COMUNICAZIONE DIGITALE

ANNO 4 – N. 1-2

GENNAIO–DICEMBRE 2018

Registrazione
Tribunale di Roma
n. 195 del 12 maggio 2005

Comunicazione digitale

Periodico semestrale
del Centro Studi Comunicazione Istituzionale
e Innovazione Tecnologica (ComIT)

Contributi di
Giacomo Buoncompagni
Mirto Silvio Busico
Nicola Busto
Maria Cupolo
Christian Ferrari
Massimo Montanile
Claudia Romito
Saverio Rubini
Elisabetta Zuanelli

Aracne editrice

www.aracneeditrice.it
info@aracneeditrice.it

www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

via Vittorio Veneto, 20
00020 Canterano (RM)
(06) 45551463

ISBN 978-88-255-2162-7
ISSN 2284-1725

I edizione: dicembre 2018

Indice

5 *Indice*

RICERCA E SVILUPPO

7 *Christian Ferrari*
La gestione del *cybersecurity risk*: oggetto e metodologie

1. Il quadro normativo sulla cybersecurity e gli impatti in termini manageriali ed organizzativi: l'approccio basato sul rischio, *7* – 2. *Cyber-risk management*, *11* – 2.1. L'architettura del *cyber-risk*. *Malicious* e *non-malicious cyberthreat*, *12* – 2.2. Comunicazione e consultazione, *15* – 2.3. Definizione del contesto, *17* – 2.4. *Cyber-risk assessment*, *19* – 2.4.1. *Cyber-risk identification: malicious* e *non-malicious cyberthreat*, *22* – 2.4.2. *Cyber-risk analysis*, *28* – 2.4.3. *Cyber-risk evaluation*, *32* – 2.5. *Cyber-risk treatment*, *35* – 2.6. Monitoraggio e revisione, *36* – 3. Tassonomie di *cyberthreat*, *39* – 4. Tassonomie, modelli di rappresentazione delle *cyberthreat* e ontologie. La *Platform Ontology of Cybersecurity* (POC), *43* – 5. Considerazioni conclusive. Le vulnerabilità dei *cyber-system* derivanti da incongruenze concettuali e di processo. Il necessario "sforzo" di uniformazione, 47

51 *Giacomo Buoncompagni*
Immersi nel digitale: profilo del cittadino mediale e nuovi processi comunicativi. Un'analisi socio-culturale

MERCATI E TENDENZE

59 *Elisabetta Zuanelli*
Dalla *customer experience* alla *user experience*: un percorso all'indietro nel marketing digitale

1. *Customer experience* e *user experience*, *59* – 2. Le conoscenze di sfondo, *61* – 3. Pre-condizione metodologica: la qualità del *software* e l'usabilità, *63* – 4. L'usabilità, *64* – 5. Interattività, progettazione, valutazione, *66* – 6. L'analisi *desk* di usabilità e la *user experience*, *67* – 7. L'analisi e il Protocollo usabilità/architetture del CReSEC / Comunicazione digitale / Pragmema, *69* – 8. La *task analysis*, *71* – 9. Conclusioni, *71*

73 *Saverio Rubini*
Copie di salvataggio in un computer: come, dove e perché

1. L'attacco informatico ha avuto successo, *59* – 2. "Periodicamente": cioè?, *75* – 3. Una semplice tecnica di copia: nonno-padre-figlio, *76* – 4. Dove eseguire le copie, *78*

FORMAZIONE

81 *Massimo Montanile, Maria Cupolo, Claudia Romito*
La formazione privacy ai tempi del GDPR: un modello innovativo

1. Premessa, *81* – 2. Considerazioni di contesto, *82* – 3. Sfide e opportunità del GDPR, *85* – 4. La cultura della sicurezza, *87* – 4.1. Principi di *risk management*, *88* – 4.2. Peculiarità del *risk management*, *88* – 4.3. Il *Franework* ISO 31000, *89* – 5. L'approccio vincente, *90* – 5.1. Perché l'*e-learning?*, *91* – 5.2. Il modello 70:20:10 nell'era digitale, *92* – 5.3. Obiettivi, *93* – 5.4. Formazione su misura, *93* – 6. Efficacia della formazione *e-learning nel* Progetto Formazione FuoriClasse, *94* – 7. La formazione vista dal legale: formati, informati e sicuri, *97*

101 *Redazione*
Il Master in *Cybersecurity* e *privacy* dell'Università di Roma Tor Vergata

1. La seconda edizione del Master, *101* – 2. Lo scenario di riferimento, *102* – 3. Gli obiettivi, *102* – 4. Gli sbocchi occupazionali, *103* – 5. Articolazione del Master, *103* – 6. *Project work* e *stage* abilitante obbligatorio, *104* – 7. Certificazioni conseguibili, *106* – 8. I soggetti promotori, *108* – 9. Modalità d'iscrizione al Master, *112*

STORIE E OPINIONI

115 *Nicola Busto*
"L'Intelligenza Artificiale per l'Europa" e il ruolo di avanguardia dello AI HLEG della European AI Alliance

1. L'Intelligenza Artificiale e il ruolo del critico tecnologico, *115* – 2. L'opacità dell'inconscio tecnologico, *117* – 3. L'iniziativa europea in tema di IA, *118* – 4. AI HLEG e AI Alliance: l'avanguardia della critica tecnologica, *119*

