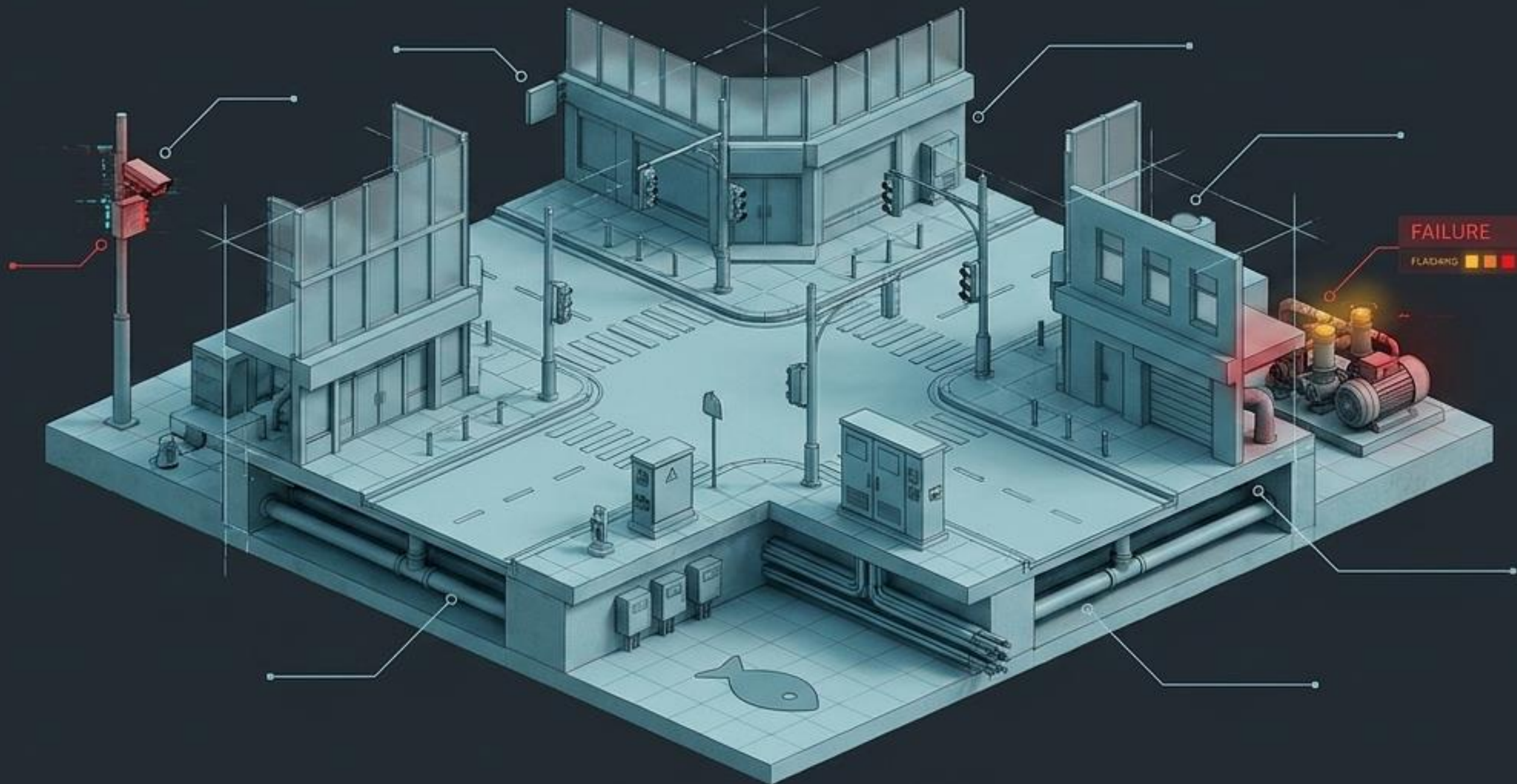


CYBER SECURING SMART CITIES

When everything is connected, everything is an attack surface.



YOU DID NOT WALK INTO THIS ROOM ALONE.

Before we talk about cities, count the connected devices within 10 metres of you right now.



The building's HVAC.

The router.



Your phone.



The display.

