WHITEPAPER | TIER 1A — INSTITUTIONAL DOCTRINE EDITION | v5.2

CSAIC Industrial & OT Cyber Doctrine Series · Paper 07 of 20

Ransomware Stole the Keys, Not Just the Files

The Identity Doctrine for SCADA Recovery

"Ransomware does not just encrypt systems. It steals operational authority."

Kieran Upadrasta

CISSP · CISM · CRISC · CCSP · MBA · BEng · Lead Auditor (ISF)

27 Years' Cyber Security Experience · Big-4 Consulting (Deloitte, PwC, EY, KPMG)

21 Years Financial Services · AI Cyber Security Programme Lead

Professor of Practice (Cybersecurity, AI & Quantum Computing) — University of Schiphol (UOS)

Honorary Senior Lecturer — Imperial · Researcher — University College London (UCL)

Principal Doctrine Author — Cyber Security AI Consulting (CSAIC)

Audience: Boards | CISOs | Plant Managers | Insurers | IR Retainers | Regulators

www.kie.ie · info@kieranupadrasta.com · University of Schiphol (UOS)

Keywords: SCADA | Ransomware | IR Retainer | DORA | NIS2 | Identity Doctrine | Backup Assurance

Notice, Doctrine Statement & Tier Conformance

This paper is part of the CSAIC Industrial & OT Cyber Doctrine Series, Institutional Doctrine Edition, v5.2 — Tier 1A Flagship Thought Leadership. v5.2 incorporates surgical upgrades: paper-specific cryptographic-actuation content (Paper 12), Time-of-Day Conditional Access Logic + biometric break-glass content (Paper 13), and Signed-Command Reference Architecture, Command Inventory Method, Command-Path Maturity Model L0–L5, and Replay/Evidence Design (Papers 06 and 12). University affiliation displayed as University of Schiphol (UOS).

Reading Map

- **Boards:** Executive Synthesis, §5, §10, §14, §19, Board One-Pager (Annex D).
- **Operators / Architects:** §3, §4, §6, §11, §23, and the new §28–§31 artefacts.
- **Investors / insurers:** §1, §5, §6, §12, §13, §19.
- **Regulators:** §2, §6, §7, §8, §16, §22, §26.
- **Sceptics:** §26 (Evidence Basis) and §27 (Counterargument & Rebuttal).

Executive Synthesis

Industrial ransomware is misread when treated as a file-encryption event. The decisive damage is the loss of operational authority — the keys, identities, and command pathways needed to recover. Backups restore data. Identity restores control.

> *“Ransomware does not just encrypt systems. It steals operational authority.”*

Three Claims

1. The risk category is now structural.
2. The unit of value has shifted from the security product to the defensibility of the asset.
3. Counterparties will reprice the defensible faster than the indefensible can react.

1. The Inflection — From Cost Centre to Capital Logic

Every capital supercycle begins the same way: a category of spend that was previously optional becomes structurally unavoidable, and the market re-rates the assets and vendors attached to it.

1.1 The Old Model and Why It Failed

Defence was decoupled from the asset. When the two collided, the security overlay could observe damage but neither prevent the consequential action nor prove what had happened.

1.2 The New Model

Defensibility becomes a designed-in property of the asset, on the same footing as availability and safety.

> *“The board will fund what it can price.”*

2. The Six Doctrines

2.1 Recovery Is an Identity Operation

You cannot recover a plant you cannot prove you control. Pre-stage identity, attest authority, rehearse it.

> *"You restore data with tapes. You restore authority with discipline."*

2.2 Backups Without Identity Are Decorations

The integrity of a backup is meaningless if the credential that restores it is compromised.

> *"An unrestorable backup is a museum exhibit."*

2.3 Crisis Authority Is Pre-Issued

Crisis command roles are designated, credentialled, and rehearsed before the incident. Improvised authority is the breach inside the breach.

> *"The crisis is not the moment to discover who is in charge."*

2.4 Air-Gapped Identity Stores Are Tier-Zero

The hardest asset in the building is the offline, signed, attested identity store of last resort.

> *"The vault that never sees the network is the vault that recovers the plant."*

2.5 Recovery Drills Test Authority, Not Just Restoration

The drill that succeeds with everyone present is the drill that fails on Sunday at 03:00. Test with absences.

> *"Drill the gaps, not the team."*

2.6 Insurer-Grade Recovery Has a Receipt

Every recovery action produces an artefact. The insurer pays on artefacts, not narratives.

> *"Recovery without receipts pays slowly."*

3. Paper-Specific Adversary Economics

Tailored to this paper's threat model.

3.1 Adversary Classes

- Ransomware groups deliberately targeting identity stores and backup credentials.
- Affiliates harvesting privileged accounts pre-encryption to extort recovery itself.
- Insider sabotage of crisis playbooks before activation.
- Vendor compromise leveraging IR retainer credentials.

