

IT Resiliency: dalla continuità operativa alla sopravvivenza del business

Perché la resilienza dei servizi IT è diventata una priorità di business, di brand e di governance — e cosa devono fare CIO, CTO e responsabili infrastrutture per costruirla.

Un whitepaper a cura di Angelo Maturi

Executive Summary 3

La criticità dei servizi IT oggi.....4

 Complessità e dipendenza crescenti.....4

 Il caso CrowdStrike: anatomia di un single point of failure globale.....4

 La dimensione Geopolitica.....4

La resilienza IT come priorità del CIO.....5

 Dalla cybersecurity al cyber resilience.....5

 Un tema da consiglio di amministrazione.....5

 Implicazione per i vertici IT.....5

Quanto costano i disservizi: i numeri.....6

 I benchmark di riferimento..... 6

 I costi nascosti.....6

 Costo orario del fermo per dimensione e settore (benchmark) - tabella.....6

Il quadro normativo: DORA, NIS2 e oltre.....7

 DORA - Digital Operational Resilience Act.....7

 NIS2 e il D.Lgs. 138/2024 in Italia.....7

 Dora o NIS2? Come si coordinano.....7

Le best practice: otto pilastri della resilienza IT.....8

 Dai pilastri all'azione.....8

Conclusioni.....9

Appendice - Fonti e riferimenti.....10

Executive Summary

La resilienza IT non può più essere considerata solo una questione tecnica confinata al data center: negli anni, è diventata sempre più un tema di sopravvivenza del business, di tutela del brand e di responsabilità degli organi di governo aziendali. Le organizzazioni moderne erogano valore attraverso servizi digitali interconnessi; quando questi servizi si fermano, a fermarsi non è "l'IT", ma il fatturato, la fiducia dei clienti e, sempre più spesso, il valore per gli azionisti.

La dimensione del fenomeno è ormai macroeconomica. Secondo la ricerca **The Hidden Costs of Downtime** condotta da Splunk (Cisco) con Oxford Economics, il costo aggregato del downtime non pianificato per le aziende Global 2000 ha raggiunto i **600 miliardi di dollari l'anno, in crescita del 50% in soli due anni**. L'impatto medio per singola organizzazione è di circa 95 milioni di dollari di ricavi persi all'anno, con un calo medio del 3,4% del valore azionario dopo un singolo incidente significativo.[1]

Che un singolo punto di fallimento possa propagarsi all'intera economia non è più un'ipotesi teorica: l'incidente CrowdStrike del luglio 2024 ha reso inutilizzabili circa 8,5 milioni di dispositivi Windows in poche ore, causando perdite dirette stimate in 5,4 miliardi di dollari alle sole aziende Fortune 500, con sanità, banche e trasporto aereo tra i settori più colpiti. [4,6]

Questa nuova consapevolezza si riflette nelle priorità dei vertici IT. Da diversi anni "cybersecurity e gestione del rischio" guida le agende dei CIO, e Gartner descrive un vero e proprio **"rebranding" della cybersecurity in cyber resilience**: l'obiettivo non è più solo impedire gli incidenti, ma garantire la capacità di assorbirli e recuperare rapidamente. Il 93% dei consigli di amministrazione considera ormai la sicurezza una minaccia diretta al valore per gli azionisti.[8,9]

Il tema ha infine una crescente valenza **geopolitica e regolamentare**. La sovranità digitale, la riduzione della dipendenza da pochi fornitori critici e la localizzazione delle forniture pesano sempre di più nelle scelte tecnologiche. Parallelamente, due interventi normativi europei — il regolamento **DORA** per il settore finanziario e la direttiva **NIS2** (recepita in Italia con il D.Lgs. 138/2024) — trasformano la resilienza operativa da buona pratica facoltativa a obbligo di legge, con responsabilità personali per gli organi apicali e sanzioni fino al 2% del fatturato globale. [13,16]

In sintesi:

Oggi la continuità dei servizi digitali coincide con la continuità del business. Garantirla non è più una scelta tecnica né una buona pratica: è una **responsabilità di governo**, misurabile in valore d'impresa e sancita dalla legge.