123 *Mirto Silvio Busico*
«La proprietà è un furto», disse il possidente…

LIBRI

129 *Elisabetta Zuanelli*
L'Università e l'immagine

133 *Nota sugli autori*

La gestione del *cybersecurity risk*: oggetto e metodologie

Christian Ferrari

1. Il quadro normativo sulla *cybersecurity* e gli impatti in termini manageriali ed organizzativi: l'approccio basato sul rischio

Due norme di recente introduzione, la Direttiva UE 2016/1148 (*Network and Information Security* – c.d. "Direttiva NIS"), recante misure per elevare il livello di sicurezza di reti e sistemi informativi delle cosiddette infrastrutture critiche (Operatori dei Servizi Essenziali e Fornitori di Servizi Digitali) e il Regolamento UE 2016/679 (*General Data Protection Regulation* – c.d. GDPR), che introduce disposizioni atte a garantire la protezione delle persone fiche con riguardo al trattamento di dati personali, definiscono per la prima volta un nuovo quadro di *governance* in tema di *cybersecurity* (in particolare, NIS) e introducono nuovi obblighi (sia la NIS e sia il GDPR), in termini di misure di sicurezza e di notifica degli incidenti cibernetici, indirizzati a organizzazioni sia pubbliche sia private.

Le norme citate richiedono che tali organizzazioni debbano garantire la protezione delle reti e dei sistemi informativi, nonché dei dati e delle informazioni che ivi transitano e sono trattate. Il legislatore, dunque, individua per la prima volta un interesse pubblico sotteso alla sicurezza dello spazio cibernetico, riconoscendo, al tempo stesso, autonomia alle organizzazioni, stabilendo che siano loro stesse a dover determinare le misure tecniche e organizzative di sicurezza adeguate al rischio, atte a

garantire la protezione di reti, sistemi e dati. Il legislatore, poi, compie un ulteriore passo in avanti, laddove introduce il principio di *accountability*, che obbliga i soggetti destinatari delle norme a dimostrare, innanzi alle autorità pubbliche preposte ("autorità competenti", per la NIS; "autorità di controllo", per il GDPR), l'adeguatezza al rischio delle misure di protezione individuate e implementate.

Nell'approccio NIS e GDPR, dunque, la protezione di reti e sistemi informativi passa inevitabilmente attraverso il processo di gestione del rischio, finalizzato alla sua identificazione, valutazione e, se ritenuto opportuno, all'introduzione di misure di sicurezza di tipo tecnico e organizzativo atte a ridurlo a un livello accettabile. Ciò comporta, anzitutto, che l'organizzazione, sia pubblica sia privata, pianifichi e implementi il processo di gestione del rischio alla sicurezza di reti, sistemi e dati, scandendolo nelle due principali fasi di cui si compone: il *risk assessment* e il *risk treatment*[1].

La *compliance* alla normativa europea brevemente analizzata e, più in generale, la sopravvivenza delle organizzazioni nell'attuale contesto economico e sociale è strettamente correlata alla capacità che queste hanno nell'implementare correttamente le misure di sicurezza, a tutela del patrimonio informativo, la cui violazione delle proprietà di riservatezza, integrità e disponibilità potrebbe comportare, ad esempio, rilevanti impatti in termini di *business,* e, con riferimento agli operatori e ai fornitori, cioè le infrastrutture critiche dell'economia, a tutela del funzionamento dell'economia e della società digitale.

Diverso è l'approccio al rischio che emerge dal dettato normativo della direttiva NIS e quello che emerge dalla lettura delle disposizioni del GDPR: nel primo (NIS), infatti, la gestione del rischio coinvolge direttamente gli *asset* interni all'organizzazione; nel secondo (GDPR) la protezione da garantire coinvolge solamente in maniera indiretta gli *asset* dell'organizzazione, mentre il bene primario da tutelare sono i diritti e le libertà degli interessati cui i dati personali si riferiscono[2].

---

[1] La suddivisione del processo di *risk management* in queste due macro fasi è, in particolare, riportata nello *standard* ISO 31000 e ripreso da altri *standard* quali quello sulla sicurezza delle informazioni ISO/IEC 27001.

[2] Ciò comporta impatti rilevanti, in particolare, nella determinazione del livello di rischio: non è detto, infatti, che un rischio categorizzato come "basso" dall'organizzazione possa essere ugualmente "basso" anche in termini di impatti per

La relazione tra *risk management*, misure di sicurezza e protezione di dati e informazioni, soprattutto personali, ruota attorno alla protezione e sicurezza di reti e sistemi informativi, ossia attorno al concetto di *cybersecurity*. Al riguardo, sono stati elaborati diversi *framework* e *standard* internazionali che hanno introdotto *best practice* e controlli di sicurezza per mitigare i rischi connessi al *cyberspace*.

Un primo modello di particolare rilevanza è quello elaborato dal National Institute Standard and Technology (NIST)[3], che ha introdotto nel 2014 un *framework* specifico sulla *cybersecurity*; circa un anno più tardi, sul modello americano, è stato pubblicato un *framework* nazionale dal Centro di Ricerca Cyber Intelligence and Information Security e dal Consorzio Interuniversitario Nazionale per l'Informatica (CINI)[4].