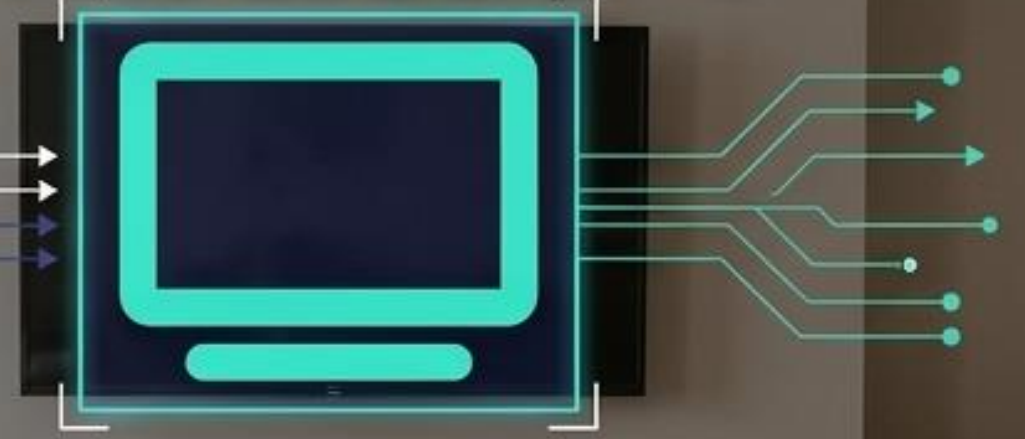
**EACH ONE IS A TINY COMPUTER SOMEONE ELSE CAN TALK TO.
A SMART CITY IS JUST THIS ROOM — MULTIPLIED BY A FEW MILLION.**

HOME ROUTER



The front door to your digital life

SMART TV



A microphone and a screen that sees you

CCTV CAMERA



Built for safety, prized by attackers

CITY SYSTEMS



Water, power, traffic, transit

The Box in Your Hallway: The Router that Phones Home.



**100,000+ routers
beaconing to China.**

20+ Chinese-made models ping a fixed domain every ~35 seconds, running unauthenticated commands as admin.



**A hidden password in
Tenda routers.**

An undocumented second login grants full admin with any username. A budget favourite in India.



**CERT-In flagged TP-Link at
CVSS 10.0.**

HIGH advisories on TP-Link routers. Led India's WLAN market at 27%.

STATE-RUN REALITIES: The FCC banned foreign-made routers. Chinese APTs found hiding backdoor implants in firmware to spy on ministries and run espionage.

The Screen on Your Wall: The TV that Watches Back



Every 10 min.

Skyworth smart TVs scanned home Wi-Fi networks grabbing the name, IP, and MAC of every device, shipping it to a firm claiming 140M TVs.



'Mainland China'

TCL contained flaws letting anyone download the TV's entire filesystem. Stated data-residency: Mainland China.



217,771

The number of infected Android-TV devices in India inside the Vo1d botnet. Many shipped pre-infected from the factory.

You bought a television. You installed a sensor that never sleeps

The Geometric Blast Radius



One Home.
(1 router + 1 TV
+ a phone).



One Street.
(x100 homes, all
misconfigured the
exact same way).



**One City
Command Centre.**
(x millions of devices).

Same flaw. Same vendor. A million times the blast radius.

The Confirmed Threat: Watched through our own cameras.



9 Chinese CCTV cameras (SIM-enabled) near Indian defence sites.



Live feeds routed via Chinese cloud servers.



3 months of surveillance relayed to foreign handlers; 6 arrests made.



India's Response: Mandatory security certification resulted in effective bans on foreign hardware. Indian brands now hold 80%+ of the market. The threat was real enough to redraw national procurement policy.

THE BOTNET CONSCRIPTION: 600,000 CAMERAS BROKE THE INTERNET.



THE SAME BOTNET CODE IS ACTIVE. IN 2022, ATTACKERS USED HACKED INTERNET-FACING CAMERAS AS COMMAND NODES TO TARGET REGIONAL POWER LOAD-DESPATCH CENTRES.

The Scale of the Connected World.

The attack surface is defined by machines, not humans.

Devices, not people—and the curve only bends upward by 2025.

INDIA'S RAPID ATTACK SURFACE EXPANSION

A central brain for a city is a single place to hurt.

₹1.55 L CR
INVESTED

▲ 29.4 LAKH
CYBER INCIDENTS

100

SMART CITIES &
7,700+ PROJECTS



The Physical Consequences of Digital Breaches.

Documented intrusions bridge the air-gap into reality.

