QBE
At the heart of it

Construction: dalla progettazione alle violazioni cyber

La trasformazione digitale sta ridefinendo il rischio informatico nei progetti di costruzione e infrastrutturali

Tre messaggi chiave:

1. Perché l’adozione di sistemi digitali sta ampliando la superficie di attacco informatico nel settore delle costruzioni

2. Come gli incidenti cyber possono impattare sull'operatività dei cantieri

3. Perché la resilienza informatica deve estendersi lungo tutta la catena di fornitura e ai sistemi operativi

Introduzione

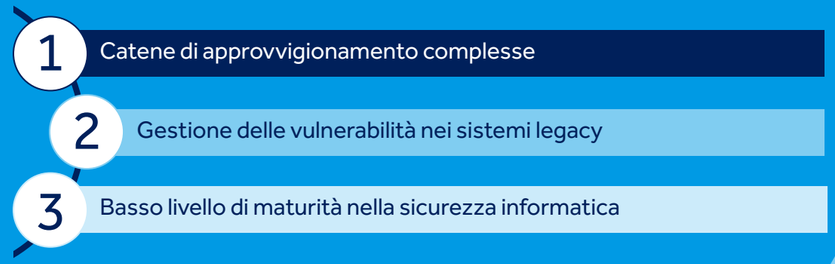
La trasformazione digitale sta ridefinendo il settore edile, ma la governance del rischio non sempre riesce a tenere il passo. Man mano che le organizzazioni adottano nuove tecnologie e digitalizzano la realizzazione dei progetti, emergono nuove esposizioni nei sistemi aziendali e negli ambienti operativi, con conseguenti nuovi rischi di interruzione digitale e impatti nel mondo reale.

I grandi progetti di costruzione si basano su supply chain complesse, tempistiche serrate e strumenti digitali interconnessi, il che porta ad un aumento significativo dei rischi informatici. I sistemi legacy, le soluzioni digitali implementate rapidamente e le connessioni con terze parti non adeguatamente protette possono introdurre vulnerabilità che gli attori delle minacce sono sempre più in grado di sfruttare. In questo contesto in evoluzione, le autorità di regolamentazione pongono crescente enfasi su una solida gestione del rischio informatico nei sistemi informativi (IT), nella tecnologia operativa (OT)[1] e lungo la catena dei fornitori terzi.

Con il continuo accelerare della digitalizzazione, le società del settore edile e delle infrastrutture si trovano ad affrontare rischi informatici e digitali in aumento. Gli elevati requisiti di continuità operativa e la dipendenza da numerosi appaltatori e fornitori rendono il comparto un bersaglio particolarmente attraente per gli attori di ransomware ed estorsione. Allo stesso tempo, le crescenti tensioni geopolitiche hanno alimentato un forte aumento del cybercrime rivolto alle infrastrutture critiche e ai settori correlati.

Anche i rischi di convergenza (ossia quelli che emergono quando IT, OT, digitale, persone e processi fisici convergono, creando superfici di attacco più ampie e interdipendenti) sono in aumento. I criminali sfruttano i sistemi legacy poco protetti e la crescente integrazione tra ambienti IT e OT per massimizzare gli attacchi o ottenere vantaggi finanziari/geopolitici. Le interruzioni dei sistemi critici e/o dei fornitori possono comportare fermi d'attività, controversie contrattuali, rischi per la sicurezza e conseguenze più ampie di natura finanziaria, normativa e/o reputazionale.

Figura 1: I 3 principali rischi digitali per il settore edile secondo gli esperti di Control Risks[2]

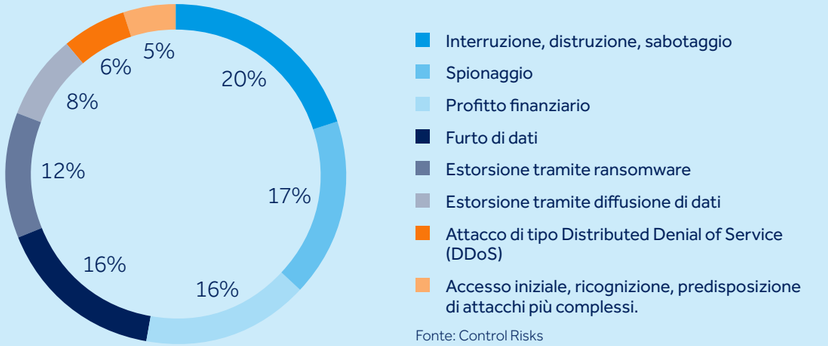


1 Tecnologia operativa: hardware e software che rilevano o provocano cambiamenti nel mondo fisico, attraverso il monitoraggio e il controllo diretti di dispositivi fisici, apparecchiature/processi industriali e infrastrutture.
2 Sulla base di un'indagine condotta tra gli esperti senior di Control Risks specializzati in rischi digitali, attivi nelle funzioni di cyber threat intelligence, cyber advisory e risposta agli incidenti.