Un secondo *standard* molto diffuso, rappresentato dalla famiglia ISO/IEC 27000, riporta norme disciplinanti requisiti e linee guida per garantire la sicurezza delle informazioni all'interno dell'organizzazione, garantendo l'implementazione, nell'ottica di miglioramento continuo, di un Sistema di Gestione sulla Sicurezza delle Informazioni. È necessario specificare, però, che la famiglia ISO/IEC 27000 riguarda la sicurezza delle informazioni in generale, racchiudendo solo in parte i controlli di *cybersecurity*[5].

---

gli interessati. Questo aspetto apre, tra l'altro, particolari difficoltà applicative delle disposizioni dell'art. 32 GDPR.

[3] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Gaithersburg, 2014.

[4] *Italian Cyber Security Report. Un framework nazionale per la Cyber Security*, a cura di R. Baldoni e L. Montanari, Sapienza Università di Roma e CINI, Roma, 2015

[5] Solamente alcuni dei controlli dell'Allegato A della norma ISO/IEC 27001 sono specifici di *cybersecurity*. Esiste una differenza tra il concetto di *sicurezza delle informazioni* e *cybersecurity*? La sicurezza delle informazioni rappresenta una categoria ampia, in quanto riferita a qualsiasi informazione che può avere un valore (*asset*) per l'organizzazione. Al proprio interno questa macro-categoria contiene un'ulteriore area di specificazione, ossia la *cybersecurity*: il rapporto tra le due, quindi, dovrebbe essere letto come in un rapporto di genere-specie. La sicurezza delle informazioni, in generale, si pone a tutela e protezione delle informazioni di valore per l'organizzazione, tutelandone la riservatezza, l'integrità e la disponibilità da minacce e fonti di minaccia di tipo fisico, umano e tecnologico; la *cybersecurity*, invece, attiene alla protezione dalle *cyberthreat*, da un lato delle informazioni che circolano nel *cyberspace* attraverso le reti e i sistemi informativi dell'organizzazione: la riservatezza, l'integrità e la disponibilità devono essere quindi riferite alle infor-

Sia il *framework* citato, sia le norme della famiglia ISO/IEC 27000 utilizzano un approccio basato sul rischio: per garantire la sicurezza di reti e sistemi informativi, dunque, è necessario che l'organizzazione attui un processo di *cyber-risk management*, individuando gli *asset* e le relative vulnerabilità e minacce principali, identificando, analizzando e ponderando i rischi nella fase di *risk assessment* e trattandoli, quando lo ritiene opportuno, nella fase di *risk treatment*.

A fianco del *framework* NIST e della ISO/IEC 27001 si pongono ulteriori *standard* internazionali dedicati alla gestione del rischio alla sicurezza delle informazioni. Il primo, elaborato dall'Open Group, e descritto nel documento *Open Information Security Management Maturity Model* (O-ISM3)[6]; il secondo, elaborato dal Software Engineering Institute, e descritto nel *technical report* denominato *Operationally Critical Threat, Asset and Vulnerability Evaluation* (OCTAVE) Allegro[7]: entrambi si basano su un diverso approccio per processi, ma entrambi sono caratterizzati dalla finalità, simile, funzionale a conciliare gli obiettivi di *business* con gli obiettivi di sicurezza.

Riprendendo in parte i *framework* e gli *standard* citati, di seguito sono descritti gli aspetti principali di un processo di gestione del *cybersecurity risk*, confrontato opportunamente con le tecniche e metodologie più diffuse e utilizzate per la gestione del rischio alla sicurezza delle informazioni e, più in generale, con il processo di *risk management*. A fianco e a sostegno di questo processo *core*, si pone, inoltre, l'essenziale attività di analisi delle minacce cibernetiche esistenti che potrebbero compiere attacchi nei confronti delle reti e dei sistemi dell'organizzazione: nei paragrafi successivi, dunque, saranno analizzate le principali metodologie in uso per la definizione di tassonomie di *cyberthreat*, analizzando infine l'espansione di metodologie innovative di categorizzazione di rischi e minacce, basate sull'ontologia.

---

mazioni trattate attraverso le tecnologie ICT utilizzate dall'organizzazione stessa. Dall'altro lato, la *cybersecurity* si occupa anche della protezione e della resilienza di infrastrutture, reti e sistemi informativi.

[6] THE OPEN GROUP, *Open Information Security Management Maturity Model (O-ISM3)*, Version 2.0, Reading, 2017

[7] R.A. CARALLI, J.F. STEVENS, L.R. YOUNG, W.R. WILSON, *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*, Software Engineering Institute, Pittsburgh, 2007

2. *Cyber-risk management*

Al pari dei processi implementati per la gestione del rischio alla sicurezza delle informazioni, anche per la *cybersecurity* è necessario individuare i rischi che potrebbero compromettere reti e sistemi informativi: più in generale, la *cybersecurity* può essere intesa come la protezione, attraverso processi e controlli, dei *cyber-system* dalle *cyberthreat*[8]. L'interconnessione continua con il *cyberspace* per lo svolgimento delle proprie attività *core*, vincola potenzialmente qualsiasi organizzazione alla realizzazione di un processo continuo di gestione del rischio *cyber* assicurando, per quanto possibile, che le reti e i sistemi informativi siano affidabili e resilienti.

