Helion

DEPOZITE & LOGISTICĂ

5

TOP INCIDENTE DE SECURITATE

2024-2026

Helion

5 TOP INCIDENTE DE SECURITATE

DEPOZITE & LOGISTICĂ

Furturile și brețele de securitate din depozite și centre logistice sunt o amenințare majoră pentru lanțurile de aprovizionare. Ele pot varia de la jafuri organizate, ce exploatează vulnerabilități fizice, până la furturi interne realizate de angajați cu acces privilegiat. Consecințele depășesc pierderile financiare: reputația companiei, continuitatea operațiunilor și încrederea clienților pot fi grav afectate. Într-o eră a digitalizării și automatizării, securitatea trebuie privită holistic, combinând bariere fizice, tehnologii avansate de monitorizare și politici ferme de protecție cibernetică.

În acest material am colectat **5 studii de caz de rezonanță** privind brețele de securitate din industria logistică, pentru a ilustra concret riscurile și lecțiile învățate.

© Helion 2026

1

FedEx

Furtul de iPhone-uri în valoare de ~$2M



Poză simbol

FedEx | Furtul de iPhone-uri în valoare de ~$2M

Context general

Două persoane au pretins că sunt angajații companiei autorizate să preia transportul de electronice. Ele au ridicat dintr-un depozit FedEx 38 de cutii cu iPhone-uri 17 Pro Max, în valoare de aproape 2 milioane USD.



Locație: SUA, FLORIDA
Anul: 2026

Cauze și vulnerabilități

- Verificarea insuficientă a identității: documentele prezentate de infractori nu au fost confirmate direct cu operatorul logistic real.
- Accesul neautorizat în zona de încărcare: infractorii au folosit un camion închiriat pentru preluarea mărfii.
- Lipsa unei baze de date cu vehicule autorizate și a unui mecanism de verificare a numerelor de înmatriculare.
- Absența unei autorizări suplimentare pentru mărfurile de mare valoare.

Impact

- **Reputație afectată** pentru operatorul logistic prin asocierea cu deficiențe în verificarea identității și autorizarea ridicării mărfurilor.
- **Riscuri operaționale**: întârzierea livrării de marfă cu valoare ridicată, alocarea de resurse suplimentare pentru investigații interne.
- **Compromiterea siguranței lanțului logistic** de către persoane care au folosit identități false.

Lecții învățate

- **Sistem ANPR** în zona de încărcare care verifică automat numerele de înmatriculare. Astfel, camionul închiriat ar fi putut fi identificat ca neautorizat.
- Verificarea identității prin mai multe metode, inclusiv metode de **control acces**.
- Utilizarea **dispozitivelor de localizare** și a **alertelor în timp real**, împreună cu supravegherea video.

© Helion 2026

2

CEVA Logistics

Furturi de marfă de peste $18.3M



Poză simbol

CEVA Logistics | Furturi de marfă de peste $18.3M

Context general

Au avut loc opt incidente separate în care au fost sustrase semiremorci încărcate cu electronice de mare valoare în valoare totală de peste 18,3 milioane USD (produse Apple, AMD, Verizon, Lenovo).



Locație: SUA, CALIFORNIA
Perioada: ultimele 12 luni

Cauze și vulnerabilități

- Externalizarea încărcăturilor (outsourcing) către transportatori neverificați.
- Parcări/depozite nesecurizate: remorcile sunt lăsate în yard-uri de depozit fără protecție adecvată.
- GPS neactivat în cazul unei remorci sustrase cu produse în valoare de 15M USD;
- Posibil complice intern (insider) și verificări slabe de identificare/acces neautorizat pentru persoane și vehicule.

Impact

- **Pierderi financiare** de zeci de milioane USD pentru Ceva Logistics – în 2024-2025 au fost estimate pierderi de peste 18,3 milioane USD.
- **Reputație afectată,** risc ridicat pentru clienți și parteneri – furturile repetate sub managementul Ceva au generat îngrijorare publică și discuții în industrie.
- **Riscul operațional:** întreruperi, gestionarea riscurilor sporite, costuri crescute.

Lecții învățate

- **Selectarea și verificarea transportatorilor** terți trebuie să fie riguroasă — nu doar pe hârtie, ci cu audit și monitorizare continuă.
- **Yard-urile de depozit** trebuie **securizate** fizic (garduri, iluminat, control acces) și monitorizate constant (sistem CCTV funcțional).
- Toate remorcile ar trebui dotate cu **GPS, și tracker-e active**; dacă sunt neactivate, devin inutile ca măsură de securitate.