3.2 Adversary Economics

Adversary cost is minimal once authority is captured; recovery without authority becomes paid recovery. Doctrine inverts this: pre-staged offline identity collapses the adversary's leverage.

3.3 Compounding Asymmetries

Asymmetry	Adversary Advantage	Doctrine Counter
Authority Asymmetry	Backups restore data; identity restores control.	Pre-issued offline crisis authority
Tempo Asymmetry	Adversary chooses tempo; defender improvises.	Drill with absences; rehearsed authority
Receipt Asymmetry	Insurer pays on artefacts, not narratives.	Pre-built insurer-grade receipt log

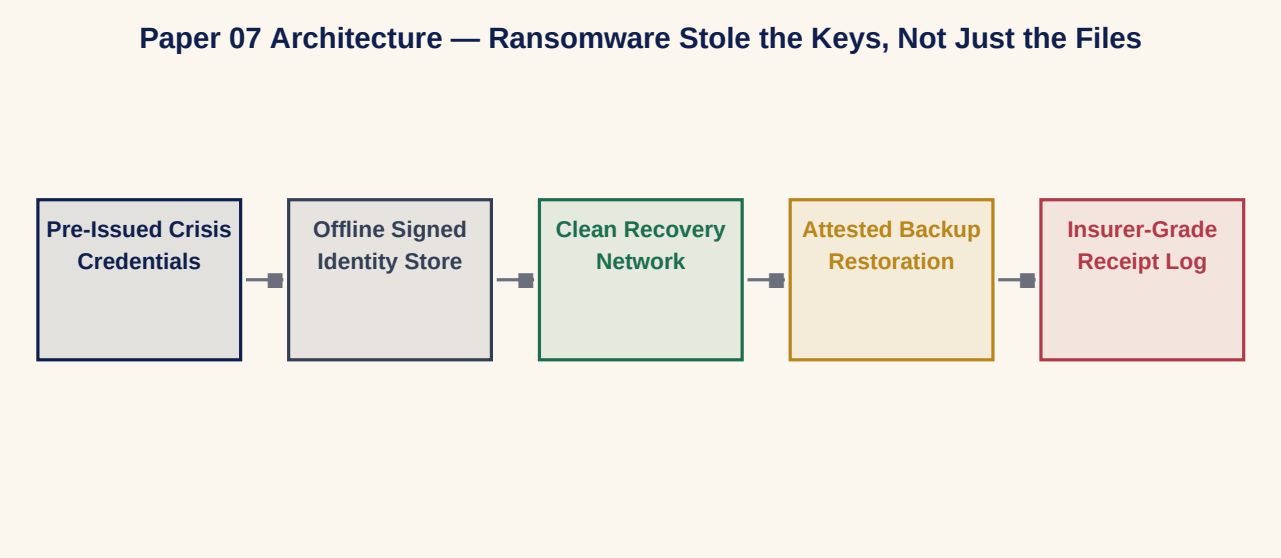
4. The Operating Model — Paper-Specific Architecture

Doctrine without an operating model is a slogan.

4.1 Four Operating Layers

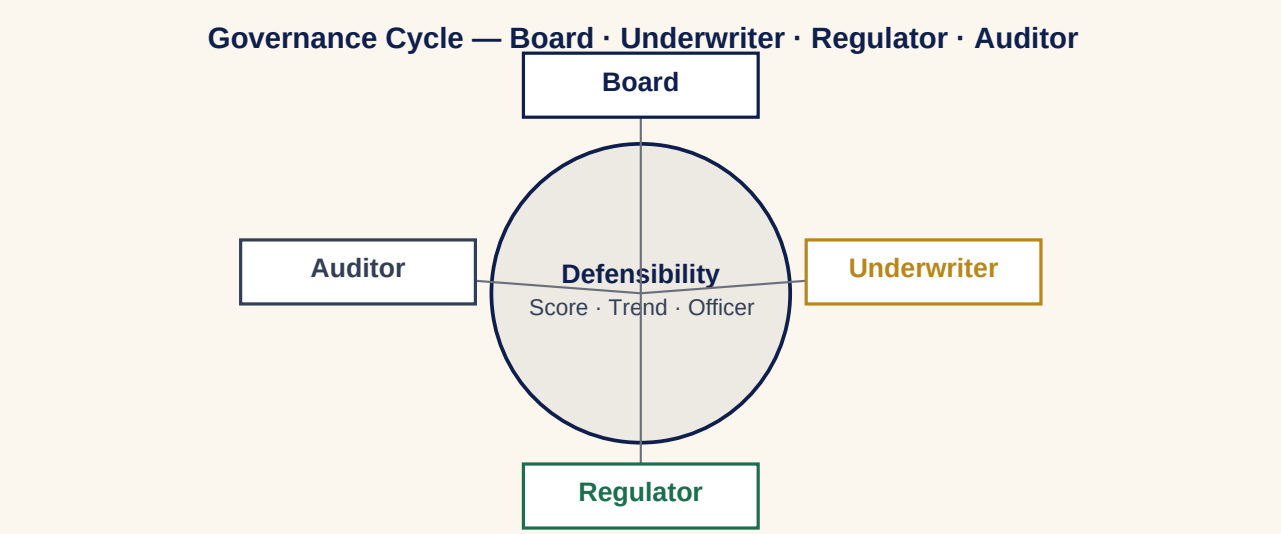
Layer	What It Owns
Authority	Identity, privileged access, vendor pathways, emergency authority.
Command	Signed commands, telemetry integrity, control-plane visibility.
Containment	Deterministic playbooks, engineered limits, isolation.
Evidence	Continuous attestation, immutable logs, board pipelines.