Il *cyber-risk management* può essere inteso come un processo interno e più specifico del più generale processo di *risk management* che generalmente un'organizzazione implementa per indirizzare e controllare i rischi cui è soggetta la propria attività; non tutti i rischi che attengono a reti e sistemi informativi, inoltre, possono essere ricompresi nella definizione di *cyber-risk*, ma solo quelli che sono causati dalle *cyberthreat*[9]. Il processo di gestione del rischio *cyber* deve essere poi costruito in coerenza con gli obiettivi di *business* dell'organizzazione.

Il *cyber-risk management* deve essere necessariamente inteso come un processo continuo attraverso cui un'organizzazione *identifica*, *valuta*, *pondera* e *tratta* i rischi che potrebbero avere degli impatti sui *cyber-system* e, di riflesso, su dati e informazioni che circolano al suo interno, con possibilità, da ultimo, di danneggiare gli *asset* chiave di un'organizzazione.

Secondo il CLUSIT sono cinque i fattori critici che determinano un'efficace strategia di implementazione del processo di *cyber-risk ma-*

---

[8] Per *cyberthreat* si intendono le minacce che operano nel *cyberspace* e che sfruttano le vulnerabilità dei *cyber-system* per danneggiare gli *asset* di un'organizzazione. Sul punto si veda quanto analizzato da A. REFSDAL, B. SOLHAUG, K. STOLEN, *Cyber-risk management*, Springer, Berlino, 2015, p. 29.

[9] Un esempio di *cyber-risk* causato da una *cyberthreat* potrebbe essere la violazione della disponibilità di una rete a causa di un attacco *Denial of Service* (DoS) da parte di un *hacker* o della violazione di confidenzialità di un'informazione attraverso un attacco *Man-In-The-Middle* eseguito attraverso la rete aziendale.

nagement[10]. Il primo consiste nell'acquisire il quanto più possibile, una visione "globale" del *cyber-risk*, acquisendo informazioni continuamente aggiornate sulle minacce e sulle loro evoluzioni, sull'identificazione dei *target* potenziali e sulla verifica dei livelli di protezione sia a livello di funzione dell'organizzazione, sia a livello dell'organizzazione nel suo complesso. Il secondo attiene all'identificazione degli *asset* chiave per l'organizzazione e il relativo impatto, in caso di incidente, per le sue attività *core*. Il terzo elemento riguarda la particolare attenzione che deve essere prestata agli scenari di rischio, utilizzando correttamente i dati storici e l'esperienza dell'organizzazione, dando adeguata priorità di trattamento ai rischi più significativi (cui è stato attribuito un livello più alto). Il quarto richiede la definizione di una strategia di *risk appetite*[11], condivisa opportunamente con il *management* dell'organizzazione. Il quinto, infine, è relativo all'aggregazione dei controlli di sicurezza da implementare e alla loro aggregazione di tipo trasversale all'interno dell'organizzazione.

2.1. L'architettura del cyber-risk*.* Malicious *e* non-malicious cyberthreat

All'interno della suddivisione ampiamente condivisa dei rischi cui è sottoposta un'organizzazione, che generalmente distingue *rischi speculativi* e *rischi puri*[12], il *cyber-risk* può essere inserito in quest'ultima categoria, ossia tra quei rischi che, se concretizzati, comportano solamente perdite per l'organizzazione. Per questo motivo risulta essenziale analizzare la struttura del *cyber-risk* e comprendere di quali elementi è composto, per poi poter intervenire attraverso l'implementazione di procedure, controlli e tecnologie, riducendo il rischio a un livello accettabile.

---

[10] Si veda sul punto P. PACE e A. PENNASILICO, "Cyber risk management", in *Rapporto CLUSIT 2017 sulla sicurezza ICT in Italia*, Astrea, Milano, 2017, pp. 226-232

[11] Ossia della *propensione al rischio* e, quindi, dall'insieme dei rischi che l'organizzazione è disposta a sopportare.

[12] Sul punto si vd. in particolare A. FLOREANI, *Enterprise risk management. I rischi aziendali e il processo di risk management*, I.S.U. Università Cattolica, Milano, 2004, pp. 75 ss. e U. SACCONE, *Governare il rischio. Un modello di security risk management*, Aracne editrice, Roma, 2014, pp. 61-62.

L'architettura essenziale del *cyber-risk* è articolata in due componenti: *verosimiglianza* e *impatto*[13]. Sulla *verosimiglianza* è necessario tenere conto di due aspetti principali: la probabilità che una minaccia agisca contro l'organizzazione e la probabilità che la minaccia riesca nell'intento di danneggiare uno o più *asset*, sfruttando le vulnerabilità dei *cyber-system*. Entrambi i fattori devono essere letti in maniera congiunta; per le vulnerabilità, inoltre, è necessario determinare la superficie d'attacco, il tipo di debolezza sfruttabile e la capacità di resistenza del sistema su cui la minaccia insiste. Sull'*impatto*, invece, è necessario prendere in considerazione gli *asset* dell'organizzazione, ossia tutto ciò che può avere un valore per l'organizzazione stessa. Un approccio per determinare gli impatti sugli *asset* potrebbe essere quello di scomporli in violazioni di riservatezza, integrità e disponibilità[14]: alcuni *asset*, inoltre, hanno differenti impatti per le diverse tipologie di violazione.