© Helion 2026

3

Jingdong

Furtul a peste 50.000 de dispozitive electronice



Poză simbol

Jingdong | Furtul a peste 50.000 de dispozitive electronice

Context general

Un grup organizat a sustras peste 50.000 de dispozitive electronice, inclusiv telefoane, tablete, laptop-uri și căști. Prejudiciul inițial a fost estimat la 37M de euro, dar ulterior JD.com a afirmat că pierderile sunt mult mai mici.



Locație: FRANȚA, DUGNY
Anul: 2025

Cauze și vulnerabilități

- Neutralizarea sistemului de supraveghere video de către infractori
- Sistemul de alarmă nu funcționa corect
- Compromiterea supravegherii video și nefuncționarea alarmei au lăsat depozitul vulnerabil fără un mecanism alternativ de protecție
- Rețea organizată: membrii grupării au acționat sistematic, folosind metode coordonate
- Protecție insuficientă pentru stocurile de mare valoare: 30 de paleți au putut fi scoși din depozit fără alertarea autorităților.

Impact

- **Impact comercial în perioada de vârf.** Furtul s-a produs înainte de Crăciun, într-un moment cu volum ridicat de comenzi.
- **Afectarea reputației într-un moment cheie** pentru JD.com când abia își lansase platforma de e-commerce Joybuy în Franța.
- **Riscuri operaționale:** reorganizarea temporară a activității, întârzieri în procesarea comenzilor, costuri crescute de asigurare și securitate

Lecții învățate

- **Securitate stratificată** care să împiedice accesul în depozit chiar dacă o măsură de protecție este compromisă.
- **Supraveghere video inteligentă**, senzori de mișcare, alerte dispecerat și verificări suplimentare în perioadele critice.
- **Mentenanța sistemelor de securitate** și verificarea periodică a sistemelor de alarmă

© Helion 2026

4

GardaWorld

Jaful numerar de ~$30M



Poză simbol

GardaWorld | Jaful numerar de ~$30M

Context general

Unul dintre cele mai mari jafuri de numerar din istoria Los Angelesului: hoții au pătruns depozit de numerar operată de GardaWorld și au reușit să spargă atât clădirea, cât și seiful, plecând cu până la 30 de milioane USD.



Locație: SUA, CALIFORNIA
Anul: 2024

Cauze și vulnerabilități

- Sisteme de alarmă compromise: mai multe alarme au fost declanșate înainte și în timpul jafului; unele au fost tratate drept „false”, ceea ce a redus vigilența.
- Furtul a fost descoperit abia când seiful a fost deschis a doua zi.
- Posibilă complicitate internă: succesul operațiunii sugerează acces la informații privilegiate despre clădire și despre volumele de numerar.
- Lipsa redundanței: seiful nu părea dotat cu senzori seismici sau sisteme de detecție directă.

Impact

- **Pierdere directă**: aproximativ 30 milioane USD cash.
- **Reputație**: GardaWorld a intrat sub scrutin public și mediatic privind măsurile sale de securitate.
- **Operațional**: investigație federală și locală, verificări extinse la alte locații similare.

Lecții învățate

- **Redundanță obligatorie**: două sisteme de alarmă independente și senzori de vibrație/seismici direct pe seif.
- **Auditul și testarea** continuă a sistemelor de securitate pentru remedia punctele vulnerabile.
- **Verificarea angajaților**, acces diferențiat la informații, audituri regulate.

© Helion 2026

5

CHO America

Furt din depozit
de ulei de măsline
de ~$2,5M

Poză simbol

CHO America | Furt din depozit de ulei de măsline de ~$2,5M

Context general

Un depozit din Texas, unde era stocat ulei de măsline premium marca Terra Delyssa, a fost ținta unui jaf. Hoții au sustras 18 paleți încărcați cu recipiente de ulei, în valoare estimată la 2,5 milioane USD.



Locație: SUA, TEXAS
Anul: 2024

Cauze și vulnerabilități

- Acces fizic direct la depozit: hoții au reușit să intre și să manevreze marfă voluminoasă (18 paleți).
- Protecție insuficientă: lipsa unei monitorizări stricte și a alarmelor care să detecteze mișcarea de marfă mare.
- Planificare avansată: operațiunea necesită camioane, personal și timp, ceea ce sugerează fie complicitate internă, fie recunoaștere anterioară a obiectivului.