La criticità dei servizi IT oggi

Negli ultimi quindici anni i servizi IT sono passati dall'essere un supporto alle operazioni aziendali al costituirne la sostanza stessa. Banche che sono di fatto piattaforme software, ospedali che dipendono da cartelle cliniche elettroniche, catene logistiche orchestrate da sistemi gestionali: in tutti questi casi un'interruzione informatica si traduce immediatamente in un'interruzione del servizio reso al cliente o al cittadino.

1. Complessità e dipendenza crescenti

Tre forze rendono i servizi IT più critici e più fragili allo stesso tempo: l'aumento dell'interconnessione tra sistemi, la migrazione verso ambienti cloud e SaaS in cui il controllo sul disaster recovery è in parte ceduto al fornitore, e la concentrazione del mercato su un numero ristretto di provider di infrastruttura e sicurezza. Il risultato è che il rischio non cresce in modo lineare ma **si propaga: il guasto di un singolo fornitore può cadere a valle su migliaia di organizzazioni contemporaneamente.**

È anche per questo che la causa più frequente dei disservizi non è un evento esotico, ma il fattore umano e i processi: l'analisi dell'Uptime Institute indica che la maggioranza degli incidenti gravi deriva da errori di configurazione e da fallimenti nella gestione del cambiamento, ed è in larga parte prevenibile con processi migliori e rilevazione più tempestiva.^[12]

2. Il caso CrowdStrike: anatomia di un single point of failure globale

Il 19 luglio 2024 un aggiornamento difettoso del sensore Falcon di CrowdStrike ha mandato in crash circa **8,5 milioni di dispositivi Windows** in tutto il mondo — meno dell'1% del parco Windows globale, ma sufficiente a paralizzare aeroporti, banche, ospedali, emittenti televisive e servizi di emergenza. È stato definito il più grande blackout informatico della storia.^[6]

La società di analisi del rischio Parametrix ha stimato in **5,4 miliardi di dollari le perdite dirette per le sole aziende Fortune 500** (Microsoft esclusa), con una perdita media ponderata di circa 44 milioni per organizzazione e punte vicine ai 150 milioni per i comparti più esposti. Il settore sanitario è stato il più colpito (1,94 miliardi), seguito dal bancario (1,15 miliardi). Solo il 10-20% di queste perdite risultava coperto da assicurazione cyber.^[4,5]

La lezione per i vertici IT è evidente: non è stato un attacco, ma un aggiornamento di routine di un fornitore fidato. La resilienza non riguarda solo la difesa dagli avversari, ma la capacità di reggere il guasto di qualunque componente — inclusi i propri fornitori di sicurezza.

3. La dimensione Geopolitica

La resilienza IT è entrata nell'agenda geopolitica. La sovranità digitale e la riduzione della dipendenza da fornitori tecnologici globali sono ormai criteri espliciti nelle scelte di approvvigionamento: secondo Gartner, il 55% dei CIO governativi (esclusi gli USA) prevede di modificare il modo in cui ingaggia i fornitori tecnologici a causa delle tensioni geopolitiche e delle preoccupazioni di sovranità digitale, e la localizzazione del fornitore è diventata un fattore decisionale accanto a costo e scala.

^[10]