L’adozione di soluzioni digitali e tecnologie emergenti aumenta l’esposizione ai rischi informatici nel settore edile

Negli ultimi anni il settore edile ha accelerato gli sforzi per digitalizzare le operazioni. Le organizzazioni adottano sempre più tecnologie emergenti quali l’intelligenza artificiale (IA), i dispositivi dell’Internet delle cose (IoT)[3] e strumenti specifici del comparto, tra cui il Building Information Modelling (BIM).

Figura 2: Obiettivi degli incidenti informatici che colpiscono il settore edile e i settori delle infrastrutture critiche correlati (quota di incidenti significativi, 2023-2026)



Fonte: Control Risks

La digitalizzazione offre chiari vantaggi, tra cui un miglior monitoraggio della sicurezza, un controllo più efficace della conformità, l’automazione dei processi aziendali e una maggiore efficienza nella realizzazione dei progetti. Tecnologie come il BIM, ad esempio, possono essere utilizzate dagli appaltatori edili per collaborare da remoto sullo stesso progetto, garantendo che tutte le parti coinvolte condividano una visione aggiornata delle informazioni chiave, quali disegni e modelli degli edifici.

Tuttavia, l’integrazione di nuovi sistemi digitali amplia le superfici di attacco informatico e introduce nuove forme di rischio provenienti da una pluralità di attori. Sebbene la collaborazione remota basata sul cloud possa semplificare il coordinamento, le infrastrutture in rete sono regolarmente prese di mira da criminali informatici e attori statali che cercano di sottrarre dati sensibili o individuare punti di accesso a infrastrutture IT aziendali più ampie.

Le stesse tipologie di vulnerabilità riguardano anche altre tecnologie sempre più integrate nelle operazioni di costruzione. Ad esempio, un report del 2025 ha rilevato un aumento del 410% su base annua delle attività malware IoT rivolte al settore edile.[4] Il continuo utilizzo di sistemi legacy, le catene di approvvigionamento altamente complesse e le tempistiche stringenti dei progetti complicano ulteriormente la gestione del rischio informatico.

3 L’Internet delle cose (IoT), o comunicazione machine-to-machine (M2M), descrive i miliardi di oggetti e dispositivi collegati a Internet che comunicano tra loro con un intervento umano minimo o nullo. Tali oggetti includono elettrodomestici, automobili, carte di credito, ascensori e telecamere a circuito chiuso.
4 https://www.zscaler.com/resources/industry-reports/threatlabz-mobile-iot-ot-report.pdf

I recenti dati di settore evidenziano la portata di questa trasformazione:

56%

degli investitori nel settore edile intende destinare maggiori fondi all'adozione dell'IA.[5]

61%

dei leader del settore dichiara di attribuire priorità strategica agli investimenti in tecnologia e innovazione.[6]

34%

dei professionisti ha dichiarato di essere impegnato in fasi iniziali di test pilota per l'implementazione dell'IA, mentre un ulteriore 14,5% ha riferito di utilizzare regolarmente l'IA in uno o più processi aziendali.[7]

USD $17,72bn

Il mercato globale delle costruzioni BIM è stato valutato 4,38 miliardi di USD nel 2024 e si prevede che raggiungerà i 17,72 miliardi di USD entro il 2034.[8]

> **Nel settore edile, gli attacchi informatici non si limitano più a compromettere la riservatezza delle informazioni; interrompono la realizzazione dei progetti, bloccano le operazioni, mettono sotto pressione le catene di approvvigionamento e dimostrano quanto rapidamente la dipendenza dal digitale possa trasformarsi in rischio operativo. Man mano che il settore continua ad adottare digitalizzazione e automazione, la realtà delle minacce e dei rischi provenienti dal dominio digitale sta diventando sempre più concreta**
>
> **Partner in Digital Risks**
> Control Risks

5 https://www.rics.org/news-insights/artificial-intelligence-in-construction-report#
6 https://kpmg.com/dk/en/insights/market-trends/global-construction-survey.html
7 https://www.rics.org/news-insights/artificial-intelligence-in-construction-report#
8 https://finance.yahoo.com/news/bim-construction-industry-research-report-125300365.html

Le estorsioni e le tensioni geopolitiche alimentano i rischi di interruzione per il settore edile e delle infrastrutture

79%

Il 79% degli esperti di Control Risks ritiene che il ransomware sia la minaccia con maggiore probabilità di avere un impatto significativo sulle organizzazioni del settore edile

Il settore edile è particolarmente vulnerabile alle interruzioni operative. I progetti sono generalmente caratterizzati da tempistiche serrate e si basano su catene di approvvigionamento complesse, per cui i ritardi possono rapidamente comportare un aumento dei costi e conseguenze contrattuali. Queste caratteristiche rendono il settore un bersaglio attraente per gli attori di ransomware ed estorsione, che spesso sfruttano la sensibilità delle organizzazioni alle interruzioni operative per aumentare la pressione per il pagamento dei riscatti.