156 sirens, 90 mins

(Dallas)

230,000 lost power

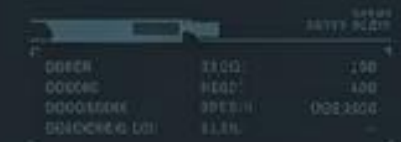
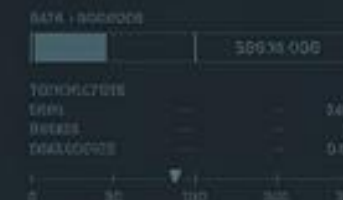
(Ukraine)

11,100 ppm Lye

(Florida)

\$17M recovery

(Atlanta)



INDIA'S INFRASTRUCTURE IS ALREADY UNDER FIRE.

Your attack surface includes everyone you choose to trust.



• AIIMS: Nov 2022
(Two weeks on paper)



• Tata Power: Oct 2022
(Internal data leaked)

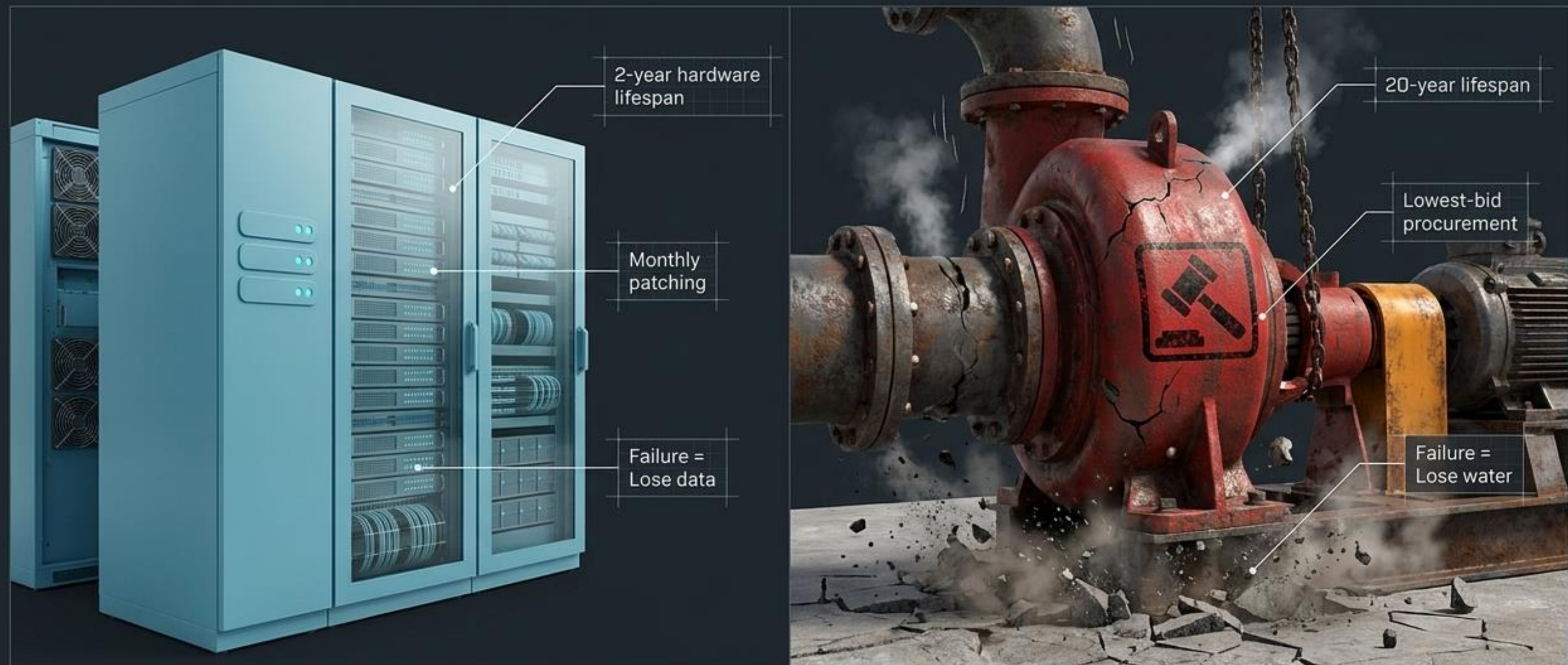
ICMR: Oct 2023
(81.5 crore records)



• Kudankulam: Jul 2026
(19,000 files leaked)