Impact

- **Blocaje logistice**: dispariția a 18 paleți afectează lanțul de aprovizionare al brandului Terra Delyssa.
- **Costuri de recuperare**: implicarea poliției, investigații, acoperire prin asigurări.
- **Imagine și încredere**: reputația furnizorului și a distribuitorului este afectată.

Lecții învățate

- **Valoarea nu e doar în numerar** sau bijuterii: și bunurile alimentare premium pot atrage jafuri organizate.
- **Securitate adecvată pentru volume mari**: camere, senzori și alarme adaptate pentru detectarea mutării paleților întregi.
- **Control acces și audit extern**: verificări regulate pentru a depista complicități interne sau breșe de procedură.

© Helion 2026

Helion

ESTE DEPOZITUL SAU LANȚUL LOGISTIC ÎN SIGURANȚĂ?

Studiile de caz arată că furturile din depozite și lanțuri logistice nu mai vizează doar bani sau bunuri de lux, ci și produse alimentare premium sau materiale de construcții. Toate incidentele au avut în comun breșe de securitate exploatate de grupuri organizate, uneori cu ajutor intern, iar pierderile financiare și reputaționale au fost semnificative.

PRINCIPALELE LECȚII ÎNVĂȚATE

Redundanța sistemelor de securitate este esențială (alarme independente, senzori seismici, monitorizare 24/7).

Controlul accesului și prevenirea amenințărilor interne reprezintă factori critici — verificarea personalului și limitarea accesului pe zone.

Tehnologii avansate precum etichetarea RFID, GPS și sisteme inteligente de analiză video pot reduce semnificativ riscurile.

Protecție proporțională cu valoarea stocului: nu doar cash sau electronice necesită măsuri stricte, ci și bunuri aparent „banale” cu valoare de piață mare.

Coordonare și comunicare între locații, parteneri și autorități sunt vitale pentru detectarea tiparelor și recuperarea prejudiciilor.

Audit și testare continuă a sistemelor de securitate pentru a descoperi vulnerabilitățile înainte de a fi exploatate.

Helion

RECOMANDĂRI PENTRU SECURITATEA LOGISTICĂ ȘI A DEPOZITELOR

1. Securizare perimetrală și fizică robustă (garduri, iluminat, bariere, acces diferențiat).

2. Monitorizare în timp real prin CCTV, senzori de mișcare și alarme conectate la centre de intervenție.

3. Implementarea redundanței: alarme multiple, senzori direct pe seifuri sau paleți, trackere GPS pe remorci și containere.

4. Procese stricte de verificare a partenerilor logistici și a personalului (screening, audituri externe, rotație).

5. Digitalizare și trasabilitate: RFID, coduri unice și soluții de supply chain visibility pentru bunurile de valoare.

6. Politici antifurt stratificate: zone cu acces controlat pentru produse premium, depozitare separată și inventariere frecventă.

© Helion 2026

Helion

Helion este un integrator de soluții avansate de securitate, cu o experiență de peste 30 de ani. Compania oferă servicii complete de securitate fizică și cibernetică, precum și platforme ERP pentru optimizarea proceselor organizaționale.

De la înființare, Helion a instalat sisteme de securizare în peste 6000 de obiective. La ora actuală, Helion S.A. are în mentenanță peste 800 de obiective pentru diferite categorii de clienți. 50 de obiective sunt de interes strategic.

Puncte de lucru permanente: București, Oradea, Cluj, Timișoara

Email: contact@helion.ro

Telefon: +40 725 144 444

www.helion.ro

Resurse

https://www.nbcmiami.com/news/local/man-arrested-in-brazen-2-million-iphone-heist-in-doral-authorities-say/3788197/
https://www.freightwaves.com/news/cargo-theft
https://www.scmp.com/economy/global-economy/article/3337610/burglary-jdcom-warehouse-france-prompts-investigation-speculation
https://eu.usatoday.com/story/news/nation/2024/04/23/30-million-cash-heist-los-angeles/73424069007/
https://nypost.com/2024/10/08/us-news/2-5m-worth-of-premium-terra-delyssa-olive-oil-stolen-from-texas-warehouse