La resilienza IT come priorità del CIO

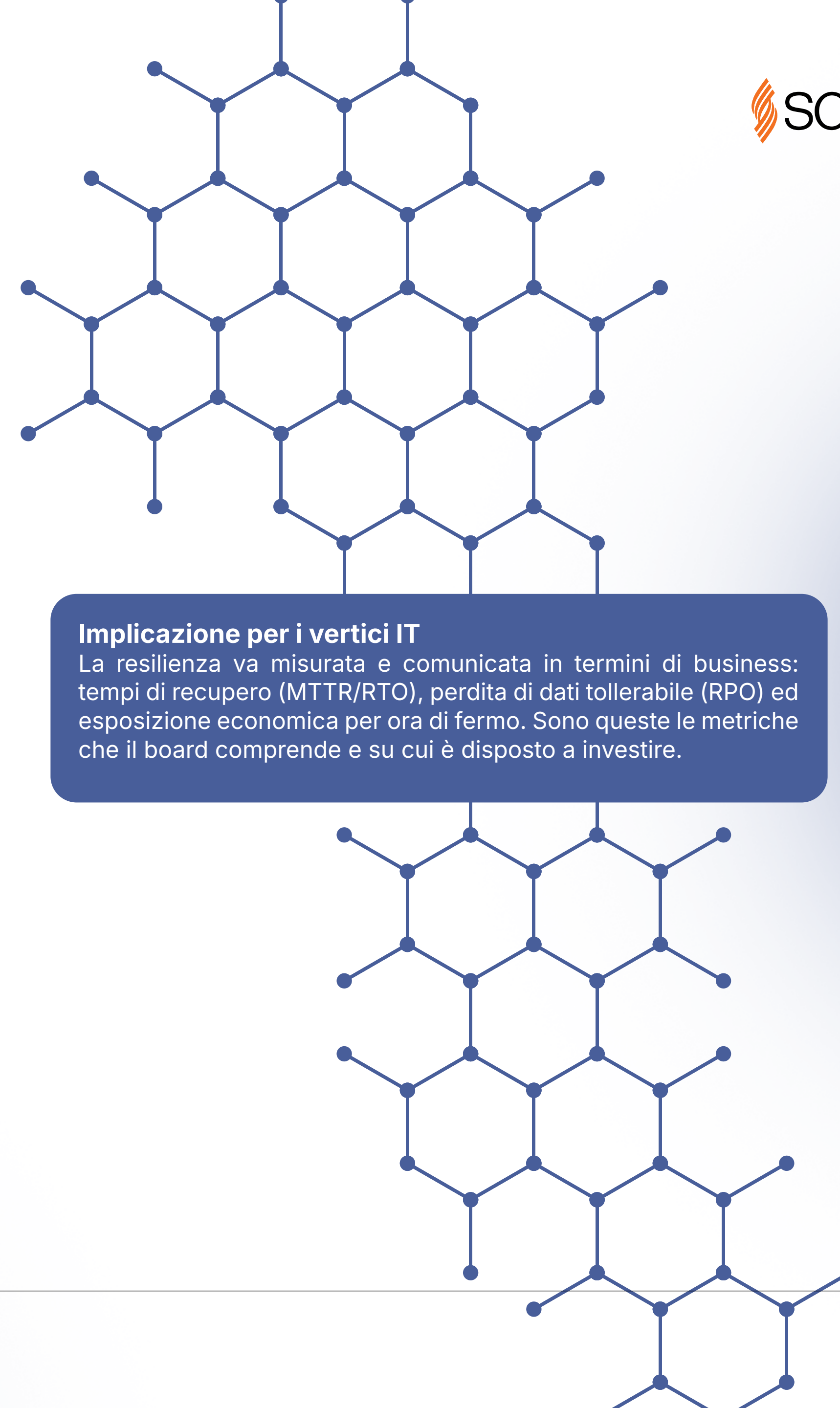
Le rilevazioni sulle priorità dei CIO convergono da anni su un punto: la gestione del rischio e la sicurezza occupano stabilmente le prime posizioni. Nelle survey Gartner condotte su oltre 1.400 dirigenti IT, "cybersecurity e gestione del rischio" è rimasta priorità numero uno per più anni consecutivi, affiancata oggi dall'operativizzazione dell'AI e dalla strategia dati.^[7]

1. Dalla cybersecurity alla cyber resilience

Il cambiamento più significativo è di paradigma. Gartner descrive nel rapporto **Predicts 2026** un vero e proprio rebranding del programma di cybersecurity in **cyber resilience**: poiché si dà ormai per scontato che gli incidenti siano inevitabili, l'attenzione si sposta dal tentativo di impedirli alla capacità di limitarne l'impatto e recuperare rapidamente. Nello stesso rapporto si prevede che entro il 2028 il 50% dei CISO si veda assegnata anche la responsabilità del disaster recovery, oltre a quella dell'incident response.^[8]

2. Un tema da consiglio di amministrazione

La resilienza ha smesso di essere un argomento tecnico per diventare una questione di governance. Secondo Gartner, il 93% dei consigli di amministrazione considera la cybersecurity una minaccia al valore per gli azionisti, spingendo i CIO a trattare la protezione come un risultato strategico di business e non come una funzione tecnica. Il CIO è sempre più chiamato a fare da "traduttore" tra il linguaggio del rischio tecnologico e quello degli obiettivi aziendali.^[9]



Quanto costano i disservizi: i numeri

Tradurre la resilienza in una decisione di investimento richiede di quantificare il costo dell'alternativa, cioè del fermo. I dati più recenti convergono su cifre che rendono il business case difficile da ignorare.