Un'indagine del 2023 sulla resilienza dei datacenter nel settore edile ha rilevato che per il 77% degli intervistati cinque giorni è il tempo massimo tollerabile senza accesso alla documentazione di progetto prima di subire gravi impatti operativi.[9]

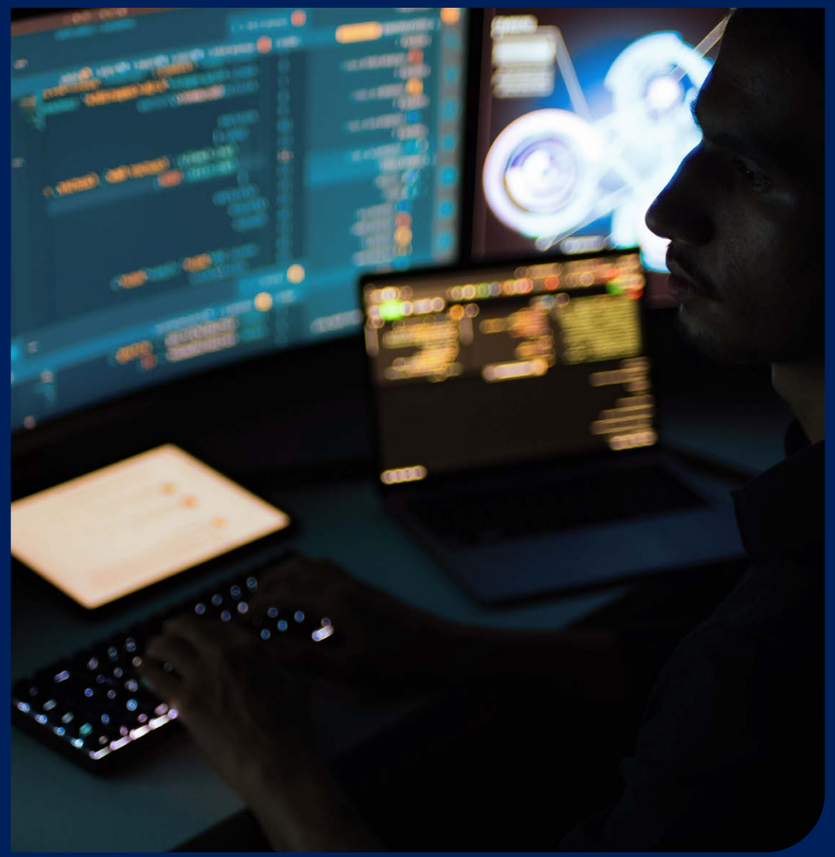
Nel 2025, gli incidenti ransomware hanno causato in media 24 giorni di inattività per episodio. Nel settore edile, interruzioni di questa durata possono causare ritardi significativi, incidere su subappaltatori e fornitori terzi e generare danni reputazionali a lungo termine.[10]

I costi degli incidenti variano significativamente a seconda di fattori quali l'entità dell'interruzione operativa e l'eventuale sottrazione di dati sensibili.

Tuttavia, un ordine di grandezza dei costi per le imprese di costruzione emerge da un caso di estorsione tramite furto di dati avvenuto nel 2020 nel Regno Unito: in quell'occasione, i costi di ripristino e consulenza hanno raggiunto i 7 milioni di sterline, a cui si sono aggiunte sanzioni dell'Information Commissioner pari a 4,4 milioni di sterline.[11]

9 https://www.construction.com/reports/enhanced-data-resilience-will-help-the-design-and-construction-industry-face-the-risks-that-impact-their-businesses/
10 https://www.totalassure.com/blog/average-ransomware-recovery-time-2025
11 https://constructionmanagement.co.uk/poor-cyber-security-cost-interserve-11m-to-clean-up/

Caso Di Studio



Operazione di doppia estorsione prende di mira una società di costruzioni e ingegneria civile