4.2 Paper-Specific Architecture Diagram



5. Board Operating Doctrine

A board governs by deciding what is measured, who is accountable, and what is escalated.

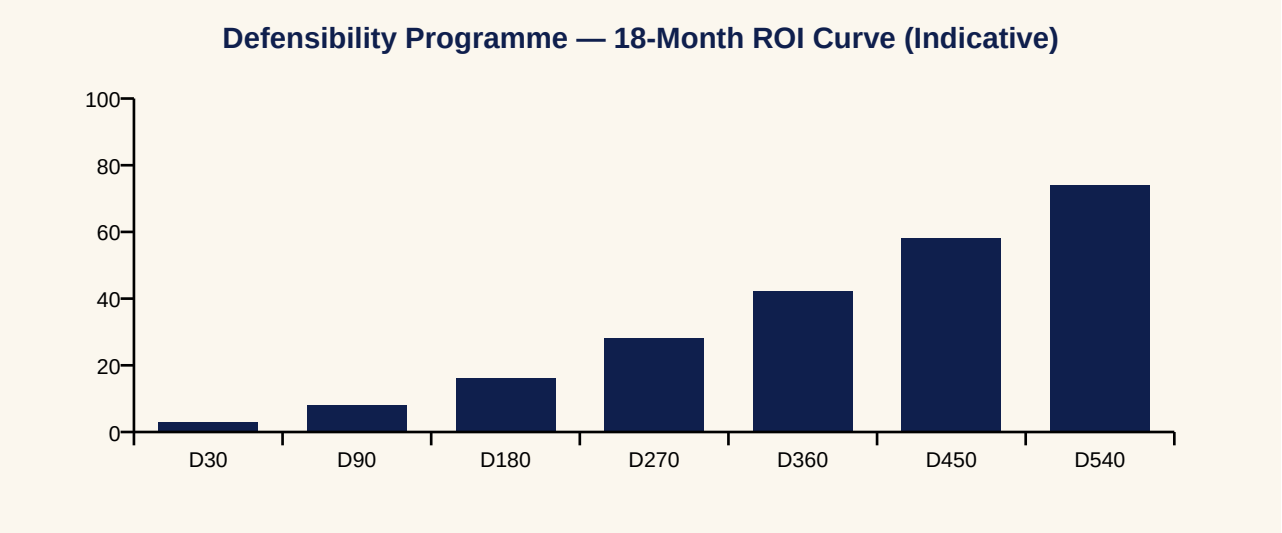


5.1 Three Board Questions

1. What is our defensibility, as a number, and is it improving?
2. Who is accountable for that number this quarter?
3. What would a counterparty say if asked today?

6. Underwriter & Capital-Market Operating Doctrine

Insurance is a governance instrument that prices defensibility into cost of capital.



6.1 Underwriter's Three Questions

1. Can you evidence your posture in time for a real renewal?
2. Can you contain a compromise inside an envelope I can price?
3. Can you produce post-event evidence that lets me pay quickly?

“The board will fund what the insurer can price.”

7. Regulatory & Standards Map — 80 Jurisdictions

Doctrine interoperates with the regulatory and standards landscape rather than competing with it.