I benchmark di riferimento

- **15.000 dollari al minuto** è il costo medio del downtime per organizzazione secondo The Hidden Costs of Downtime 2026 di Splunk/Oxford Economics.^[1]
- **95 milioni di dollari di ricavi persi all'anno** per organizzazione — quasi il doppio rispetto al 2024 — e un calo medio del 3,4% del valore azionario dopo un singolo incidente.^[1]
- **Oltre il 90% delle aziende** mid-size e large dichiara che un'ora di fermo costa più di 300.000 dollari; il 41% colloca il costo tra 1 e 5 milioni di dollari l'ora (ITIC 2024-2025).^[11]
- **600 miliardi di dollari l'anno** è il costo aggregato per le Global 2000, in crescita del 50% in due anni rispetto ai 400 miliardi del 2024.^[1,3]

I costi nascosti

Le perdite dirette — ricavi mancati, straordinari, penali contrattuali — sono solo la parte visibile. I costi nascosti, più lenti ma spesso più pesanti, comprendono l'abbandono dei clienti, l'erosione reputazionale e le sanzioni regolamentari. La ricerca rileva che dopo un incidente servono in media circa 60 giorni perché la percezione del brand si riprenda, e che le aziende arrivano a spendere cifre molto elevate in campagne di recupero della fiducia.^[1,12]

Costo orario del fermo per dimensione e settore (benchmark)

Categoria	Costo orario	Nota
Piccole imprese	da ~25.000 \$/ora	impatto sproporzionato sul cash flow
Medie / grandi imprese	oltre 300.000 \$/ora (90%)	ITIC 2024-2025
Grandi enterprise (fascia alta)	1 – 5 mln \$/ora (41%)	ITIC 2024-2025
Servizi finanziari	oltre 5 mln \$/ora	settore tra i più esposti
Sanità	oltre 1 mln \$/ora	rischio anche per la sicurezza dei pazienti

Fonti: ITIC 2024-2025 (via Gatling); Splunk/Oxford Economics 2026. Valori indicativi a fini di benchmark

Il quadro normativo: DORA, NIS2 e oltre

La resilienza operativa digitale è oggi un obbligo di legge. Due interventi europei ne hanno ridefinito il perimetro, spostando il baricentro dalla mera prevenzione alla capacità dimostrabile di resistere, rispondere e recuperare.

DORA — Digital Operational Resilience Act

Il regolamento (UE) 2022/2554, noto come DORA, **si applica dal 17 gennaio 2025** e crea un quadro armonizzato di gestione del rischio ICT per il settore finanziario europeo. Essendo un regolamento — e non una direttiva — è direttamente applicabile in tutti gli Stati membri, senza bisogno di recepimento nazionale, e riguarda circa 22.000 entità finanziarie oltre ai loro fornitori ICT. ^[13,15]

I cinque pilastri di DORA:

- **Gestione del rischio ICT** — governance e framework documentati.
- **Gestione e notifica degli incidenti** — classificazione e segnalazione degli incidenti ICT gravi entro tempi stretti.
- **Test di resilienza operativa digitale** — incluso il threat-led penetration testing (TLPT) ogni tre anni per le entità più critiche.
- **Gestione del rischio di terze parti ICT** — obblighi contrattuali su exit strategy, audit e livelli di servizio.
- **Condivisione delle informazioni** sulle minacce informatiche.