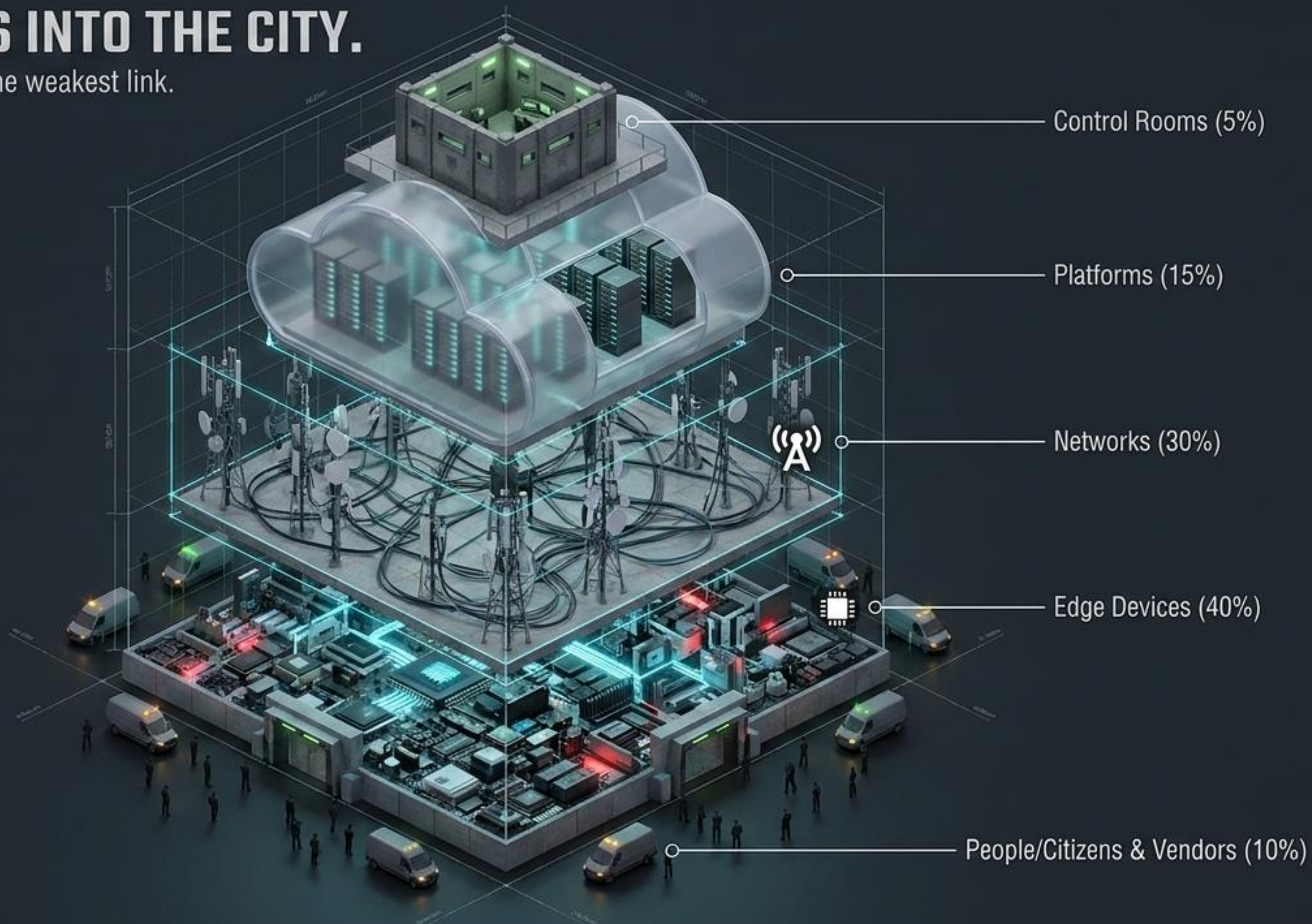
IT VS. OT IS THE HARDEST PROBLEM.

Physical machines have no undo button.



THE SIX DOORS INTO THE CITY.

Attackers only need to find the weakest link.



THE ANATOMY OF A SMART CITY ATTACK.

Every catastrophic failure follows the exact same four steps.

1. Foothold

Attacker gains initial entry through a vulnerable edge device.

2. MOVE

Lateral movement through the network, escalating privileges.

3. FIND

Identify and target critical operational technology (OT) systems.