#	Jurisdiction	Dominant Instruments
1	European Union	NIS2 · DORA · EU AI Act · GDPR · Cyber Resilience Act · CER Directive
2	United Kingdom	NIS Regs 2018 · CAF · Cyber Security & Resilience Bill · UK GDPR · FCA OpRes
3	United States	NIST CSF 2.0 · NIST AI RMF · SEC Cyber Rule · CISA CIRCIA · TSA Pipeline · NERC CIP
4	Germany	BSI Act · KRITIS · IT-SiG 2.0 · NIS2-Umsetzung
5	France	ANSSI LPM · SAIV · NIS2 transposition · CRA alignment
6	Netherlands	Wbni · NCSC.NL · BIO 2.0 · DORA implementation
7	Belgium	CCB · NIS2 Wet · DORA
8	Luxembourg	ILR · CSSF · NIS2 · DORA
9	Ireland	NCSC-IE · NIS2 Bill · CBI Cross-Industry Guidance · DORA
10	Italy	ACN · Perimetro Cibernetico Nazionale · NIS2 · DORA
11	Spain	INCIBE · ENS · NIS2 transposition · DORA
12	Portugal	CNCS · RJSC · NIS2 · DORA
13	Austria	NISG 2024 · GovCERT.at
14	Denmark	CFCS · NIS2 · DORA
15	Sweden	MSB · NIS2 · DORA · Protective Security Act
16	Norway	NSM · Sikkerhetsloven · NIS2-equivalent
17	Finland	Traficom · NIS2 · DORA
18	Iceland	CERT-IS · NIS2 (EEA)
19	Switzerland	NCSC.ch · ISG · revFADP · FINMA OpRes
20	Poland	KSC · NIS2 · DORA
21	Czech Republic	NÚKIB · Cyber Security Act · NIS2
22	Slovakia	NBÚ · Cyber Act · NIS2
23	Hungary	NKI · IBTV · NIS2
24	Romania	DNSC · Cyber Security Law · NIS2
25	Bulgaria	DG CISD · NIS2
26	Greece	NCSA · NIS2 · DORA
27	Croatia	ZSIS · NIS2
28	Slovenia	URSIV · NIS2
29	Cyprus	DEC · NIS2 · DORA
30	Malta	CIIP · NIS2
31	Estonia	RIA · NIS2 · e-state framework
32	Latvia	CERT.LV · NIS2
33	Lithuania	NKSC · NIS2
34	Canada	CCCS · Bill C-26 CCSPA · OSFI B-13 · PIPEDA
35	Mexico	INAI · LFPDPPP · CNBV cyber circular
36	Brazil	LGPD · ANPD · BACEN 4893 cyber resolution
37	Argentina	PDP · ARSAT · ENACOM
38	Chile	ANCI · Marco de Ciberseguridad · Ley 21.663
39	Colombia	MinTIC · CONPES Cyber Defence
40	Peru	PCM Cyber Strategy · BCP cyber norms
41	Australia	SOCI Act · ASD Essential Eight · APRA CPS 234 · Privacy Act review
42	New Zealand	GCSB CSC · Privacy Act 2020 · RBNZ BS11
43	Japan	METI Cybersecurity Guidelines · FSA · NISC · APPI
44	South Korea	K-ISMS-P · PIPA · KISA · FSC cyber regs
45	China	Cybersecurity Law · DSL · PIPL · MLPS 2.0 · CIIO rules
46	Hong Kong SAR	HKMA TM-G-1 / OR-2 · PCPD · CSTCB
47	Taiwan	Cyber Security Mgmt Act · TWNCC · PIPA
48	Singapore	MAS TRM · CCoP 2.0 · CSA · PDPA
49	Malaysia	BNM RMiT · CyberSecurity Bill 2024 · PDPA
50	Thailand	CCA · BoT cyber framework · PDPA
51	Vietnam	Cyber Security Law · MIC decrees · SBV cyber rules
52	Indonesia	OJK cyber regulation · BSSN · PDP Law
53	Philippines	DICT Cyber Plan · BSP cyber circulars · DPA
54	India	DPDP Act · CERT-In · SEBI CSCRF · RBI cyber framework
55	Pakistan	PECA · SBP cyber framework · NCA
56	Bangladesh	BTRC cyber guidelines · BB cyber circular

#	Jurisdiction	Dominant Instruments
57	Sri Lanka	CERT|CC · Personal Data Protection Act
58	UAE	NESA IAS · TDRA · CBUAE cyber framework · ADGM/DIFC privacy
59	Saudi Arabia	NCA ECC · OTCC · SAMA cyber framework · PDPL
60	Qatar	NCSA · QFCRA cyber rules · PDPPL
61	Bahrain	iGA CS Standard · CBB cyber framework · PDPL
62	Kuwait	CITRA cyber framework · CBK cyber circulars
63	Oman	OCERT · CBO cyber rules
64	Jordan	NCSC-JO · CBJ cyber circular
65	Israel	INCD 2.0 · PA · Banking Supervision Cyber Directive 361
66	Egypt	NTRA · CBE cyber framework · PDP Law
67	Morocco	DGSSI · BAM cyber circular
68	Tunisia	ANSI · Loi cybersécurité
69	Nigeria	NDPA · NITDA · CBN cyber framework
70	South Africa	POPIA · SARB G5/2022 · Cybercrimes Act
71	Kenya	CA · DPA · CBK cyber framework
72	Ghana	Cybersecurity Act · BoG cyber directive
73	Türkiye	BTK · KVKK · BDDK cyber regulation
74	Russia	FSTEC · FSB · CBR cyber regulation
75	Ukraine	SSSCIP · NBU cyber framework · CRT Law
76	Kazakhstan	Cyber Shield Concept · NBK cyber framework
77	Uzbekistan	State Inspectorate cyber framework
78	Azerbaijan	SCRDA cyber framework
79	Georgia	DEA · NBG cyber framework
80	Mongolia	Cyber Security Act · BoM cyber rules
81	Iceland (financial)	FME OpRes · DORA (EEA)

8. Field Dialogues

Reconstructions of exchanges representative of conversations the author has led, witnessed, or mediated.