Una novità rilevante è l'estensione della vigilanza diretta ai fornitori ICT designati come critici: a novembre 2025 le Autorità europee di vigilanza ne hanno individuati 19, tra cui i principali provider cloud. Le sanzioni possono arrivare al 2% del fatturato annuo mondiale per le entità, e fino all'1% del fatturato giornaliero per i fornitori critici. ^[14,15]

DORA o NIS2? Come si coordinano

Per il settore finanziario DORA è la normativa specialistica e prevale su NIS2 in caso di sovrapposizione (principio di lex specialis). Le organizzazioni non finanziarie nei settori critici ricadono invece sotto NIS2. Molte realtà dovranno inoltre coordinare questi obblighi con il Cyber Resilience Act e la direttiva CER sulle infrastrutture critiche.

NIS2 e il D.Lgs. 138/2024 in Italia

La direttiva (UE) 2022/2555 (NIS2) ha un ambito molto più ampio: copre numerosi settori "altamente critici" e "critici", distinguendo tra **soggetti essenziali e soggetti importanti**. L'Italia l'ha recepita con il **D.Lgs. 138/2024, in vigore dal 16 ottobre 2024**. Secondo i dati dell'Agenzia per la Cybersicurezza Nazionale (ACN), oltre 20.000 organizzazioni sono state inserite nell'elenco nazionale, di cui più di 5.000 classificate come essenziali. ^[16,17]

Il 2026 è l'anno del passaggio dalla compliance formale a quella sostanziale.

Le scadenze chiave: dal 15 gennaio 2026 è pienamente operativo il regime di notifica degli incidenti significativi al CSIRT Italia (pre-notifica entro 24 ore, notifica entro 72 ore); le misure di sicurezza di base vanno implementate entro l'autunno; e da ottobre 2026 l'ACN potrà avviare le attività ispettive. ^[16,18]

Per i soggetti essenziali sono previste **43 misure e 116 requisiti** articolati su gestione del rischio, governance, continuità operativa, gestione degli incidenti e formazione. Particolarmente significativa è la **responsabilità personale degli organi apicali** (art. 23): amministratori e organi direttivi devono approvare e vigilare sulle misure, rispondendo delle violazioni. Le sanzioni arrivano a 10 milioni di euro o al 2% del fatturato per i soggetti essenziali, e a 7 milioni o all'1,4% per quelli importanti. ^[17,18]

Le best practice: otto pilastri della resilienza IT

Costruire resilienza significa agire su due piani inscindibili: i processi e la tecnologia. Di seguito otto pilastri di alto livello che ogni organizzazione dovrebbe presidiare, indipendentemente dal settore. Non sono un elenco di prodotti, ma capacità da sviluppare e mantenere nel tempo.

Governance e ruoli dedicati.

La resilienza ha bisogno di un proprietario. Definire ruoli, responsabilità e gruppi di lavoro dedicati — con un mandato chiaro dal board e accountability degli organi apicali — è il primo passo. È anche un requisito esplicito di NIS2 e DORA, che attribuiscono la supervisione agli organi di amministrazione.^[17]

Assessment periodico della postura IT.

Non si può migliorare ciò che non si misura. Una valutazione strutturata e ricorrente della maturità — architetture, processi, dipendenze, fornitori — consente di individuare le lacune prioritarie e di indirizzare gli investimenti dove l'esposizione è maggiore, invece di distribuirli uniformemente.

Architetture conformi alle best practice di settore.

Eliminare i single point of failure, progettare ridondanza e isolamento dei guasti, adottare strategie multi-region o multi-cloud dove la criticità lo richiede. Il caso CrowdStrike ha mostrato quanto sia pericoloso che un singolo componente — anche di un fornitore fidato — possa propagare un guasto all'intero sistema.^[4]

Backup immutabili e strategia 3-2-1-1-0.

I backup sono diventati il bersaglio primario degli attacchi: gli operatori ransomware colpiscono l'infrastruttura di backup prima di cifrare la produzione. La risposta è mantenere almeno una copia immutabile (WORM), separata logicamente e fisicamente, con amministrazione distinta da quella di produzione, secondo il modello 3-2-1-1-0.^[20,21]

Isolated Recovery Environment / Clean Room.

Ripristinare direttamente in produzione rischia di reintrodurre il malware. Un ambiente di ripristino isolato (IRE) o "clean room" — logicamente e fisicamente separato dalla produzione — consente di restaurare, scansionare e validare i sistemi in quarantena prima di rimetterli in linea, partendo dal presupposto che l'ambiente primario possa essere compromesso.^[19,20]

Test e simulazioni periodiche.