4. STRIKE

Execute the final command, causing catastrophic physical failure and city-wide impact.

ALERT

THE RESILIENCE PLAYBOOK.

Cut any single link and the attack dies.

CHAOTIC INPUT
(UNSEGMENTED NETWORK)



ORDERLY OUTPUT
(VERIFIED SECURE NODES)



1. Count every connected device because you cannot secure what you cannot see.

2. Segment networks so a compromised thermostat cannot reach a municipal database.

3. Watch for anomalies continuously across both IT and OT environments.

PROCUREMENT AS ACTIVE DEFENSE

Security bolted on after purchase costs multiples of the tender

CHAOTIC INPUT
(UNSECURED SUPPLY CHAIN)

TENDER GATE
(SECURITY VERIFICATION)

ORDERLY OUTPUT
(CLEAN DIGITAL SUPPLY CHAIN)

VULNERABLE INPUT

Threat models
No default passwords
SBOM
24-hr breach notice
Right to audit

VERIFIED SECURE NODES

1. Demand a current Software Bill of Materials (SBOM) for all vendor code.

2. Mandate patch support guarantees for the entire lifetime of the physical hardware.

3. Require a definitive exit plan that revokes access and rotates credentials at handover.

THE PROCUREMENT GOLDMINE: 7 QUESTIONS TO STOP A BREACH



WHERE DOES THE DATA PHYSICALLY GO?

(‘The cloud’ is not an answer. Name the country)



WHO MADE THE FIRMWARE & CAN WE UPDATE IT?

(No written support end-date = do not buy)



ARE THERE DEFAULT PASSWORDS?

(Device must force change on setup)



SHOW ME YOUR SBOM.

(Software Bill of Materials. Can’t list it = can’t secure it)



IS IT CERTIFIED?

(Insist on TEC/STQC and ETSI EN 303 645)



HOW IS IT SEGMENTED?

(A camera must never reach the water plant)



CAN WE RUN THE CITY IF THIS DIES?

(Manual, offline fallbacks are non-negotiable)

AUDIT CHECKLIST: CRITICAL CONTROLS

DATA FLOW VALIDATION

LIFECYCLE MANAGEMENT

CERTIFICATION COMPLIANCE

HOW IS IT SEGMENTED?

RESILIENCE PLANNING

THE TEN-QUESTION CITY CYBER SCORECARD

Score honestly today to prevent a crisis tomorrow.



SCORE 8-10: RESILIENT

SCORE 4-7: EXPOSED BUT FIXABLE

SCORE 0-3: THE FISH TANK

Category	Score	Weight	Weighted Score
Category 1	10	1	10
Category 2	8	2	16
Category 3	6	3	18
Category 4	4	4	16
Category 5	2	5	10
Category 6	1	6	6
Category 7	0	7	0
Category 8	0	8	0
Category 9	0	9	0
Category 10	0	10	0
Total		50	70