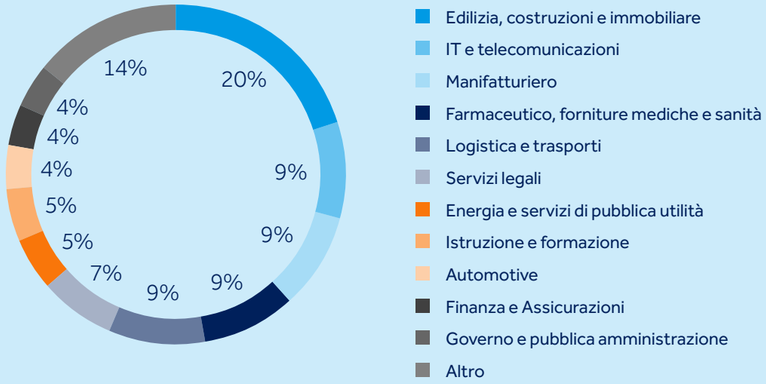
Nel febbraio 2023, la società britannica di costruzioni e ingegneria civile Lagan Specialist Contracting Group (Lagan SCG) è stata colpita da un'operazione di doppia estorsione. L'incidente è stato successivamente attribuito a Lockbit, un'organizzazione criminale informatica altamente sofisticata con una lunga storia di operazioni ransomware ad alto impatto.

La società colpita ha subito il furto di una notevole quantità di dati sensibili relativi ai dipendenti, inclusi numeri di passaporto e coordinate bancarie. Il set di dati sottratto è stato successivamente pubblicato sul dark web, con il rischio di ulteriori attività fraudolente. Nel maggio 2023 è stata avviata un'azione legale collettiva con l'obiettivo di indagare su come sia stata possibile la violazione dei dati sensibili e su come questa abbia inciso sulla sicurezza dei dipendenti.[12]

Non risultano dati pubblici relativi all'impatto subito da Lagan SCG per l'incidente. Tuttavia, solo poche settimane prima lo stesso attore della minaccia aveva preso di mira Royal Mail con modalità simili, causando gravi interruzioni delle operazioni aziendali. Secondo quanto riportato, Royal Mail ha speso 10 milioni di sterline in misure di ripristino e resilienza informatica, a dimostrazione del potenziale impatto finanziario di questi attacchi.

12 https://www.kpl-databreach.co.uk/lagan-specialist-contracting-group/

Figura 3: Settori presi di mira negli incidenti ransomware nel 2025[13]



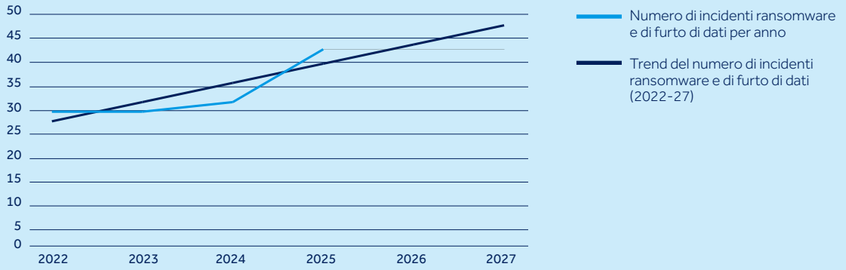
Fonte: Control Risks

I gruppi di cyber crime stanno inoltre sfruttando l'espansione delle superfici di attacco all'interno del settore. Man mano che le imprese edili implementano connessioni remote attraverso reti di appaltatori e fornitori, ad esempio per facilitare sistemi BIM collaborativi, il numero di potenziali punti di accesso per i criminali si moltiplica.

Analogamente, gli attori di ransomware sono diventati sempre più capaci di colpire le infrastrutture OT. Un report sulla sicurezza informatica pubblicato a febbraio ha rilevato che nel 2025 119 gruppi hanno preso di mira organizzazioni industriali, con un aumento del 49% su base annua. Complessivamente, questi gruppi hanno colpito 526 organizzazioni nel settore delle costruzioni, con significative interruzioni operative osservate in tutti i casi in cui il ransomware è stato propagato negli ambienti OT.[14]

Quando ciò avviene, il ransomware può compromettere i sistemi di controllo industriale (ICS), ossia software, hardware e tecnologie di rete specializzate che monitorano e controllano i processi industriali, causando l'arresto dei macchinari fisici e limitando o bloccando completamente il controllo degli utenti su sensori, sistemi di sicurezza integrati e componenti fisici quali valvole e pompe.

Figura 4: Operazioni di estorsione tramite ransomware e furti di dati ai danni dei settori dell'edilizia e delle infrastrutture critiche correlate (sulla base di incidenti significativi a livello globale, 2022-2025)



Fonte: Control Risks

13 I dati di Control Risks incudono gli incidenti che hanno preso di mira i settori edilizio, delle costruzioni e immobiliare, inclusi il real estate, la gestione immobiliare e altri sottosettori correlati. I dati di Control Risks indicano che il comparto dell'edilizia, delle costruzioni e dell'immobiliare è stato il principale bersaglio degli attacchi ransomware nel 2025. Sebbene il settore delle costruzioni sia stato uno dei principali bersagli degli attori di ransomware nel 2025, questi dati sono influenzati anche da un numero significativo di incidenti che hanno colpito entità del settore edilizio e immobiliare.