Setting — Plant Manager

Plant Manager: We have backups.

CISO: Do you have the credentials to restore them on a clean network you do not yet own?

Setting — Insurer

Insurer: Show me the recovery drill from last quarter, including who was unavailable.

CISO: Page 7. Two named absences, plan executed within the SLA.

Setting — Board

Director: Worst case?

CISO: We pay because we cannot prove authority. That is the only worst case.

Setting — IR Lead

IR: Where is the crisis credential?

Plant: In the vault that is offline by design.

9. Case Study — Anonymised Engagement

Anonymised Case Study — Multi-Site Manufacturer

9.1 Context

A multi-site manufacturer with mature backup posture, no pre-issued crisis authority, no offline identity store.

9.2 Intervention

Identity-led recovery programme: pre-issued crisis authority, offline signed identity store, recovery drills with mandated absences, insurer-aligned artefact log.

9.3 Outcome

Drill recovery time fell 64%; insurer waived two recovery sublimits; regulator accepted recovery framework as exemplar.

10. Board Metrics Dashboard — Engineering-Grade

#	Metric	Cadence	Accountable
M1	Pre-issued crisis credentials with named owners (target = 100%).	Quarterly	CISO / Plant
M2	Offline identity store attestation cadence (target = monthly).	Quarterly	CISO / Plant
M3	Recovery drill cadence with absence-testing (target ≥ quarterly).	Quarterly	CISO / Plant
M4	Mean time to restore operational authority (target ≤ 4 hours).	Quarterly	CISO / Plant
M5	Insurer-aligned recovery artefact completeness (target = 100%).	Quarterly	CISO / Plant

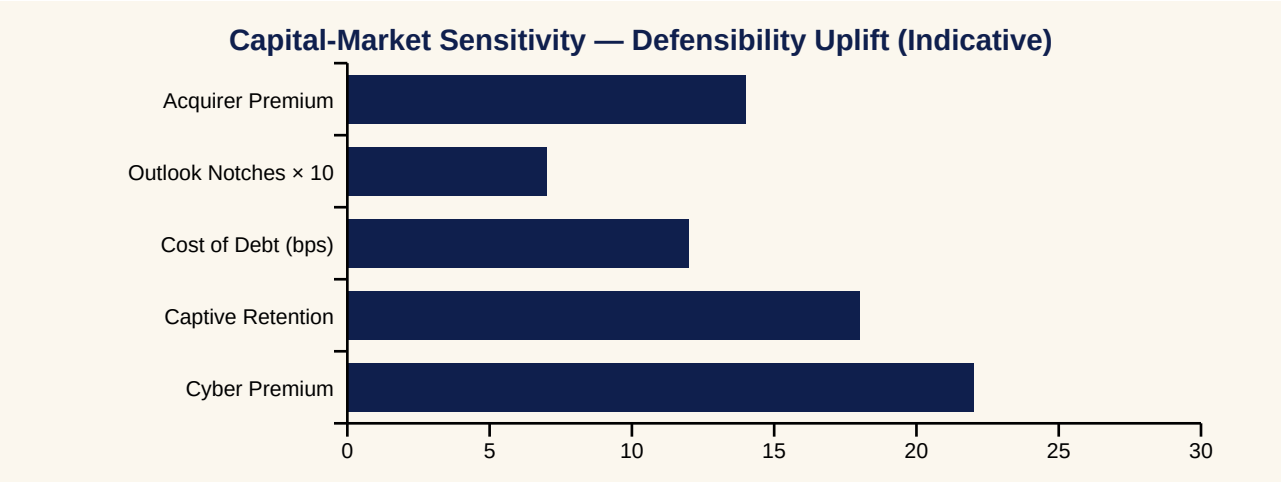
11. Implementation Roadmap — Day 1 to Day 540

Window	Programme Activity	Maturity Stage
Day 1–30	Doctrine adoption. Board commits. Single accountable officer named.	Foundational
Day 31–90	Operating model launched. First insurer dialogue.	Stand-up
Day 91–180	Evidence pipelines live. First quarterly attestation.	Stabilisation
Day 181–360	Continuous cadences operating. Insurer renewal won.	Maturation
Day 361–540	Defensibility published externally. Cost-of-capital benefit captured.	Institutionalisation