Il primo passo necessario, dunque, è quello di redigere un inventario degli *asset*, attraverso cui sviluppare una prioritizzazione degli *asset* medesimi e portare, dunque, l'organizzazione a individuare quelli con valore maggiore. Per realizzare questo inventario può essere utile mappare tutti i sistemi e i dati rilevanti per l'organizzazione. Una volta identificati, gli *asset* devono essere valutati. È comunque importante sottolineare che non è possibile eliminare del tutto il *cyber-risk*, ma solo ridurlo a un livello accettabile attraverso l'introduzione di specifici controlli[15].

---

[13] Le due parti sono essenziali per poter definire un evento come '*cyber-risk*'. Infatti, affermare che un attacco *hacker* possa compromettere il funzionamento della rete aziendale e rendere così impossibile fornire un servizio *online*, per esempio, non è rappresentare un rischio, quanto descrivere un impatto. Così come affermare che un'organizzazione sia soggetta tutti i giorni a decine di *malware spam* o *phishing attack* sulla propria *e-mail* non significa rappresentare il rischio, poiché non è adeguatamente rappresentato e descritto il relativo impatto.

[14] L'organizzazione dovrebbe domandarsi, per esempio: quale sarebbe l'impatto in termini di *business* (concorrenzialità, reputazione, introiti, ecc.) sull'organizzazione nel caso in cui fossero violate la riservatezza, l'integrità o la disponibilità di una rete o di un sistema?

[15] Né gli interventi sulla verosimiglianza, né quelli sugli impatti possono eliminare definitivamente il rischio. Riguardo alla verosimiglianza, per esempio, non può essere eliminato definitivamente il rischio che un attaccante violi la rete aziendale: ciò che può essere fatto è introdurre apposite contromisure (es. gestione di *password* "robuste" per consentire l'accesso alla rete, scansioni periodiche della rete per veri-

Uno dei principali aspetti che caratterizza il *cyber-risk* rispetto agli altri rischi cui sono sottoposti le attività e gli *asset* dell'organizzazione, è quello relativo alle minacce e alle loro specifiche peculiarità. Anzitutto, le minacce che contribuiscono a scaturire il *cyber-risk* sono dette *cyberthreat*, in quanto sfruttano vulnerabilità dei *cyber-system* per recare danni agli *asset* dell'organizzazione. Le specifiche peculiarità delle *cyberthreat*, inoltre, caratterizzano il processo di gestione del rischio *cyber*, incidendo sull'articolazione della fase di *risk assessment* che si articola, in questo contesto, in due principali tipologie.

Una prima tipologia è detta *malicious cyberthreat*, che caratterizza il *cyber-risk* in quanto derivante (la minaccia e, di conseguenza, il rischio) da una fonte malevola intenzionale (per esempio, la probabilità che un *hacker black hat* effettui un accesso non autorizzato a dati altamente sensibili per l'organizzazione, per la loro pubblicazione all'esterno e, dunque, con rilevanti impatti in termini reputazionali, è un *cyber-risk* causato da una *malicious cyberthreat*). Una seconda tipologia è, invece, definita *non-malicious cyberthreat* se la minaccia non è intenzionale. Un esempio potrebbe essere la probabilità che si verifichi la comunicazione accidentale di un'informazione sensibile da parte di personale non adeguatamente formato a un altro soggetto rispetto al destinatario autorizzato e legittimato a ricevere e leggere l'informazione stessa, con impatti rilevanti per le attività di *business* dell'organizzazione).

Non rientra all'interno della definizione di *cyber-risk*, per esempio, la probabilità che un incendio danneggi un *server* con possibili impatti in termini di *denial of service* per i clienti, a meno che questo non sia stato causato da una *malicious cyberthreat*.

---

ficare la presenza di eventuali vulnerabilità, *firewall*, scansione periodica dei MAC *address* per verificare che non siano presenti dispositivi sconosciuti, ecc.), per ridurre le probabilità che l'attaccante possa riuscire nell'intento di compiere un attacco. Allo stesso modo riguardo agli impatti: gli impatti negativi derivanti da un *data breach* che ha comportato la cancellazione dei dati delle carte di credito dei clienti può essere in parte contrastato attraverso una regolare procedura di *back-up*. Ciò nonostante, l'attacco può sempre comportare ad un'interruzione, per quanto breve, nei servizi erogati. Sul punto si veda C. GALLOTTI, *Sicurezza delle informazioni. Valutazione del rischio, sistemi di gestione, la norma ISO/IEC 27001:2013*, lulu.com, Morrisville, 2017, pp. 96-97.

Le prospettive riportate comportano differenti impatti sulla fase di valutazione dei rischi, rappresentandone un diverso punto di partenza. Nel caso delle *malicious cyberthreat*, infatti, l'identificazione dei rischi dovrebbe avvenire attraverso l'analisi della fonte di minaccia, in particolare degli elementi essenziali e delle caratteristiche dell'avversario quali motivazioni, abilità, competenze tecniche e risorse a disposizione. Nel caso delle *non-malicious cyberthreat*, invece, sarebbe opportuno partire dall'identificazione degli *asset*, all'attribuzione a questi di un valore e, infine, all'analisi di come tali *asset* potrebbero essere danneggiati.

