The 22nd Economic International Conference
Challenges and Opportunities for a Sustainable Development
Stefan cel Mare University of Suceava, 2026

ORGANIZATIONAL RESILIENCE: A META-ANALYTICAL FRAMEWORK FOR HEALTHCARE CYBERSECURITY (2021-2025)

Petronela Alice GRIGORESCU
Alexandru Cătălin NEAGU
Dan Marius COMAN
Marian SOCOLIUC

Context & Motivation

- Digital transformation of hospitals (IoMT, EHR, telemedicine) has created systemic vulnerabilities alongside undeniable clinical benefits.
- Cyberattacks are no longer limited to data confidentiality — they are a direct threat to human life.
- Healthcare recorded the highest average data breach cost for the 14th consecutive year: $10.93M per incident (IBM Security 2024).
- "Cybersecurity is no longer an optional feature of hospital management; it is a core component of clinical resilience."

Research Objectives & Hypotheses

Research Objectives

- **Identify dominant attack vectors** in healthcare cybersecurity during 2021–2025
- **Quantify the financial and operational impact** of cyber incidents on healthcare systems
- **Assess the effectiveness of current defensive strategies** (including AI-based solutions)
- **Examine the clinical impact** of cyberattacks on patient safety and quality of care
- **Test four research hypotheses** at the intersection of outdated technology, human vulnerability, and emerging cyber-extortion strategies

Hypotheses

- **H1: Digitalisation without Zero Trust**
- **H2: Triple extortion & reputational impact**
- **H3: Legacy systems as primary vector**
- **H4: Training reduces social engineering ≥30%**

Evolution of Cyberattack Costs (2021–2025)

Year	Total Cost (M USD)	Data Recovery (%)	Business Interruption (%)	Other (%)
2021	9.23	45%	25%	30%
2022	10.87	40%	32%	28%
2023	12.54	35%	38%	27%
2024	14.92	30%	45%	25%
2025	**16.31**	28%	**48%**	24%

+77%

cumulative cost increase
$9.23M → $16.31M

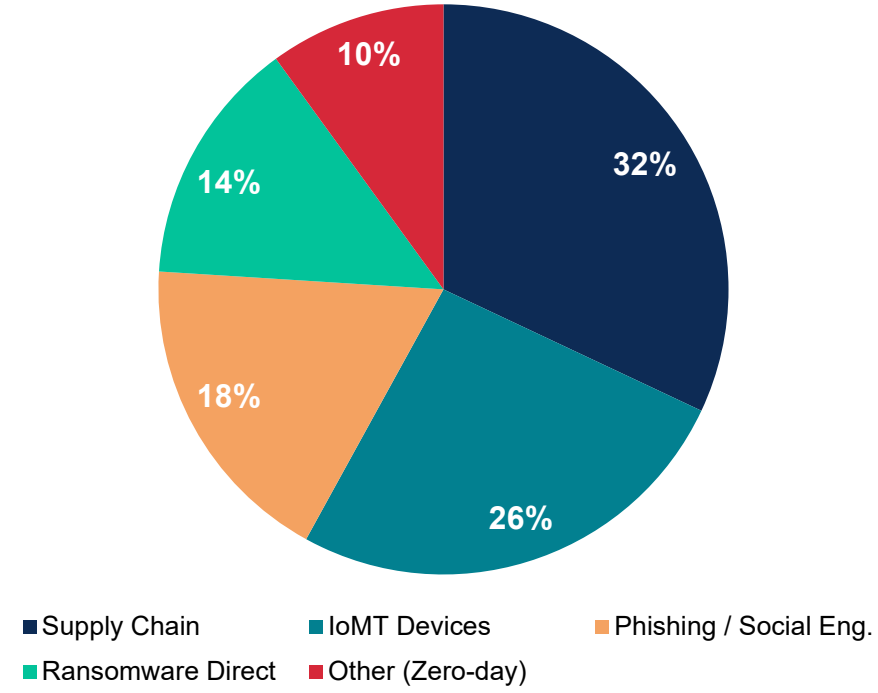
25% → 48%

business interruption
share (2021 → 2025)

Key insight: The dominant cost has shifted from data recovery to business interruption — reflecting a deliberate attacker strategy to maximise economic and social damage.