14 https://5943619.hs-sites.com/hubfs/312-Year-in-Review/2026/Dragos-2026-OT-Cybersecurity-Report-A-Year-in-Review.pdf?hsCtaAttrib=205683189348

Caso Di Studio

Un General Contractor preso di mira in un incidente di doppia estorsione[15]

Nel marzo 2024, l'impresa generale di costruzioni statunitense Skender Construction è stata presa di mira in un'operazione di doppia estorsione da parte di un criminale non identificato.

Nell'ambito dell'operazione, l'attore della minaccia ha ottenuto accesso ed esfiltrato dati sensibili relativi a oltre 1.000 individui. I dati sottratti includevano, secondo quanto riportato, informazioni sui passaporti e numeri di previdenza sociale, il che ha costituito un aggravamento del rischio di attività fraudolente ai danni delle persone coinvolte nel breve-medio termine.

L'attore della minaccia è inoltre riuscito a cifrare i sistemi IT associati a Skender Construction. Tuttavia, la società aveva predisposto backup dei dati per proteggere la propria operatività dall'impatto derivante da un eventuale attacco, riuscendo così a ripristinare completamente i sistemi in tempi rapidi e a limitare l'impatto operativo dell'incidente ransomware.

15 https://www.constructiondive.com/news/skender-ransomware-attack-chicago-maine/712844/

Al di là degli attacchi intenzionali, dal 2024 si è registrato un significativo aumento degli incidenti informatici gravi prendono di mira le infrastrutture nazionali critiche (CNI) nei Paesi occidentali.[16]

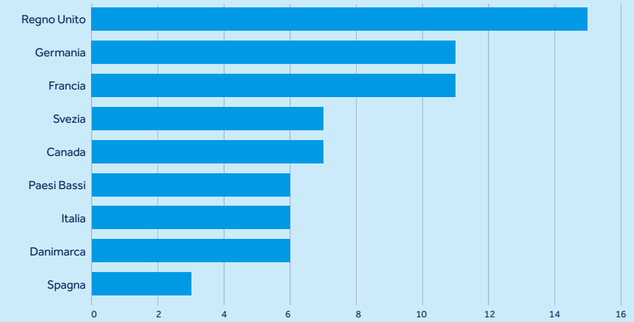
Questi episodi spesso si inseriscono in contesti di tensioni geopolitiche più ampie, come quelle tra la Russia e i membri della NATO, o tra Stati Uniti, Israele e Iran. Gli attacchi informatici fanno sempre più parte, insomma, di strategie più ampie di guerra ibrida.

Sebbene le società edili raramente rappresentino il bersaglio primario di tali operazioni, la loro prossimità alle infrastrutture nazionali critiche, in virtù del loro ruolo nella progettazione e costruzione, le rende spesso vittime sia intenzionali sia collaterali. Una società edile, ad esempio, può essere compromessa come conseguenza di un attacco che prende di mira un operatore di infrastrutture critiche oppure subire interruzioni a causa di un incidente informatico che colpisce direttamente un fornitore o un partner.

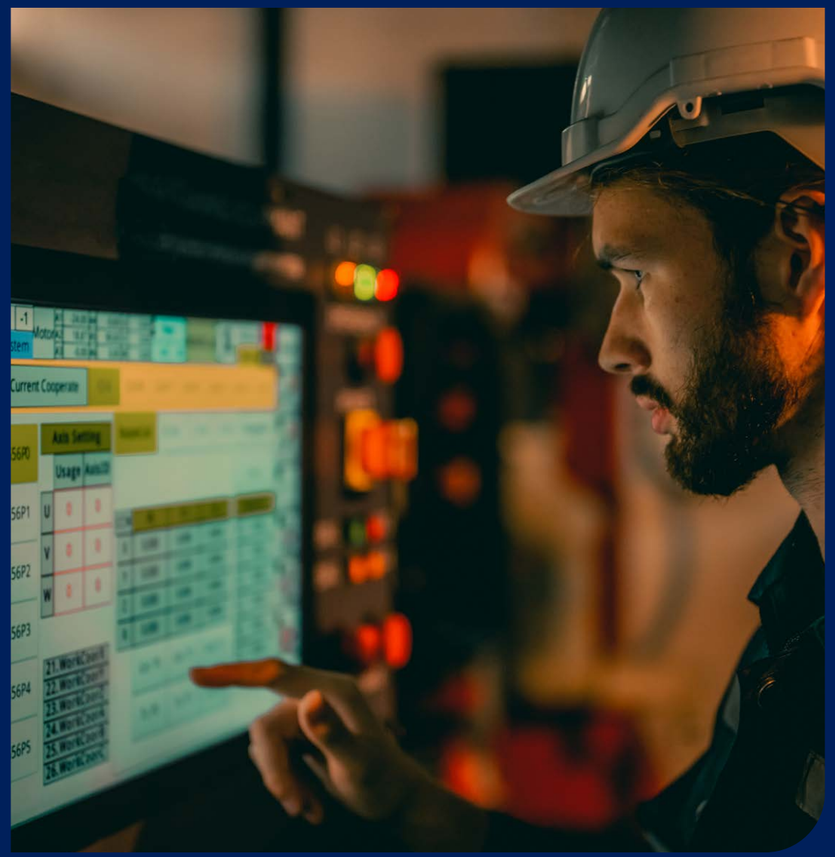
> **La convergenza tra progetti edilizi e sviluppo delle infrastrutture nazionali critiche è destinata a favorire attività di targeting del settore motivate o influenzate da fattori geopolitici, laddove ostacoli la realizzazione di progetti critici. Ciò è particolarmente rilevante negli Stati in cui la situazione geopolitica è vicina a un punto critico – sono quelli dove i cyber criminali legati a gruppi statali cercheranno di esercitare un impatto economico sui propri rivali."**
>
> **Global Head of Cyber Threat Intelligence**
> Control Risks