2.2. Comunicazione e consultazione

Il processo di *cyber-risk management* viene articolato in fasi distinte; le principali si articolano in *assessment* e *treatment*. A fianco di queste due fasi centrali si pongono due ulteriori attività che qualificano le modalità di svolgimento del processo di *risk management*, introducendo aspetti che incidono sull'attività di valutazione e trattamento del rischio. Tali attività a supporto consistono nell'attività di *comunicazione e consultazione* e nell'attività di *monitoraggio e revisione*. La prima delle due attività è oggetto di analisi in questo paragrafo.

È fondamentale che l'organizzazione fornisca, condivida e ottenga, in uno scambio reciproco continuo, informazioni con gli *stakeholder*[16] sia interni sia esterni all'organizzazione riguardo a diversi aspetti relativi alla gestione del rischio. La determinazione del livello di rischio, infatti, è spesso influenzata dalla percezione di chi sta valutando: è importante, quindi, che un'organizzazione riesca a raccogliere le varie "prospettive" di percezione del rischio in modo tale da poter avere una visione il quanto più possibile globale e completa, essenziale per trattare correttamente i rischi[17].

---

[16] Varie sono le definizioni date al concetto di *stakeholder*. Si riporta in nota la definizione data dalla norma UNI ISO 31000 sulla gestione del rischio, che traduce il termine *stakeholder* con "portatore di interesse", ossia come "persona o organizzazione che può influenzare o essere influenzata da, o percepire se stessa come influenzata da, una decisione o attività". Sul punto si veda UNI ISO 31000, *Gestione del rischio*, p. 6.

[17] Sul punto si veda quanto riportato nella norma ISO/IEC 27005:2011, p. 25.

La gestione della sotto-fase di *comunicazione e consultazione* ha come finalità, da un lato, garantire che il punto di vista degli *stakeholder* sia preso in considerazione durante le varie fasi del processo di gestione del rischio e nei relativi processi decisionali (per esempio relativamente alla scelta delle modalità di trattamento del rischio); dall'altro lato, aumentare la consapevolezza e il senso di responsabilità di tutti i soggetti coinvolti nel processo di *risk management*[18]. È essenziale che siano condivise, in particolare, le risultanze derivanti dalla fase di *risk assessment* e sulla presentazione del piano di trattamento dei rischi.

In relazione al *cyber-risk* questo sotto-processo, seppur ampiamente applicabile, presenta due principali peculiarità, entrambe legate alle caratteristiche intrinseche del *cyberspace* e alla sua estensione globale, che, in parte, ne rendono più complessa l'attuazione[19]. Una prima peculiarità attiene al fatto che gli *stakeholder*, potenzialmente, potrebbero essere distribuiti in qualsiasi punto del pianeta: ciò comporta una classificazione e categorizzazione dei vari portatori di interesse maggiormente dettagliata, nonché una riflessione ulteriore circa le modalità per fornire, condividere e ottenere informazioni rilevanti per la gestione del rischio.

Una seconda peculiarità, inoltre, è relativa alle minacce rappresentate da *hacker* e attaccanti in generale che potrebbero causare incidenti da qualsiasi parte del mondo con impatti considerevoli sui *cyber-system* dell'organizzazione: in questo caso, dunque, l'organizzazione dovrebbe prevedere dei meccanismi *real-time* di comunicazione con i vari *stakeholder* coinvolti in un eventuale attacco per uno scambio tempestivo delle informazioni.

L'organizzazione dovrebbe, inoltre, dotarsi di un proprio registro continuamente aggiornato, contenente informazioni riguardo a *cyber-threat*, vulnerabilità e incidenti, profili potenziali ed effettivi di avversari e strategie attuali e future di gestione del *cyber-risk*. Un'efficiente comunicazione e consultazione risultano fondamentali, in particolare, per la gestione degli incidenti, che deve essere idonea a garantire che le informazioni siano tempestivamente e puntualmente condivise per

[18] Sul punto si vd. U. SACCONE, *Governare il rischio*…, cit., pp. 246-247
[19] Cfr. P. PACE e A. PENNASILICO, "Cyber risk management", cit., pp. 34-35.

rispondere in maniera adeguata e arginare gli impatti dell'incidente stesso.

2.3. Definizione del contesto

La definizione del contesto rappresenta una sotto fase fondamentale del processo di *risk management*[20]: sulla base di questa vengono costruite le fasi di valutazione e trattamento del rischio. Nel corso della fase di definizione del contesto, infatti, sono definiti, da un lato, i perimetri all'interno dei quali considerare i rischi e, dall'altro, gli obiettivi generali che si intendono perseguire con il processo di *risk management*. Nella definizione del contesto viene stabilito l'ambiente nel quale l'organizzazione opera, considerando sia i fattori interni[21] (l'organizzazione nel complesso, compresa la propria articolazione in termini organizzativi), sia i fattori esterni[22] (l'ambiente nel quale l'organizzazione opera), compresi gli obiettivi di *business*[23]: sulla base di questi elementi, inoltre, vengono stabiliti *criteri di base*, essenziali per tutto il processo di *risk management*.