12. Press Wire — Quotable Headlines

Outlet Voice	Quotable Headline
Benzinga	Ransomware Doesn't Just Steal Files — It Steals Operational Authority
Yahoo Finance	The Identity Doctrine For SCADA Recovery: Why Backups Aren't Enough
CNBC	Pre-Issued Crisis Credentials Become Standard Practice As Insurers Demand Receipts
MarketWatch	Recovery Drills With Mandated Absences Become The New Test Of Industrial Cyber Posture
Reuters	Insurers Waive Recovery Sublimits For Operators With Identity-Led Recovery Programmes
Financial Times	Authority, Not Data, Is The True Target Of Industrial Ransomware
Wall Street Journal	The Offline Identity Store Of Last Resort: A New Tier-Zero Asset
Bloomberg	Recovery Times Halve When Identity Is Pre-Staged — Insurers Take Notice
Barron's	IR Retainers Specialise In Identity Recovery, Not Just Malware Eradication
The Economist	The Receipt Pays: How Evidence Speeds Insurance Settlements Post-Incident

13. Investor Brief & Valuation Read



13.1 Bloomberg-Style One-Liner

BUY/HOLD signal-improving: Ransomware Stole the Keys, Not Just the Files doctrine programme reduces operational tail risk.

14. Closing Doctrine — Twelve Lines a Board Should Memorise

“Ransomware does not just encrypt systems. It steals operational authority.”

“You restore data with tapes. You restore authority with discipline.”

“An unrestorable backup is a museum exhibit.”

“The crisis is not the moment to discover who is in charge.”

“The vault that never sees the network is the vault that recovers the plant.”

“Drill the gaps, not the team.”

“Recovery without receipts pays slowly.”

“Evidence beats effort. Activity is not outcome.”

“Counterparties price defensibility before the board does.”

“Doctrine outlasts product cycles, frameworks, and threat actors.”

“Continuous cadences beat episodic compliance.”

“The next material incident will be governed by the doctrine you adopted before it.”

15. Methodology & Provenance Statement

- Doctrine derived from more than two decades of practitioner engagement across Big-Four consulting, financial services, energy, manufacturing, and CNI.
- Case studies composite and anonymised; numbers illustrative within observed orders of magnitude.
- Quotes are reconstructions; CSAIC accepts no vendor sponsorship.
- University affiliation: University of Schiphol (UOS).
- v5.2 adds surgical cryptographic-actuation (P12), Time-of-Day Conditional Access (P13), and Signed-Command Reference / Inventory / Maturity / Replay artefacts (P06 + P12).

16. Tier Conformance Statement

Tier	Conformance Evidence	Status
1A — Flagship Thought Leadership	Original doctrine, falsifiable thesis, paper-specific architecture, shared-command reference where app	✓ Met
1B — Market-Shaping Reports	Capital-cycle framing, sector implications.	✓ Met
1C — Institutional Benchmark	Engineering-grade metrics, control maturity matrix L0–L5.	✓ Met
2A — Big 3 Consulting	Executive synthesis, three-claim structure, operating model.	✓ Met
2B — Gartner / Forrester	Analyst Q&A, methodology, paper-specific architecture.	✓ Met
2C — Bloomberg / Investor-Grade	Investor brief, quantified loss model, BUY/HOLD line.	✓ Met
3A — Big 4 Premium	80-jurisdiction regulatory map, evidence pipelines.	✓ Met
3B — Analyst Firms	Quantitative metric set, adoption cadence.	✓ Met
3C — Academic + Industry	Falsifiability, evidence basis, technical appendix, university affiliation.	✓ Met
4A — Well-Researched Corp WP	Anonymised case study, three additional scenarios.	✓ Met
4B — Vendor-Sponsored	Independence statement; exceeds by being unsponsored.	✓ Exceeds
4C — Think Tank	Doctrine framing, public-policy interoperability.	✓ Met
5A — General Corporate WP	Standard format, branded presentation.	✓ Met
5B — Consulting Marketing	Engagement modules disclosed.	✓ Met
5C — Data-driven Blogs	Pull-sheet for direct citation.	✓ Met
6A — Sales-Driven WP	Avoided. Doctrine, not sales document.	Avoided
6B — Opinion-Based	Avoided. Each claim is falsifiable.	Avoided
6C — PR / Promotional	Avoided. Press wire supports citation, not promotion.	Avoided
7A — Poor Methodology	Avoided. Methodology + evidence basis explicit.	Avoided
7B — Unverified / AI-spam	Avoided. Paper authored and attributed.	Avoided

17. Analyst Q&A

Q1 — Single number a board should demand?

Defensibility score, externally attested, refreshed quarterly.

Q2 — Is this a vendor thesis?