16 Control Risks

Figura 5: Numero di incidenti gravi causati da gruppi legati a interessi statali che hanno preso di mira Canada, Danimarca, Francia, Germania, Italia, Paesi Bassi, Spagna, Svezia e Regno Unito
(incidenti significativi osservati, 2022-2026)



Fonte: Control Risks



Un cyberattivista filo-russo prende di mira infrastrutture idriche

Nel 2024, il gruppo filo-russo Z-Pentest ha condotto un attacco informatico distruttivo contro un'azienda idrica danese. Dopo aver ottenuto l'accesso ai sistemi di controllo, il gruppo ha manipolato i livelli di pressione dell'acqua, causando la rottura di almeno tre condutture e lasciando 500 famiglie senza acqua per diverse ore.[17]

Nell'aprile 2025, lo stesso attore ha preso di mira una diga norvegese, aprendo le valvole di scarico e rilasciando milioni di litri d'acqua nell'arco di quattro ore prima che gli operatori riacquisissero il controllo del sistema. Le cause dell'attacco sono riconducibili a una protezione inadeguata delle password di un pannello di controllo accessibile via web e alla mancata corretta separazione tra sistemi OT e sistemi IT connessi a Internet. [18]

Da allora si sono verificati incidenti simili, tra cui un tentativo di attacco informatico contro un impianto idrico in Polonia.[19] Queste operazioni fanno parte di un più ampio modello di attività informatiche dirompenti che prendono di mira le infrastrutture nazionali critiche. Sebbene tali attacchi abbiano finora colpito principalmente i servizi di pubblica utilità e le entità del settore energetico, è probabile che in futuro tattiche analoghe possano interessare anche settori adiacenti, come quello delle costruzioni.

17 https://www.euronews.com/2025/12/19/denmark-blames-russia-for-cyberattacks-on-water-utility-and-election-websites
18 https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/
19 https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/

La convergenza tra IT e OT amplia la superficie di attacco e aumenta il rischio operativo

Con l'accelerazione della digitalizzazione, le società edili integrano sempre più i sistemi IT con gli ambienti OT. Se implementata in modo efficace, la convergenza IT/OT può semplificare le operazioni consentendo la comunicazione automatizzata tra i sistemi e migliorando sia la supervisione dei progetti sia i processi chiave.

Tuttavia, tale convergenza accresce anche il rischio informatico. Se i sistemi non sono integrati in modo sicuro, gli attori delle minacce che ottengono accesso alle reti IT possono essere in grado di spostarsi negli ambienti OT senza essere rilevati. Un report del 2026 ha rilevato che l'81% degli incidenti OT del 2025[20] possono essere ricondotti ad una segmentazione inadeguata tra sistemi IT e OT. [21]

I rischi derivanti da vulnerabilità architetturali nella convergenza IT/OT sono ulteriormente aggravati dal continuo utilizzo di sistemi legacy, dalla concessione di accessi remoti a terzi e da pratiche di sicurezza informatica inadeguate, quali il riutilizzo delle credenziali.

Gli attori delle minacce sono sempre più determinati a prendere di mira direttamente i sistemi OT.[22] Dal 2024 si è registrato un aumento degli incidenti informatici che coinvolgono proxy legati a interessi statali e mirati ai sistemi di controllo industriale (ICS) nel settore dei servizi di pubblica utilità in Europa e Nord America.

Anche i criminali informatici colpiscono sempre più spesso gli ambienti OT. Secondo quanto riferito da un fornitore specializzato in sicurezza OT, nel 2025 il 23% dei casi di incident response gestiti ha riguardato attacchi ransomware rivolti a sistemi OT, con impatti diretti sulla continuità operativa.

