MITSUBISHI ELECTRIC · PRACTICAL CYBER × DACTA × APEXAGEN

The BMS Cyber-Sales Training

Day 1 — The Context & The Code

Practical Cyber DACTA APEXAGEN TECHNOLOGY

GET SET UP NOW — ON YOUR PHONE

Everything's at bms.ethanseow.com

- **Check in** for today's session — Day 1 & Day 2
- The **10 hands-on drills** we run through the day
- **Download** today's slides to keep

YOUR TRAINER

Ethan Seow

- Creator of the **Practical Cyber Framework** — the method behind these two days
- CEO, **Practical Cyber** · Co-founder & CEO, **Centre for AI Leadership (C4AIL)**
- ISACA Singapore **2023 Infosec Leader of the Year** · ISC2 **2023 APAC Rising Star**
- CABCY EXCO & Cybersecurity Lead · Div0 Lead Crew · TEDx & Black Hat Asia speaker
- I sell, teach and defend cyber **and** AI for a living — that intersection is this class

BEFORE AI — WHERE I STARTED

A doctor's foundation

Trained in medicine — the discipline of diagnosis, evidence, and decisions you are accountable for. It is the same instinct I bring to cyber and AI.

BEYOND MEDICINE — BUILDING & PERFORMING

What I've built, and played

Who's in the room

Who you are

Mitsubishi Electric BMS **sales & tender team**

What you sell

You sell chillers, lifts, HVAC, controllers, access & CCTV

Not IT

You are **not** here to become the IT department

The objective — by 17:30 tomorrow

Read, translate, defend

Read a real cyber tender · **translate** it · **defend** it

An advisor

You won't become technical — you'll become an advisor who **can't be fooled**

The proof

Proof: sort the real Section 42, then pitch it to a board

The two days

Day 1

the building, the code, the jargon, the Pillars

Day 2

AI as a governed co-pilot, then the pitch

Hands-on

Hands-on throughout — **bms.ethanseow.com**

The cyber section is where the deal is won or lost — on trust, not price.

It's not "the IT department's paragraph." It's the part where the owner depends on you for 15–20 years.

The misclassification

The mistake

Most teams treat cyber as a **compliance Thorn** to dodge

The reality

It's actually a **Rose** — a differentiator to lead with

The conversion

This class converts the Thorn into the Rose

MODULE 1

The IT/OT Bridge

Why a hacked HVAC plant or lift is a business and life-safety risk.

IT — Information Technology

- Runs **information**: email, records, payments
- When IT fails, **data leaks**
- Worst case: a breach, a headline, a fine

IT
Runs information
A breach leaks data
Confidentiality first

vs

OT
Runs physical processes
A breach stops the building
Safety first

Same word — **different stakes**.

OT — Operational Technology

- Runs **physical processes**: chillers, AHUs, lifts, fire, power
- When OT fails, **something physical happens**
- A building is almost entirely OT

IT
Runs information
A breach leaks data
Confidentiality first

vs

OT
Runs physical processes
A breach stops the building
Safety first

Same word — **different stakes**.

Same word "security" — different stakes

- IT: keep the **data** safe
- OT: keep the **process** safe — and people
- You can't borrow the IT playbook wholesale