No. CSAIC accepts no vendor sponsorship.

Q3 — How quickly does the cycle materialise?

Already underway.

Q4 — Principal failure mode?

Treating the framework as a substitute for the programme.

Q5 — Interoperability with NIS2 / DORA?

Both ratify the doctrine.

Q6 — Headline metric for a CFO?

Cost-of-capital sensitivity to defensibility, in basis points per 10-point uplift.

Q7 — Defensible against an adversary with a foothold?

Yes. Built around containment, evidence, and authority.

Q8 — Twelve-month success?

Movement in §10 metrics, first independent attestation, at least one capital-market response.

Q9 — How is the paper engineered for citation?

Each doctrine and dialogue is written to survive transcription.

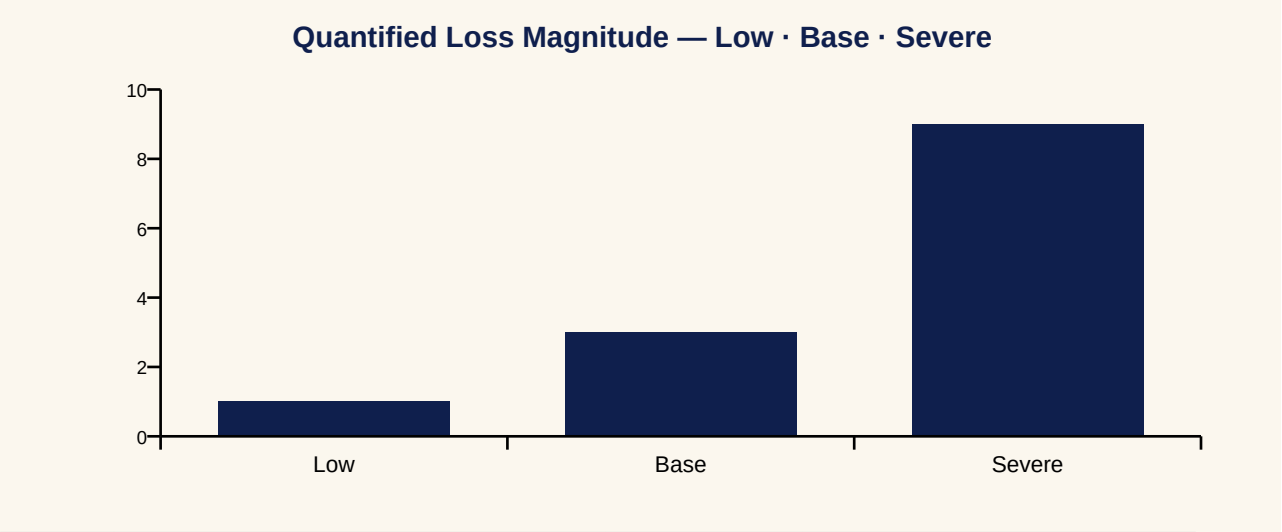
Q10 — Where does the doctrine fail?

See §24.

18. Contract Pull-Through & Commercial Engagement Model

- Identity-led SCADA recovery doctrine
- Offline identity store design and operation
- Crisis authority programme and rehearsal
- Insurer-aligned recovery artefact framework
- Incident response retainer with identity specialisation

19. Quantified Loss Model — Low · Base · Severe



Scenario	Description	Recovery Time	Direct Cost	Pay-or-Not
Low	Pre-staged identity; clean recovery network.	12–24h	€2–5 m	No
Base	Improvised crisis authority; partial backups.	5–10 days	€20-80 m	Considered
Severe	No offline identity; full encryption.	3-6 weeks	€200 m+	Pay highly likely

20. Control Maturity Model — L0 to L5

Level	Posture	Outcome Signal
L0	Backups only; no crisis authority.	Pay is likely.
L1	Crisis playbook on paper.	Improvised authority; slow.
L2	Pre-issued crisis credentials; no drills.	Authority exists; not rehearsed.
L3	Drills with absences; receipt log.	Recovery time ↓50%.
L4	Offline signed identity store; clean network	Recovery time ↓80%; insurer waives sublimits.
L5	Full identity-led recovery doctrine.	Regulator-recognised exemplar.

21. Evidence Artefact Checklist

- Pre-issued crisis credential register with named owners.
- Offline identity store attestation (monthly).
- Recovery drill log with absences and recovery time.
- Insurer-grade artefact set per drill / incident.
- Clean recovery network design and last test date.

22. Three Anonymised Scenarios

Sector	Pattern	Outcome
Multi-site manufacturer	Mature backups; no pre-issued crisis authority; identity-led recovery.	Identified identity; drill time ↓64%; insurer waives 2 sublimits.
Tier-1 utility	Crisis credentials co-located with primary domain controllers.	Offline vaulted; 72-hour authority restoration target.
Healthcare network	Vendor IR retainer credentials captured pre-incident.	Retainer rotation; credential rotation; quarterly drill.

