cabreza

BUSINESS CASE & ROI • January 2026

The Business Case for OT Resilience

Quantifying the ROI of resilience investments for leadership

EXECUTIVE SUMMARY

> Manufacturing downtime costs $50,000-$125,000 per hour. Average OT incident costs $2.8 million. This whitepaper quantifies the business case for resilience investments, examines what produces measurable ROI, and provides frameworks for making the case to leadership.

The Cost of Disruption

When cyber incidents hit operational technology, the costs are immediate, tangible, and frequently massive.

Manufacturing downtime costs:

METRIC	COST
Median downtime cost	$125,000/hour (ABB)
Average downtime cost	$50,000/hour (Siemens)
Large manufacturer daily cost	$1.1 million
Automotive assembly line	$22,000/minute

These figures represent production loss only—not investigation, remediation, regulatory penalties, customer impact, or reputational damage.

Recovery takes time:

METRIC	PERCENTAGE
Recovery takes >1 week	49%
Recovery takes >1 month	29%
Downtime >12 hours	49%
Full day+ of downtime	33%

At $50,000-$125,000 per hour, a one-week outage produces $8.4-21 million in production loss alone. Half of organizations experience recovery processes lasting that long.

Incident costs are significant:

METRIC	AMOUNT
Average OT cyber incident	$2.8 million (IBM 2024)
Manufacturing incident range	$200K - $2 million
Average cyber claim payment	$812,360
Global OT cyber risk (annual avg)	$31 billion (Dragos/Marsh)

Colonial Pipeline: What a Major Incident Actually Costs

The May 2021 Colonial Pipeline attack provides detailed cost visibility.

The attack: Compromised VPN password (inactive account, no MFA) → IT ransomware → OT shutdown (precautionary)

Direct costs:

- Ransom paid: $4.4 million (75 Bitcoin)
- Ransom recovered: $2.3 million (by DOJ)
- Duration: 6 days

Cascading impact:

- Fuel supply affected: 45% of East Coast
- Emergency declarations: 17 states + DC
- Charlotte stations out of fuel: 71%
- Washington DC stations out of fuel: 87%
- Gas prices: >$3/gallon (highest since 2014)

The ransom—while headline-grabbing—was the smallest cost. Six days of shutdown for the largest refined products pipeline in the US cascaded into regional infrastructure crisis. The economic impact measured in billions.

A single compromised credential without MFA caused this. Prevention would have been cheap. Recovery was not.

Insurance Market Pressure

The cyber insurance market is forcing security investment whether organizations want it or not.

Coverage is harder to obtain:

CHALLENGE	STATISTIC
First applications denied	41%
Premium increase without OT security	37%
Claims involving orgs lacking MFA	82%
Vendors losing contracts due to coverage gaps	67%

The 41% denial rate indicates insurers require controls many organizations lack. Common denial reasons: missing MFA, inadequate endpoint protection, no incident response plan, insufficient segmentation.

Insurers require specific controls:

1. Multi-factor authentication (MFA)
2. Endpoint Detection & Response (EDR)
3. Encrypted/offline backups
4. Incident Response Plan
5. Network segmentation

These requirements align with resilience capabilities. Organizations that can't demonstrate them face coverage denial, premium increases, or contract barriers.

The ROI Evidence: What Actually Produces Returns

Tested backups: 85% reduction in downtime

The math: If average downtime without tested backups is 5 days, and with tested backups is 0.75 days, at $500,000/day that's $2.125 million savings per incident. The cost of implementing and testing backups is far less.

Regulated sites: 50% fewer financial losses

The SANS 2025 finding deserves emphasis: regulated sites experienced 50% fewer financial losses and safety impacts. They didn't have fewer incidents—they had better capabilities to contain and recover.

The mechanism: regulations force organizations to operationalize discipline. Required IR plans get practiced. Required controls get implemented.

Training: $260,000 reduction in breach costs

Strategic employee training correlates with measurable cost reduction. The 1.7x readiness improvement from tabletop exercises represents similar return.

Detection speed: ~100 days faster identification/containment

Organizations with mature detection capabilities identify and contain breaches faster. Each day faster means reduced data loss, reduced operational impact, reduced total cost.

Making the Case to Leadership

Frame as risk management, not IT spending:

Not: "We need $500K for security tools."

Instead: "We face $2.8M expected loss from OT incidents. This $500K investment reduces exposure by 60%, with expected ROI in first prevented or shortened incident."

Quantify current exposure:

- Annual probability of incident: 10-30% (based on industry data)
- Average incident cost: $2.8 million
- Expected annual loss: $280K-$840K
- 45% of organizations experienced >$500K impact in 12 months
- 27% exceeded $1 million

Connect to outcomes leadership cares about:

LEADER	METRICS THAT RESONATE
CFO	Risk exposure, insurance costs, expected loss
COO	Downtime probability, recovery time, production availability
CEO	Competitive position, regulatory exposure
Board	Fiduciary responsibility, enterprise risk

Document the cost of inaction:

- Insurance: 41% application denial, 37% premium increase
- Regulatory: NIS2 penalties up to €10M/2% turnover
- Non-compliance breach premium: 12.6% higher costs
- Contract barriers: 67% of vendors lost opportunities due to coverage gaps

Highest-ROI Investments

Based on evidence, prioritize:

1. **Tested OT backups** — 85% downtime reduction. Exceptional ROI, relatively low investment.
2. **Multi-factor authentication** — Prevents credential-based attacks. 82% of claims involved organizations without MFA. Colonial Pipeline's root cause.
3. **Incident response planning and exercises** — 50% lower incident costs for organizations with practiced capabilities. 1.7x readiness from tabletops.
4. **Network segmentation** — Contains attack spread. Reduces blast radius. Required by most regulations and insurers.
5. **Employee training** — $260K reduction in breach costs. Affects prevention, detection, and response.

The resilience portfolio:

CAPABILITY	FUNCTION
Prevention	Reduce probability of successful attack
Detection	Identify attacks when they occur
Response	Contain damage and limit spread
Recovery	Restore operations rapidly

Most organizations overweight prevention and detection while underweighting response and recovery. The evidence suggests rebalancing toward recovery produces superior risk-adjusted returns.

The Path Forward

The business case is quantifiable:

- $125K/hour downtime
- $2.8M average incident cost
- 85% downtime reduction from tested backups
- 50% lower losses with response capability

The question isn't whether to invest—the costs of inaction are clear. The question is where to invest for best returns.

The evidence points to resilience: response capability, tested backups, practiced procedures. These investments produce value even when they don't prevent a single incident. They limit damage when incidents occur.

Detection finds the fire. Resilience determines how much burns.

Sources

- IBM Security, Cost of a Data Breach Report 2024: https://www.ibm.com/reports/data-breach
- Dragos/Marsh McLennan, Global OT Cyber Risk Quantification: https://www.dragos.com/resource/quantifying-the-global-risk-to-operational-technology-in-cyber-insurance/
- Claroty, Global State of CPS Security 2024: https://claroty.com/resources/reports/the-global-state-of-cps-security-2024-business-impact-of-disruptions
- SANS Institute, State of ICS/OT Security 2025: https://www.sans.org/white-papers/state-of-ics-ot-security-2025
- Siemens, True Cost of Downtime: https://www.siemens.com/global/en/products/automation/topic-areas/true-cost-of-downtime.html
- CISA, Colonial Pipeline Analysis: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years