The 22nd Economic International Conference
Challenges and Opportunities for a Sustainable Development
Stefan cel Mare University of Suceava, 2026

Attack Vectors Distribution (2023–2025)



32% — **Supply Chain Attack**

Exponentially increasing. One compromised vendor → dozens of hospitals.

26% — **IoMT Exploitation**

Smart medical devices (infusion pumps, cardiac monitors) as entry points.

58% — **Combined Dominance**

Supply chain + IoMT = 58% of all attack vectors. Traditional defences insufficient.

The 22nd Economic International Conference
Challenges and Opportunities for a Sustainable Development
Stefan cel Mare University of Suceava, 2026

Post-Attack Clinical Impact Indicators

A cyberattack is not an IT crisis — it is a medical emergency with direct and measurable consequences for patient safety.

Indicator	Baseline	During Attack	Recovery	Change
Triage Accuracy	95%	**70–80%**	7–10 days	-20%
Waiting Time (min)	45 min	**120–180 min**	14–21 days	×3–4
Medical Error Rate	0.8%	**2–3%**	28 days ⚠	**×3**
Cancelled Surgeries	2%	**40–60%**	21–28 days	**×25–30**

Longest recovery: Medical error rate (28 days). Cause: physicians work on incomplete information under extreme time pressure. Technical restoration alone is insufficient — organisational recovery adds further delay.

The 22nd Economic International Conference
Challenges and Opportunities for a Sustainable Development
Stefan cel Mare University of Suceava, 2026

Artificial Intelligence: Offensive vs. Defensive

⚔ AI OFFENSIVE

Exploitation window

< 15 min after vulnerability disclosure

Methods

Automated scanning, zero-day exploitation

Attack success rate

65 – 75%

Detection phase

Post-breach (too late)

VS

🛡 AI DEFENSIVE (UEBA)

Monitoring

Real-time continuous behavioural analytics

Methods

User & Entity Behavior Analytics (UEBA)

Attack success rate

20 – 30%

Detection phase

Early stages (reconnaissance / lateral movement)

The 22nd Economic International Conference
Challenges and Opportunities for a Sustainable Development
Stefan cel Mare University of Suceava, 2026

Public Sector vs. Private Sector

Criterion	Public Sector	Private Sector
Primary Vulnerability	Legacy systems & rigid budgets	Excessive interconnectivity
Attack Motivation	Social destabilisation	Corporate espionage & data extraction
Response Capacity	National agencies (DNSC/CERT-RO)	Fast internal security teams
Recovery Time	72 – 96 hours	24 – 48 hours
Cybersecurity Investment	2 – 3% of IT budget	5 – 8% of IT budget

Both sectors converge on the same necessity: Zero Trust architecture — no connection is implicitly secure, regardless of internal or external origin.

The 22nd Economic International Conference
Challenges and Opportunities for a Sustainable Development
Stefan cel Mare University of Suceava, 2026

Evaluation of Research Hypotheses

H1	**VALIDATED**	Costs grew from $9.23M to $16.31M (+77%). Operational downtime rose from 25% to 48%. Digitalisation without security creates fragile institutions.
H2	**PARTIAL**	Reputational impact exceeds GDPR fines (>40% vs. ~12%). However, triple extortion remains a minority tactic (<10% of incidents) — not yet systemic.
H3	**INVALIDATED**	Supply chain (32%) and IoMT (26%) dominate. Legacy systems account for only 14%. Modern interconnectivity is the real vulnerability, not outdated infrastructure.
H4	**VALIDATED**	Phishing declined from ~26% to 18%. UEBA with trained users reduces success rates from 65–75% to 20–30%. Training works — but must be combined with technology.

Conclusions & Strategic Recommendations

"Cyber safety is patient safety. Investment in cybersecurity is not an administrative expense — it is an investment in human lives."

01 Zero Trust Architecture

No connection is implicitly secure — mandatory for both public and private institutions.

02 Proportional Investment

Minimum 5–8% of IT budget for cybersecurity. Public sector must close the gap (currently 2–3%).

03 Continuous Training

Staff education measurably reduces social engineering exposure. Training must be sustained, not one-off.

04 IT–Biomedical Coordination

IoMT devices must be secured collaboratively by IT and biomedical engineering departments.

05 Annual Strategic Reassessment

Threats evolve faster than traditional frameworks. Security strategies must be reviewed and updated annually.