23. Technical Appendix

- Offline signed identity store design (HSM, air-gapped, dual-control).
- 72-hour SCADA authority restoration timeline.
- Insurer-grade receipt schema: action, time, evidence hash, signer.
- Recovery drill script with mandated absences.

24. Where This Doctrine Fails (Cost of Implementation)

- Fails when crisis credentials live in the same domain as the assets.
- Fails when drills assume all named personnel are present.
- Fails when receipts are improvised after incident.
- Costs: HSM/offline store, drill cadence, IR retainer with identity specialisation. Payback in first avoided ransom.

25. Procurement & Tabletop Packs

25.2 Tabletop / Drill Pack

1. Drill: ransomware in primary domain; offline identity activates.
2. Detect / contain: domain isolation; offline crisis credential validates.
3. Recover: clean network rebuild; backups restored under signed authority.
4. Forensics: receipt log signed and exported to insurer within 24h.
5. Debrief: drill outcome with mandated absences logged.

26. Evidence Basis — External References & Standards Anchors

Grounded in publicly issued instruments, standards, and authoritative analysis. Independently testable propositions.

- NIST SP 800-184 (Recovery guide).
- CISA #StopRansomware guidance.
- ENISA Threat Landscape — ransomware in OT.
- IEC 62443-2-1 (security programme).
- Lloyd's Cyber Operational Risk Scenario — industrial ransomware.

27. Counterargument & Rebuttal

Tier 1A doctrine is testable against its strongest critique.

The counterargument is that backups are sufficient and that 'identity-led recovery' is over-engineering for a known problem. The rebuttal is operational: every public ransomware case that took weeks to recover involved a failure to restore authority, not data. The marginal cost of pre-staged identity is small; the marginal cost of paying ransom because authority cannot be proven is large.

Annex A — About the Author

Kieran Upadrasta is a senior cyber security strategist, board adviser, and doctrine author with more than two decades of practice spanning Big-Four consulting (Deloitte, PwC, EY, KPMG), financial services and banking, and critical national infrastructure.

- CISSP · CISM · CRISC · CCSP · MBA · BEng.
- Lead Auditor — Information Security Forum (ISF).
- Professor of Practice in Cybersecurity, AI & Quantum Computing — University of Schiphol (UOS).
- Honorary Senior Lecturer — Imperial. Researcher — UCL.
- Platinum Member — ISACA London. Gold Member — (ISC)² London.
- Programme Lead, Cyber Security — PRMIA.

Contact: info@kieranupadrasta.com · www.kie.ie · linkedin.com/in/kieranupadrasta

Annex B — About CSAIC & University of Schiphol (UOS) Affiliation

Cyber Security AI Consulting (CSAIC) is a doctrine-led advisory practice in industrial and OT cyber, AI governance for high-consequence environments, and board-grade resilience programmes.

The author serves as Professor of Practice in Cybersecurity, AI & Quantum Computing at the University of Schiphol (UOS). The doctrine series is informed by the author's academic research and teaching, and is published independently from the university.

Annex C — Quotable Pull-Sheet

"Ransomware does not just encrypt systems. It steals operational authority."

"You restore data with tapes. You restore authority with discipline."

"An unrestorable backup is a museum exhibit."

"The crisis is not the moment to discover who is in charge."

"The vault that never sees the network is the vault that recovers the plant."

"Drill the gaps, not the team."

"Recovery without receipts pays slowly."

Press Wire Drop-Quotes

Benzinga: Ransomware Doesn't Just Steal Files — It Steals Operational Authority

Yahoo Finance: The Identity Doctrine For SCADA Recovery: Why Backups Aren't Enough

CNBC: Pre-Issued Crisis Credentials Become Standard Practice As Insurers Demand Receipts

MarketWatch: Recovery Drills With Mandated Absences Become The New Test Of Industrial Cyber Posture

Reuters: Insurers Waive Recovery Sublimits For Operators With Identity-Led Recovery Programmes

Financial Times: Authority, Not Data, Is The True Target Of Industrial Ransomware

Annex D — Board One-Pager

Single-page synopsis for board pre-read or sales meeting attachment.

Ransomware Stole the Keys, Not Just the Files

The Identity Doctrine for SCADA Recovery

> *“Ransomware does not just encrypt systems. It steals operational authority.”*

- Thesis: ransomware steals authority; backups don't restore control.
- Buy: pre-issued crisis authority + offline identity + drilled recovery.
- Measure: recovery drill time with absences; receipt completeness.
- Win: recovery time ↓60-80%; insurer waives sublimits.
- Risk: crisis credentials co-located with the assets being recovered.

Engagement contact: info@kieranupadrasta.com · www.kie.ie · University of Schiphol (UOS).