Parallelamente, molti cyber criminali continuano a sfruttare le debolezze dei sistemi legacy: nel 2025, il 67,5% dei tentativi di exploit ha infatti interessato vulnerabilità note e presenti da tempo.[23]

Poiché molti sistemi OT si basano su software o hardware obsoleti che non possono essere facilmente aggiornati, questa tendenza genera significative criticità in materia di sicurezza. Sfruttando questa vulnerabilità, gli attori delle minacce possono accedere alle reti spostarsi lateralmente tra i sistemi e, in ultima analisi, compromettere ambienti operativi d'importanza critica.

Con il crescente interesse verso l'OT quale bersaglio di attacchi informatici, aumenta anche il rischio per le società di costruzione. Oltre agli impatti operativi immediati e ai rischi per la sicurezza nei cantieri, tali interruzioni possono comportare gravi perdite finanziarie, controversie contrattuali, danni reputazionali a lungo termine e persino conseguenze normative.

20 Separazione fisica o tecnica inadeguata tra sistemi IT e infrastruttura OT, che consente a un attore della minaccia di spostarsi più facilmente tra i sistemi senza essere rilevato e di condurre attività dannose sia nell'infrastruttura IT sia in quella OT. Ad esempio, un sistema OT può essere configurato in modo da consentire una comunicazione diretta e non protetta con sistemi IT aziendali, quali i server di posta elettronica, permettendo a un attore della minaccia di utilizzare un server compromesso per eseguire comandi sul sistema OT.
21 https://5943619.hs-sites.com/hubfs/312-Year-in-Review/2026/Dragos-2026-OT-Cybersecurity-Report-A-Year-in-Review.pdf?
22 https://5943619.hs-sites.com/hubfs/312-Year-in-Review/2026/Dragos-2026-OT-Cybersecurity-Report-A-Year-in-Review.pdf?
23 https://medium.com/s2wblog/detailed-analysis-of-recent-trends-in-known-exploited-vulnerabilities-c81678a47f39

Le pressioni normative introducono nuove aspettative per la gestione del rischio informatico

Figura 6: I tre principali fattori alla base dell'interesse verso il settore delle costruzioni, secondo gli esperti di Control Risks

1. Basso livello percepito di maturità nella sicurezza informatica
2. Catene di approvvigionamento complesse e network di terze parti
3. Sistemi e smart building scarsamente protetti

Le autorità di regolamentazione stanno adottando una visione sempre più ampia della sicurezza informatica e della protezione delle infrastrutture nazionali critiche. Quadri normativi quali la Direttiva aggiornata dell'Unione Europea sulle reti e i sistemi informativi (NIS2), i previsti aggiornamenti delle normative equivalenti nel Regno Unito e la proposta canadese di legge sulla protezione dei sistemi informatici critici (CCSPA) introducono nuove aspettative per le organizzazioni che operano nelle infrastrutture nazionali critiche e lungo le relative catene di approvvigionamento.

È probabile che tali requisiti normativi vengano estesi lungo le catene di approvvigionamento, interessando anche le imprese di costruzione che supportano progetti infrastrutturali.

Di conseguenza, le organizzazioni del settore dovranno adottare un approccio più strutturato, basato sul rischio e orientato alla resilienza nella gestione del rischio informatico. Ciò include il rafforzamento della governance, il miglioramento delle pratiche di sicurezza IT/OT e la predisposizione di solidi piani di risposta agli incidenti.

Figura 7: Componenti principali di una gestione efficace del rischio informatico

Governance
- Implementare una gestione completa del rischio informatico
- Stabilire supervisione e responsabilità a livello dirigenziale

Risposta agli incidenti
- Rivedere e aggiornare i piani di risposta agli incidenti e di continuità operativa, garantendo la conformità ai requisiti
- Effettuare test periodici rispetto a scenari di minaccia reali

Gestione del rischio nella catena di approvvigionamento
- Effettuare valutazioni del rischio dei fornitori
- Includere la sicurezza informatica nei requisiti contrattuali

Misure tecniche di mitigazione
- Aggiornare i controlli di sicurezza, inclusa la segmentazione di rete tra sistemi IT e OT, il controllo degli accessi, gli strumenti di rilevamento e risposta sugli endpoint (EDR) e l'applicazione degli aggiornamenti
- Mappare i sistemi legacy e sviluppare strategie di mitigazione per i sistemi che non rientrano nei normali cicli di aggiornamento

Formazione e sensibilizzazione
- Svolgere regolarmente attività di formazione e sensibilizzazione per i dipendenti
- Incoraggiare i dipendenti a segnalare attività sospette

Il punto di vista degli underwriter

Stefano Pompeo
Cyber Senior Underwriter QBE Italia

Dal punto di vista della sottoscrizione dei rischi informatici, il settore delle costruzioni occupa una posizione centrale nella valutazione delle interruzioni operative. L'ampia diffusione delle tecnologie e le modalità con cui vengono utilizzate rendono infatti il settore particolarmente esposto.