Un piano di disaster recovery non testato è un'ipotesi, non una garanzia. Esercitazioni regolari di ripristino (restore drill), simulazioni di incidente e pratiche di chaos engineering riducono il tempo medio di recupero e fanno emergere le debolezze prima che lo faccia un incidente reale. I test periodici sono anche un requisito normativo (TLPT in DORA).^[14]

Incident response e runbook documentati.

La velocità della risposta determina il costo totale dell'incidente. Procedure di incident response documentate, runbook aggiornati, catene di escalation chiare e responsabilità definite comprimono l'MTTR. I team che provano la risposta recuperano più in fretta e perdono meno. NIS2 impone tempi di notifica stringenti che richiedono processi già rodati.^[18]

Gestione del rischio di terze parti e supply chain.

La resilienza è forte quanto l'anello più debole della catena di fornitura. Mappare le dipendenze dai fornitori critici, valutarne la postura, negoziare clausole contrattuali su livelli di servizio, audit ed exit strategy è oggi un obbligo esplicito di DORA e un'aspettativa di NIS2 anche per i fornitori dei soggetti in perimetro.^[14,16]

Dai pilastri all'azione

Questi otto pilastri si rafforzano a vicenda: la governance indirizza gli assessment, gli assessment guidano gli interventi su architetture e backup, i test ne verificano l'efficacia e l'incident response ne raccoglie i frutti nel momento critico. La maturità non sta nell'adottare un singolo strumento, ma nel far funzionare insieme l'intero sistema.

Conclusioni

La resilienza IT è oggi una delle poche aree in cui rischio tecnologico, valore economico, reputazione del brand e conformità normativa convergono nello stesso punto. I numeri — 600 miliardi di dollari l'anno per le Global 2000, fino a 5 milioni l'ora per i settori più esposti, un calo del 3,4% del valore azionario dopo un singolo incidente — dimostrano che il fermo non è un inconveniente operativo, ma un evento finanziario di rilievo.^[1]

Allo stesso tempo, DORA e NIS2 hanno reso la resilienza un obbligo dimostrabile, con responsabilità che risalgono fino agli organi di governo. La buona notizia è che le organizzazioni più mature — i cosiddetti “resilience leader” — non sono quelle che spendono di più, ma quelle che investono in modo più strategico: allineano la tecnologia agli obiettivi di business, danno contesto alle persone e progettano sistemi che “si piegano senza spezzarsi”.^[1]

Il punto di partenza: conoscere la propria postura

Prima di investire conviene sapere dove si è. Un assessment strutturato della postura di resilienza IT — che metta a confronto governance, architetture, strategie di backup e ripristino, test e gestione dei fornitori con le best practice di settore e gli obblighi normativi — è il modo più efficace per trasformare gli otto pilastri di questo documento in un piano d'azione concreto e prioritizzato.

Per valutare la maturità della vostra organizzazione e definire una roadmap di resilienza, è possibile richiedere un assessment dedicato.

I dati e le affermazioni di questo white paper si basano sulle fonti elencate di seguito, citate nel testo con il numero corrispondente tra parentesi quadre.

[1] Splunk (Cisco) & Oxford Economics — The Hidden Costs of Downtime 2026 — comunicato “The \$600 Billion Wake-up Call”. <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2026/m05/the-600-billion-wake-up-call-new-splunk-research-reveals-downtime-is-a-systemic-business-crisis.html>

[2] Splunk (Cisco) — The Hidden Costs of Downtime — pagina di report ufficiale. https://www.splunk.com/en_us/form/the-hidden-costs-of-downtime.html

[3] Splunk & Oxford Economics — Edizione 2024 — \$400B annui per le Global 2000 (comunicato .conf24). https://www.splunk.com/en_us/newsroom/press-releases/2024/conf24-splunk-report-shows-downtime-costs-global-2000-companies-400-billion-annually.html

[4] Parametrix / CNN Business — CrowdStrike outage: cause e costo per le Fortune 500 (\$5,4 mld). <https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause>