I *criteri di base* definiti in questa fase attengono, più nello specifico, all'approccio complessivo al *risk management* che l'organizzazione deve definire, identificando i criteri per la ponderazione del rischio (*risk*

[20] Per contesto si intende la «combinazione di fattori interni ed esterni che possono avere degli effetti sullo sviluppo e raggiungimento degli obiettivi di un'organizzazione». Sul punto si vd. la definizione data dalla norma ISO 9000:2015.

[21] La norma ISO/IEC 27005:2011 riporta, tra i fattori interni, la *governance*, la struttura organizzativa, ruoli e responsabilità; *policy*, obiettivi e strategie implementate per raggiugerli; le capacità in termini di risorse e conoscenza; la cultura dell'organizzazione; gli *standard*, le linee guida e i modelli adottati dall'organizzazione; la forma e l'estensione delle relazioni contrattuali.

[22] Tra i fattori esterni, la norma ISO/IEC 27005:2011 citata riporta: i fattori culturali, sociali, politici, legali, finanziari, tecnologici, economici, naturali e competitivi, sia internazionali che nazionali che regionali o locali; *trend* con impatti sugli obiettivi dell'organizzazione; e, infine, percezioni e valori degli *stakeholder* esterni.

[23] L'analisi degli obiettivi di *business* richiede l'elaborazione di un quadro complessivo di sintesi con l'indicazione degli obiettivi che risultano prioritari e necessari per l'organizzazione. Il quadro deve comprendere l'analisi degli obiettivi interni (relativi, per esempio, alla produttività) e degli obiettivi esterni (relativi, per esempio, alla penetrazione in un nuovo settore di mercato). Sul punto si vd. U. SACCONE, *Governare il rischio*…, cit., p. 252.

evaluation)[24], per gli impatti dei rischi sull'organizzazione[25] e per l'accettazione del rischio. In relazione a quest'ultimo aspetto (criteri per l'accettazione del rischio), l'organizzazione dovrebbe definire criteri di accettazione per i diversi livelli di rischio. Nella definizione dei criteri di accettazione l'organizzazione dovrebbe tener conto, inoltre, di alcuni fattori, quali l'utilizzo di più soglie con l'indicazione del livello di rischio desiderato, prevedendo la possibilità che vengano accettati anche i rischi che superano le soglie individuate; del rapporto tra il profitto e il rischio stimato di una certa attività; e, infine, dell'applicazione di diversi criteri di accettazione del rischio per le diverse classi di rischio individuate. I criteri dovrebbero essere stabiliti, infine, sulla base della durata del rischio (il rischio, infatti, può essere *temporaneo* – legato a varie contingenze – o *duraturo*), sia sulla base di altri criteri, quali quelli di *business* (in ordine, per esempio, al fatturato), quelli legali e regolatori, operativi, tecnologici, finanziari e sociali di contesto.

Definito il contesto, l'organizzazione deve identificare l'ambito specifico in cui deve essere effettuata la valutazione del rischio, identificando con l'ambito tutta l'organizzazione o una parte di essa. Nell'ambito del *cyber-risk management*, rispetto alla gestione del rischio in generale, è necessario che l'organizzazione, in questa fase, comprenda e documenti in quale modo i *cyber-system* utilizzano e si interfacciano con il *cyberspace*: ciò al fine di comprendere come e dove le *cyberthreat* possono agire, così come quali *asset* possono essere coinvolti dagli attacchi[26]. L'area così definita viene detta *superficie d'attacco*, ossia l'area comprensiva dei punti attraverso cui un attac-

[24] In relazione ai *risk evaluation criteria*, questi dovrebbero essere sviluppati tenendo in considerazione il valore strategico dei processi informativi aziendali, della criticità degli *information asset* coinvolti; i requisiti legali e contrattuali applicabili; l'importanza operativa e di *business* della disponibilità, dell'integrità e della disponibilità delle informazioni; e, infine, delle aspettative e percezioni degli *stakeholder*, nonché delle conseguenze negative sulla reputazione. Sul punto si vd. la norma ISO/IEC 27005:2011, pp. 10-11.

[25] Gli impatti dovrebbero essere specificati in termini di grado del danno o dei costi causati dall'organizzazione da un evento che incide sulla sicurezza delle informazioni, considerando vari elementi, tra cui: il livello di classificazione delle informazioni coinvolte; violazioni delle informazioni; perdite economiche; distruzioni di piani o di scadenze; danni alla reputazione.

[26] Cfr. P. PACE e A. PENNASILICO, "Cyber risk management", cit., p. 3

cante o un'altra fonte di minaccia potrebbe violare il perimetro dell'organizzazione, entrando senza autorizzazione all'interno dei *cyber-system*, sottraendo le informazioni ivi raccolte, immagazzinate e circolanti ovvero danneggiandone gli *asset* correlati. L'ambito così delineato generalmente comprende informazioni e infrastrutture informative, comprensive di *software*, servizi e reti; ma l'analisi deve comprendere anche eventuali impatti su *asset* ulteriori, quali la reputazione, l'immagine e i rischi legali, nonché impatti sul personale stesso[27].