> **A hacked building isn't a data problem. It's a life-safety problem.**

IT

Runs information

A breach leaks data

Confidentiality first

vs

OT

Runs physical processes

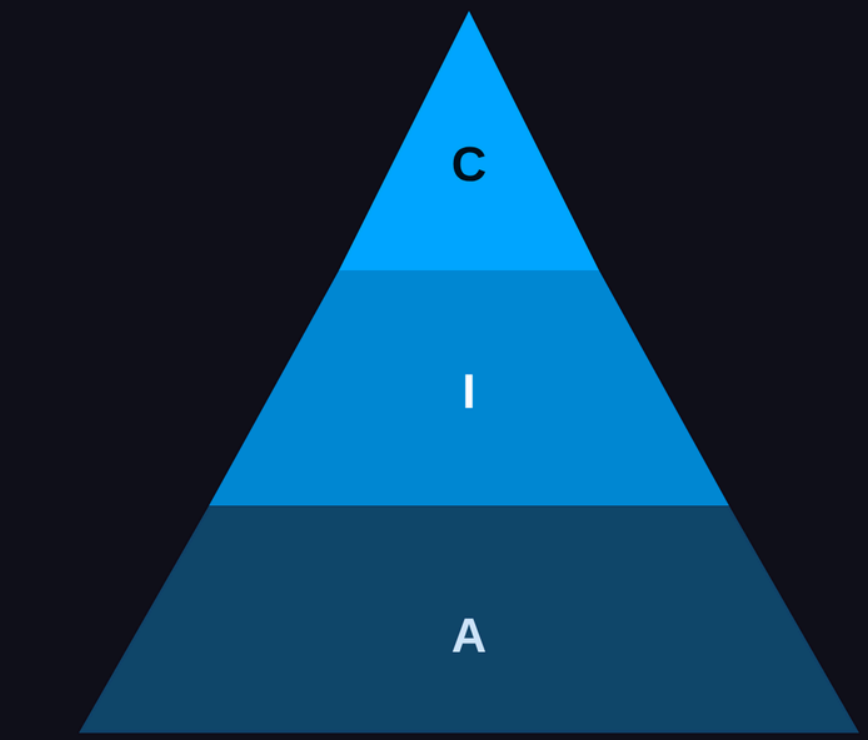
A breach stops the building

Safety first

Same word — **different stakes**.

First, what "security" means in IT — the CIA triad

- Every control you'll meet defends one of **three** properties
- You can't say why a building is different until you name what it differs from
- That reference point is **CIA**

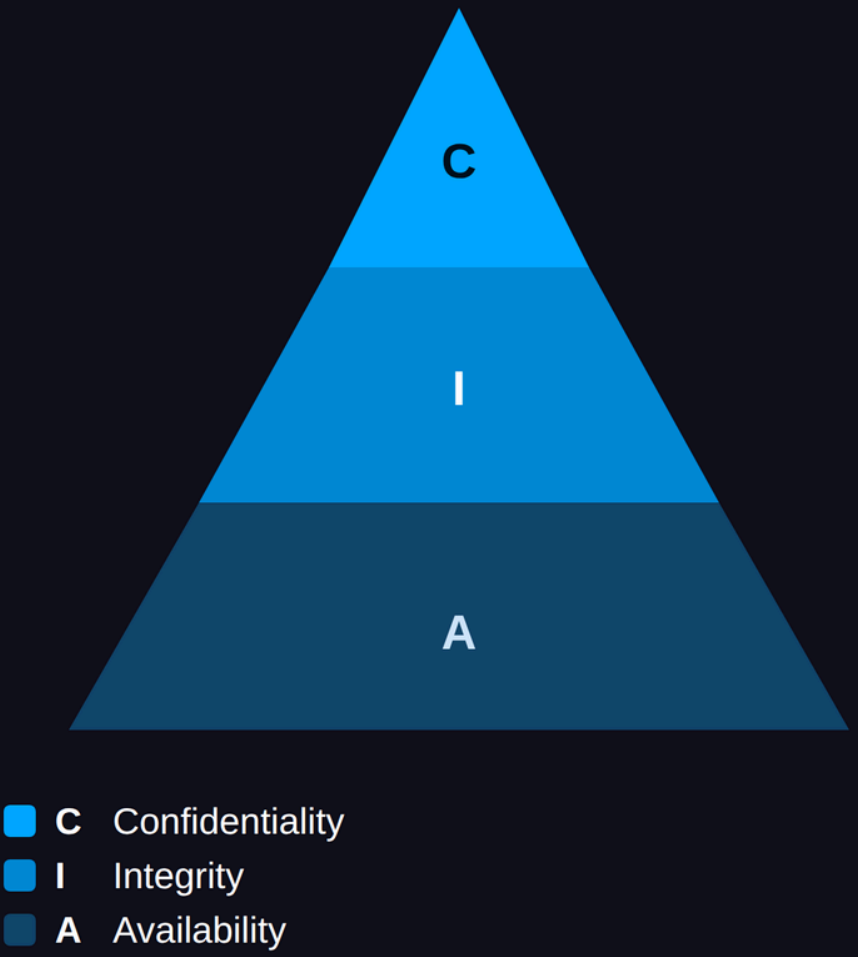


C Confidentiality
I Integrity
A Availability

IT ranks them **Confidentiality first**.