[5] Cybersecurity Dive — CrowdStrike: perdite dirette \$5,4B per le Fortune 500. <https://www.cybersecuritydive.com/news/crowdstrike-cost-fortune-500-losses-cyber-insurance/722396/>

[6] Wikipedia — 2024 CrowdStrike-related IT outages (cronologia e impatti). https://en.wikipedia.org/wiki/2024_CrowdStrike-related_IT_outages

[7] Gartner / Evanta — Top 3 Priorities for CIOs in 2026 (survey 1.400 IT executive). <https://www.evanta.com/resources/cio/survey-report/top-3-priorities-for-cios-in-2026>

[8] Gartner / Bitsight — Predicts 2026: Cybersecurity Program Rebrands to Cyber Resilience. <https://www.bitsight.com/resources/gartner-predicts-2026-cyber-resilience-the-future-of-cybersecurity>

[9] Gartner — The Top CIO Challenges (93% dei board: cyber come minaccia al valore). <https://www.gartner.com/en/articles/cio-challenges>

[10] Gartner — Survey: 52% dei CIO governativi prevede budget IT in crescita nel 2026 (geopolitica e sovranità). <https://www.gartner.com/en/newsroom/press-releases/2025-11-26-gartner-survey-reveals-52-percent-of-government-cios-expect-it-budgets-to-increase-in-2026>

[11] ITIC / Gatling — The cost of downtime — sintesi benchmark ITIC 2024-2025. <https://gatling.io/blog/the-cost-of-downtime>

[12] Uptime Institute / TechTarget — The cost of downtime: cause umane e di processo (Annual Outage Analysis). <https://www.techtarget.com/searchdatabackup/feature/The-cost-of-downtime-and-how-businesses-can-avoid-it>

[13] EIOPA (UE) — Digital Operational Resilience Act (DORA) — panoramica ufficiale. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[14] IBM — What Is the Digital Operational Resilience Act (DORA)? (TLPT, fornitori critici). <https://www.ibm.com/think/topics/digital-operational-resilience-act>

[15] Yousign — DORA Compliance: 5 pilastri, ~22.000 entità, 19 fornitori critici, sanzioni. <https://yousign.com/blog/dora-regulation>

[16] ICT Security Magazine — NIS2 e D.Lgs. 138/2024: gli adempimenti 2026. <https://www.ictsecuritymagazine.com/articoli/nis2-e-d-lgs-138-2024/>

[17] EC News — La Direttiva NIS2 nel 2026 (43 misure/116 requisiti, governance, scadenze). <https://www.ecnews.it/legale/mondo-professione/privacy/la-direttiva-nis2-nel-2026-2/>

[18] Agenda Digitale — NIS2: come adeguarsi ai nuovi obblighi cyber (scadenze e sanzioni). <https://www.agendadigitale.eu/sicurezza/obblighi-di-cyber-sicurezza-come-adeguarsi-alla-direttiva-nis2/>

[19] Google Cloud (Mandiant) — Isolated Recovery Environments: a critical layer in modern cyber resilience. <https://cloud.google.com/blog/topics/threat-intelligence/isolated-recovery-environments-modern-cyber-resilience>

[20] Cohesity — What Is Ransomware Recovery? Clean-room recovery e backup immutabili. <https://www.cohesity.com/glossary/ransomware-recovery/>

[21] Datapath — Backup Immutability Checklist (modello 3-2-1-1-0). <https://www.mydatapath.com/blog/backup-immutability-checklist-ransomware-resilient-it-environments/>

Nota metodologica: le cifre economiche provengono in prevalenza da ricerche di mercato (Splunk/Oxford Economics, ITIC, Parametrix) e vanno intese come benchmark indicativi; i valori effettivi variano per dimensione, settore e profilo di rischio dell'organizzazione. I riferimenti normativi sono aggiornati a giugno 2026.

Un white paper a cura di:



Angelo Maturi

Head of CIO Initiative HUB

E-mail:
amaturi@sorint.com

Per ulteriori dettagli o approfondimenti scrivici a:
welisten@sorint.com



BUILDING GREAT TECHNOLOGY

www.sorint.com