2.4. Cyber-risk assessment

La fase di *risk assessment* è una fase centrale del processo di *risk management* e si articola, generalmente, in tre ulteriori sotto fasi: *risk identification*, *risk analysis* e *risk evaluation*. L'*assessment* include, quindi: l'identificazione delle fonti di minaccia, ossia di fonti che generano il rischio e comprende l'individuazione delle fonti di informazioni e lo sviluppo di una metodologia di riconoscimento dei rischi specifica[28], nonché l'individuazione delle vulnerabilità esistenti e dei controlli individuati per il trattamento dei rischi (*risk identification*); la stima del livello di rischio, calcolandone la verosimiglianza e gli impatti (*risk analysis*); e, infine, una prioritizzazione dei rischi, classificati in base ai criteri di valutazione stabiliti nella fase di definizione del contesto[29] (*risk evaluation*).

Il NIST descrive gli elementi essenziali che caratterizzano generalmente una *metodologia* di *risk assessment*[30]. Un primo elemento che caratterizza il *risk assessment* è la sua articolazione in *processo*. Ciò implica una distribuzione in fasi volte a definire, in primo luogo, una panoramica di "alto livello" sul processo di *risk assessment* in generale, le attività di preparazione necessarie, le attività per condurre operativamente il *risk assessment*, le attività per comunicarne i risultati e,

---

[27] Alcuni incidenti *cyber* possono infatti causare danni fisici, attentando alla vita delle persone e all'ambiente nel quale svolgono le proprie attività.
[28] Sul punto si vd., ancora, U. SACCONE, *Governare il rischio*…, cit., p. 254
[29] Cfr. la norma ISO/IEC 27005:2011, p. 13
[30] NIST, *Information security. The fundamentals*, Special Publication 800-30, Rev. 1, US Department of Commerce, Gaithersburg, 2012.

infine, le attività per mantenere i risultati della valutazione del rischio aggiornati in via continuativa.

In secondo luogo, l'*assessment* deve essere volto a realizzare un *modello del rischio* esplicito, che definisca i termini chiave, i fattori di rischio valutabili e le loro relazioni[31]. Tipicamente tra i fattori di rischio rientrano le *minacce*[32], le *vulnerabilità*[33], gli *impatti*[34], la *verosimiglianza*[35] e le *condizioni di predisposizione*.

---

[31] La documentazione del *modello di rischio* include l'identificazione dei fattori di rischio (definizioni, descrizioni, scale di valore) e l'identificazione delle relazioni tra questi fattori (relazioni concettuali), presentate in maniera descrittiva, nonché gli algoritmi per combinare i valori.

[32] Nel citato documento del NIST, per *minaccia* si intende «qualsiasi circostanza o evento che potrebbe impattare negativamente gli *asset* e le operazioni di un'organizzazione, gli individui, altre organizzazioni o lo stato tramite i sistemi informativi, attraverso l'accesso non autorizzato, la distruzione, la rivelazione o la modifica non autorizzati dell'informazione e/o una negazione del servizio». Le minacce sono causate dalle *threat source* (fonti di minaccia), generalmente caratterizzate dall'intento e dal metodo finalizzati allo sfruttamento di una vulnerabilità (*malicious*) o da una situazione che potrebbe accidentalmente sfruttare una vulnerabilità (*non-malicious*).

[33] Una *vulnerabilità*, secondo la prospettiva del NIST, è «una debolezza in un sistema informativo, in una procedura di sicurezza, nei controlli interni o nella loro implementazione che potrebbe essere sfruttata da una fonte di minaccia». La severità di una vulnerabilità può essere determinata attraverso l'estensione dell'impatto negativo, qualora una fonte di minaccia potesse sfruttarla. Le vulnerabilità potrebbero essere dovute, per esempio, a un'inadeguata implementazione dei controlli di sicurezza, ma potrebbero derivare anche da un cambiamento del contesto di operatività dell'organizzazione dovuto, per esempio, all'identificazione di nuovi obiettivi di *business*.

[34] Per *impatto* deve intendersi la "magnitudine" di un evento che potrebbe generare un danno a processi di *business* o verso gli *asset* di un'organizzazione, come conseguenza di violazione della confidenzialità, dell'integrità e della disponibilità delle informazioni. L'organizzazione, per determinare l'impatto, dovrebbe rendere espliciti: il processo utilizzato per condurre la determinazione degli impatti; le assunzioni relative alla determinazione dell'impatto; le fonti e i metodi utilizzati; e, infine, il razionale conclusivo raccolto con riguardo alla determinazione dell'impatto.

[35] Il termine *likelihood of occurence* è inteso come *verosimiglianza di accadimento*, ossia la «probabilità che una data minaccia sia in grado di sfruttare una determinata vulnerabilità (o una serie di vulnerabilità)». La *verosimiglianza di accadimento* del fattore di rischio risulta dalla combinazione della stima della verosimiglianza che l'evento minaccia venga avviato e una stima della verosimiglianza dell'impatto (inteso in termini di impatto negativo). Il documento NIST riprende, sul punto, la distinzione tra *malicious* e *non-malicious*. Per la prima tipologia di *cyberthreat*, la verosimiglianza