Score	0	10	20	30	40	50	60	70	80	90	100
Score	0	10	20	30	40	50	60	70	80	90	100

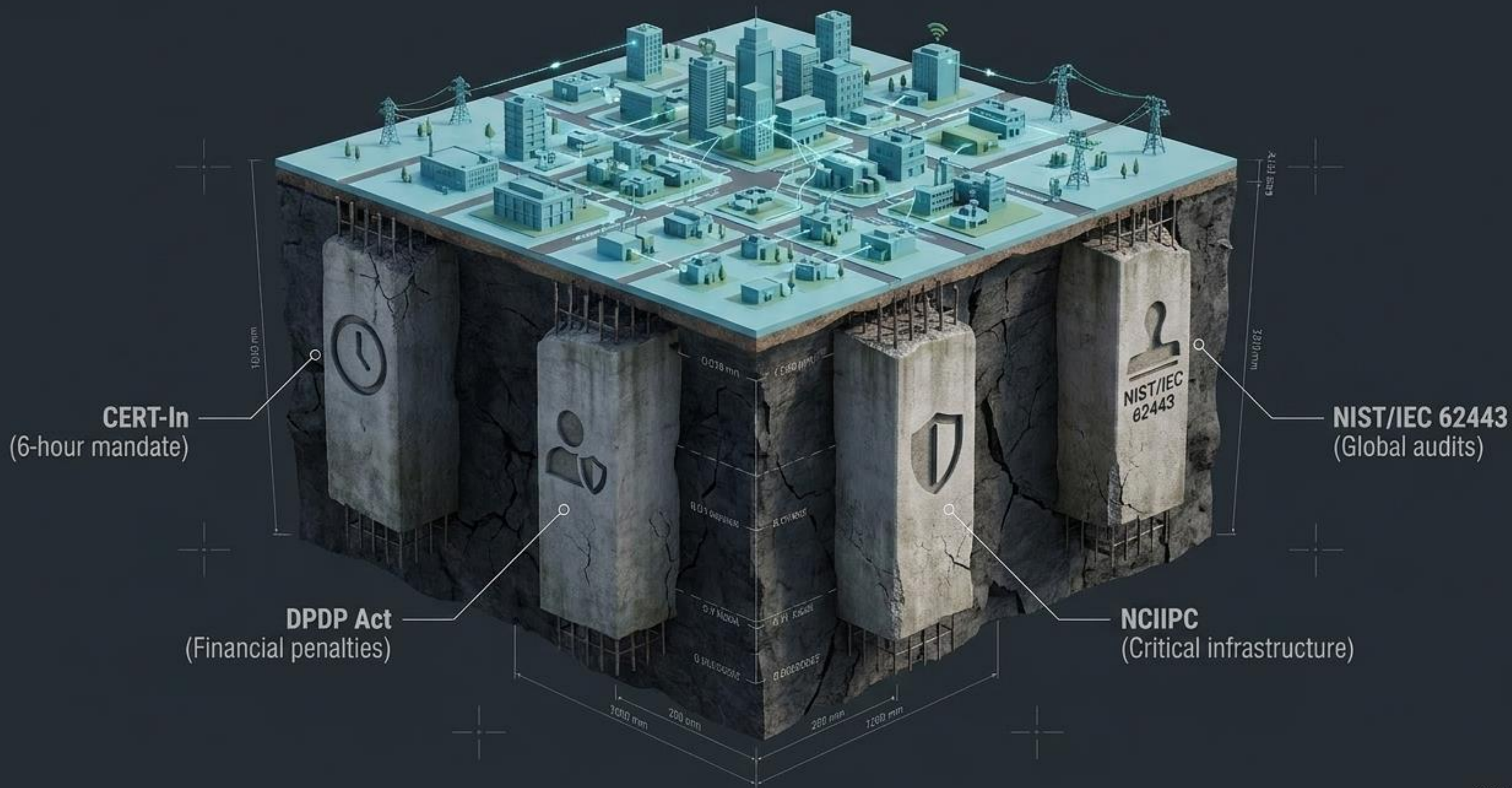
RANSOMWARE AT THE COMMAND CENTER

The most critical decisions happen in the first sixty minutes.



THE REGULATORY FOUNDATION OF RESILIENCE.

Compliance is the floor preventing collapse, not the ceiling.



THE FINAL MEASURE OF A SMART CITY.

A city is smart only when it can survive being connected.

MERELY SMART



RESILIENT



1. Can anyone show me the device list?



2. Have we rehearsed the 2 a.m. strike?



2. Have we rehearsed the 2 a.m. strike?



3. Which vendor holds our blueprints?

The background is a photograph of a city street at night, with buildings and streetlights visible. Overlaid on this is a blue wireframe grid. In the foreground, there are several 3D wireframe models of buildings and infrastructure, including a large building on the left, a series of smaller buildings in the center, and a complex of pipes and tanks on the right. The main text is centered over the middle of the image.

Security is not a feature you add. It is the foundation you build on.

Every attack tonight began with something ordinary—a default password, an unpatched box, a vendor no one questioned. Which means every defence begins with something ordinary too. That part is in your hands.

When everything is connected, make sure security is one of the connections.

Elevate your SOC with AI - Native Intelligence

SIEM

24•7 Data-Driven
Security Insights



Unified Bigdata Platform

Timeless Intelligence -
Data Foundation



Security Assurance

Identify. Prioritise.
Eliminate.



SOAR

AI & ML- Based
Automated Response



Flagship

Agentic SOC

Autonomous. Intelligent. Always-On.

EASM

See your attack
surface first



Deception

Honeypots &
Decoys



UEBA

Smarter Entity
Behaviour Analytics



NDR

Deep Intell-Driven
Network Insights



NBAD

Definitive Network
Monitoring Platform



Threat Intelligence

Noise-Nill Data
for Active Reflex



Growing Trust Nationally