Le imprese edili integrano in tempo reale sistemi IT, tecnologie operative, piattaforme di terze parti e reti della catena di approvvigionamento, spesso su più progetti attivi contemporaneamente. Ne deriva un livello di connettività e complessità elevato, che può essere sfruttato dagli attori delle minacce.

In Italia, queste tendenze si sviluppano parallelamente a un contesto normativo e commerciale sempre più stringente. L'influenza della direttiva NIS2 si riflette nelle catene di approvvigionamento e nei requisiti dei clienti, in particolare per le imprese che operano nei mercati europei, oltre che in quello italiano. Più in generale, il rischio informatico viene inquadrato come parte della resilienza operativa, con autorità di regolamentazione ed enti pubblici che si concentrano sulla capacità delle imprese di continuare a operare in presenza di interruzioni, non solo di prevenire gli incidenti. Le aspettative di base sono inoltre influenzate dalle linee guida dell'Agenzia per la Cybersicurezza Nazionale (ACN) e, per molte aziende, dimostrare la resilienza informatica sta diventando un prerequisito per aggiudicarsi incarichi, non soltanto un requisito tecnico da soddisfare.

Questo cambiamento si riflette chiaramente anche nella natura degli incidenti. Oggi molte violazioni non si limitano più alla perdita di dati o alla compromissione della privacy, ma hanno effetti diretti sulle operazioni: interrompono i flussi di lavoro, bloccano l'accesso a sistemi critici e, in alcuni casi, incidono sull'ambiente fisico attraverso sistemi operativi connessi. In sostanza, il confine tra rischio informatico e rischio operativo può considerarsi ormai superato.

Dal punto di vista della sottoscrizione, è significativo osservare come molti dei fattori alla base degli incidenti più gravi non siano particolarmente sofisticati. Spesso derivano da debolezze ben note, come sistemi legacy difficili da aggiornare, una segmentazione insufficiente tra gli ambienti, tecniche di ingegneria sociale o fornitori storici che finiscono per diventare punti di accesso involontari.

Le aziende che adottano un approccio più strutturato a questi elementi di base possono ridurre in modo significativo la propria esposizione al rischio. La segmentazione tra ambienti IT e OT, ad esempio, resta una delle misure più efficaci per limitare l'impatto di un incidente. Allo stesso modo, migliorare la visibilità sui sistemi legacy e intervenire sulle vulnerabilità note consente di eliminare alcuni dei vettori di attacco più comuni. Infine, è fondamentale che il personale sia adeguatamente formato per riconoscere tentativi di phishing, sia via e-mail sia attraverso telefonate fraudolente.

È necessario andare oltre un approccio basato esclusivamente sulla prevenzione. Sono altrettanto cruciali risposte rapide, chiare ed efficaci, fondate su piani di risposta agli incidenti testati, strutture decisionali ben definite e una comprensione realistica dei tempi di ripristino.

Sondaggio
Nell'ambito del presente rapporto, abbiamo intervistato 20 esperti senior della practice Digital Risks di Control Risks per raccogliere il loro punto di vista sulle principali minacce, sui rischi e sulle vulnerabilità nel settore dell'edilizia e delle infrastrutture. Gli intervistati provengono dai team EMEA, APAC e Americhe di Control Risks, con sedi a Londra, Berlino, Copenaghen, Hong Kong, New York, Washington, Sydney e Bogotà.

Il sondaggio include le risposte di consulenti esperti, responsabili di practice e della maggior parte dei Partner nelle funzioni Threat Intelligence, Cyber Advisory e Incident Response di Control Risks. Quando facciamo riferimento a dati o citazioni degli "esperti di Control Risks", ci basiamo sui risultati qualitativi e quantitativi emersi dal sondaggio.

Per i broker, è proprio su questo terreno che il dialogo con i clienti sta evolvendo. Le aziende sono oggi meno interessate a minacce informatiche astratte e più focalizzate sulle conseguenze concrete di un incidente per il loro business: per quanto tempo le attività potrebbero fermarsi, quale impatto avrebbero sui progetti in corso e con quale rapidità sarebbe possibile tornare operativi.

Si tratta di un cambiamento rilevante, perché nel settore edile ciò che viene assicurato, in ultima analisi, è una combinazione sempre più stretta tra rischio informatico e rischio di interruzione dell'attività.

Per maggiori informazioni su questo report, visita **qbeitalia.com** o contattaci scrivendo a **qbemilan@it.qbe.com**

QBE European Operations
QBE Europe SA/NV
Rappresentanza Generale per l'Italia
Via Melchiorre Gioia 8
20124 Milano
Italy
+39 02 3626 3500

QBEitalia.com

This report was produced by QBE with Control Risks.

QBE
At the heart of it

1220126/2605-IT