazionale. Questi operatori ricevono una notifica riservata dal Ministero dello sviluppo economico come OSE e non esiste, quindi, un loro elenco che si possa consultare. Anche i loro fornitori sono tenuti al segreto.

In ogni caso, l'elenco delle categorie ai quali possono appartenere gli OSE è presente come allegato al DL 18 maggio 2018, n. 65 e comprende energia (elettrica, petrolio e gas), trasporti (aereo, ferroviario, navigazione e su strada), settore bancario e infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile. Per gli OSE il Framework è addirittura, in una sua specifica versione, obbligatorio.

Fossi un OSE mi preoccuperei: i requisiti richiesti sono piuttosto impegnativi e stringenti. Se ciò non bastasse i tempi di adeguamento alla normativa sono ridottissimi.

Oltre agli OSE, esiste la categoria dei fornitori di servizi digitali cioè gli ISP - Internet Service Provider, i cloud provider e altri ancora. Tutti hanno ricevuto la notifica dal ministero dello sviluppo economico e, pur non facendo parte del perimetro cibernetico, vengono obbligati ad applicare la direttiva NIS 11480 e i decreti italiani di attuazione alla stessa direttiva.

A questi soggetti viene inoltre richiesto che il tavolo di Risposta all'incidente (cioè quello che viene chiamato in causa in caso di incidente cibernetico nazionale) sia caratterizzato da un'unità per ogni OSE che poi fa capo al CISRT – *Computer Security Incident Response Team* italiano.

Poiché le operazioni sono secretate non possiamo monitorare lo stato di attuazione di questo decreto che immette nell'ordinamento italiano la direttiva europea ma, a occhio, credo sia un po' in ritardo.

La normativa fissa alcuni punti essenziali delle misure di sicurezza richieste agli OSE, in una precisa *contestualizzazione* del Framework. Quello che però è importante notare è come siano stati eliminati gli standard minimi di sicurezza e introdotto l'onere di dimostrare l'adozione di misure adeguate allo specifico flusso tecnologico e operativo di una determinata azienda. Il legislatore europeo, infatti, si è giustamente reso conto che staticizzare le misure di sicurezza significava rendere la Legge insufficiente, soprattutto di fronte agli incalzanti ritmi dell'evoluzione tecnologica. Non restava quindi, per rendere possibile il business nello spazio informatico, che far diventare il vincolo legislativo più generale e far gravare l'onere delle modalità di adeguamento sull'OSE.

Questo onere, per l'azienda, è particolarmente gravoso, quasi un cortocircuito, perché a tutt'oggi non sono presenti standard di settore. Tuttavia, il Framework ci viene incontro dato che, tramite un'approfondita analisi dei rischi sulla quale innestare gli interventi di cybersecurity, saremo in grado di dimostrare l'adeguamento normativo e tecnico.

Le funzioni del Framework e il rischio quale input per la determinazione delle misure adeguate di sicurezza

Le funzioni del Framework possono essere riunite in due grandi gruppi. Il primo che comprende **Identify** e **Protect**, le quali prevedono lo studio degli asset e dei flussi dell'organizzazione. Questo permette di effettuare l'analisi dei rischi e individuare il rischio intrinseco di quella specifica azienda. Il secondo che comprende invece le altre tre funzioni **Detect, Respond** e **Recover**, le quali rappresentano **l'Incident response** o Risposta all'incidente e, quindi, **il processo che, partendo dall'identificazione di un'anomalia, permette il ritorno a una situazione di normalità.**

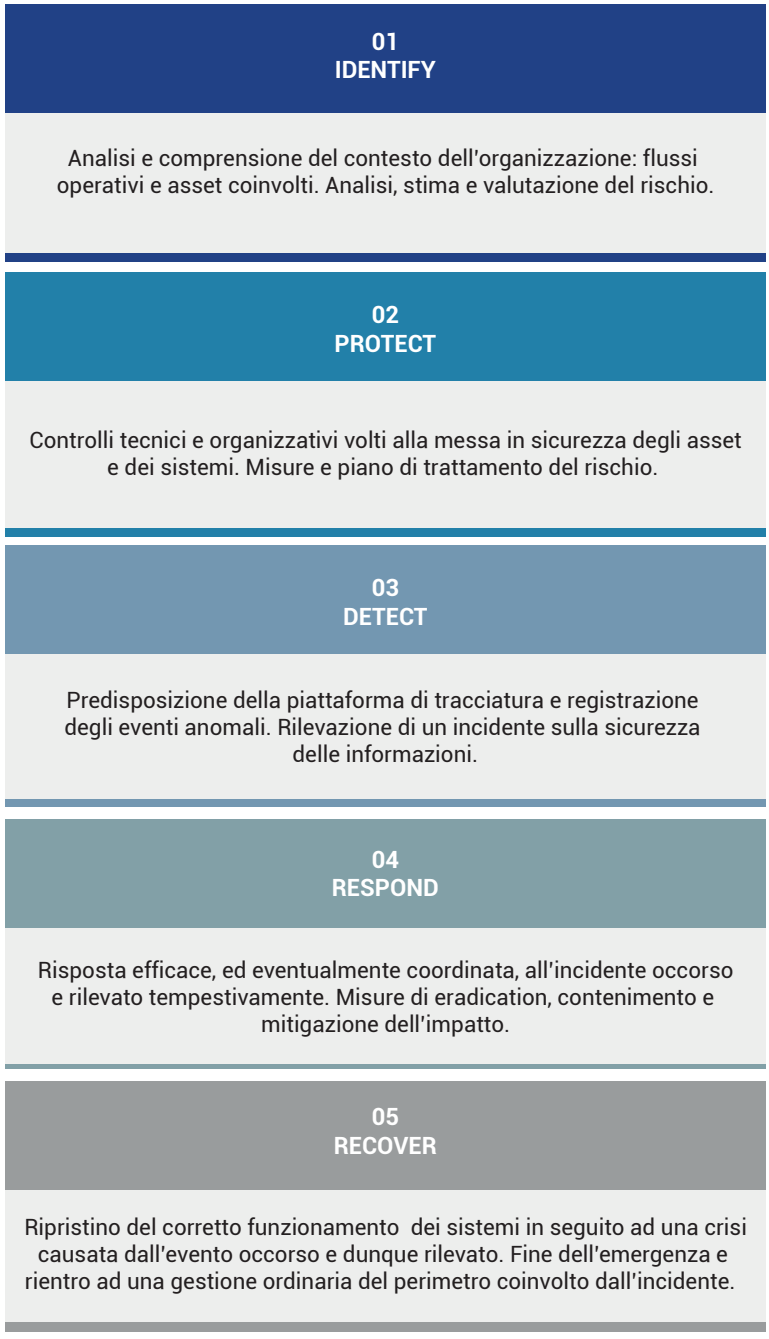


Figura 5 - Le funzioni del Framework

La cybersecurity è una componente strategica fondamentale del business, un'attività **imprescindibile** per le aziende private, così come per la Pubblica Amministrazione. Riguarda tutti: il management così come i ruoli esecutivi.

I manager, infatti, hanno una funzione di primo piano nel proteggere le aziende, non solo perché hanno **l'onere della riuscita del business** ma anche perché, in mancanza di adeguati interventi di protezione, ne può essere invocata **la responsabilità civile e amministrativa** o, se si tratta di una Pubblica Amministrazione, anche **la responsabilità per danno erariale.**

I ruoli esecutivi, attraverso la loro operatività, costituiscono la "messa a terra" della strategia, rappresentando quindi anch'essi una componente indispensabile per il successo della cybersecurity in azienda.

Una strategia di business che tenga nella giusta considerazione la cybersecurity, non solo rappresenta un notevole vantaggio competitivo per le aziende private e le Amministrazioni Pubbliche, ma è anche **un asset fondamentale** per la tutela **dell'economia**, **della sicurezza** e **della salute di tutti noi**.

Questo libro ha lo scopo di consentire, al management e alle varie funzioni aziendali, l'approfondimento delle conoscenze nell'ambito della progettazione e dell'organizzazione della cybersecurity, **un processo che hanno non solo l'obbligo, ma anche l'interesse di governare.**

Con il patrocinio di ANPD
Associazione Nazionale per la Protezione dei Dati

ISBN 979-12-210-1337-5

€ 28,00

Catanzaro, Sforza
CYBERSECURITY benvenuti nell'era della pandemia informatica
RMC editore