Confidentiality

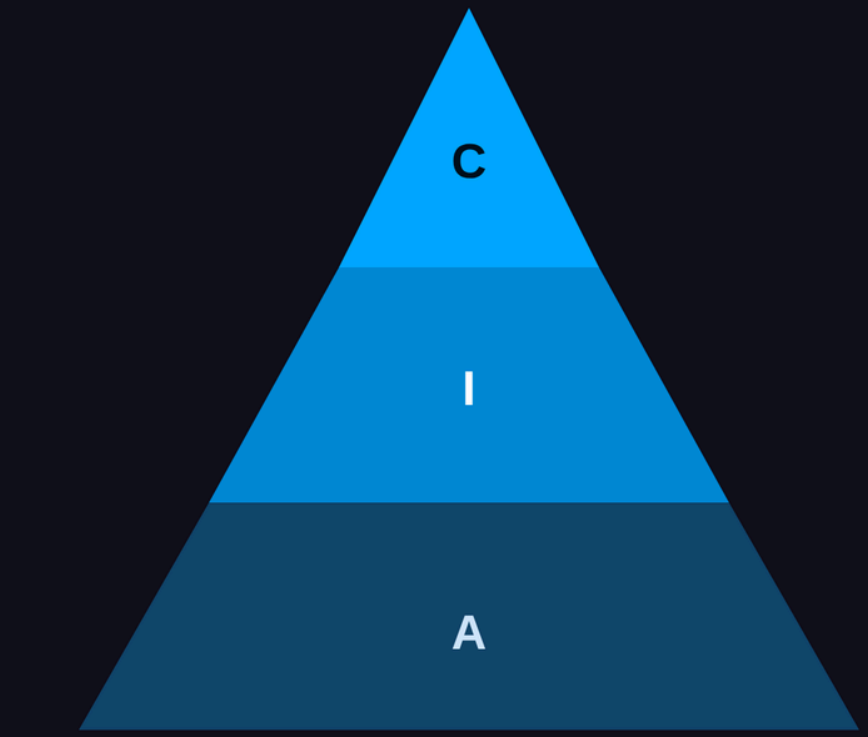
- **Secrecy** — who is allowed to **read** it
- In a building: the tenant list, CCTV, access logs
- Served by encryption, access control, authentication



IT ranks them **Confidentiality first**.

Integrity

- **Trustworthiness** — data and **commands** aren't altered
- Can you trust the screen, and what the controller was told?
- When it fails you get a **lie** — "normal" while a chiller dies (Stuxnet)

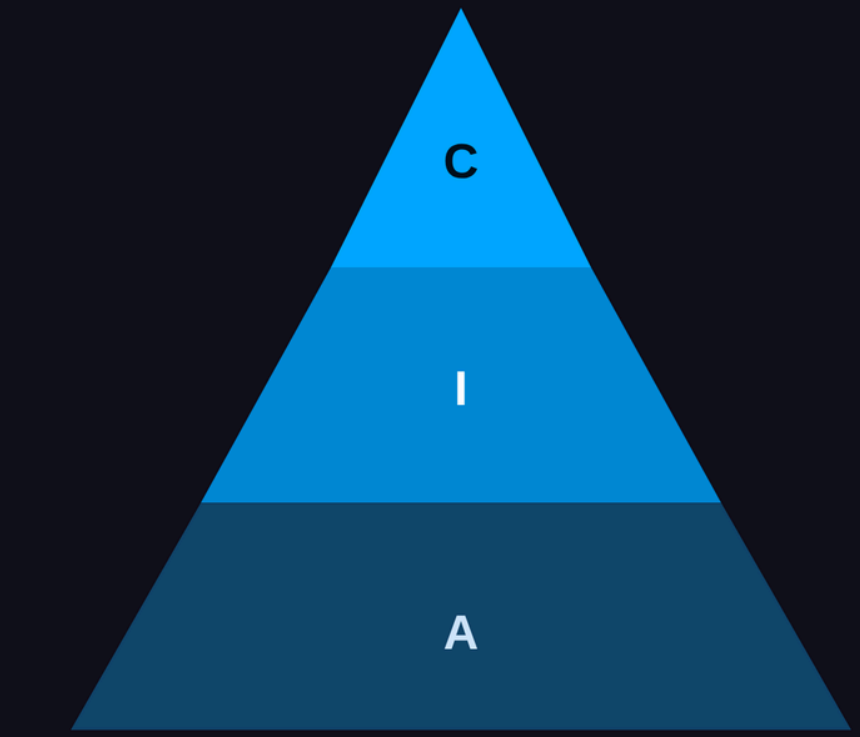


C Confidentiality
I Integrity
A Availability

IT ranks them **Confidentiality first**.

Availability

- **Up and answering** when needed
- For a hospital chiller, availability **is** the mission
- Protected by redundancy, backups — and **not** breaking it with heavy IT security



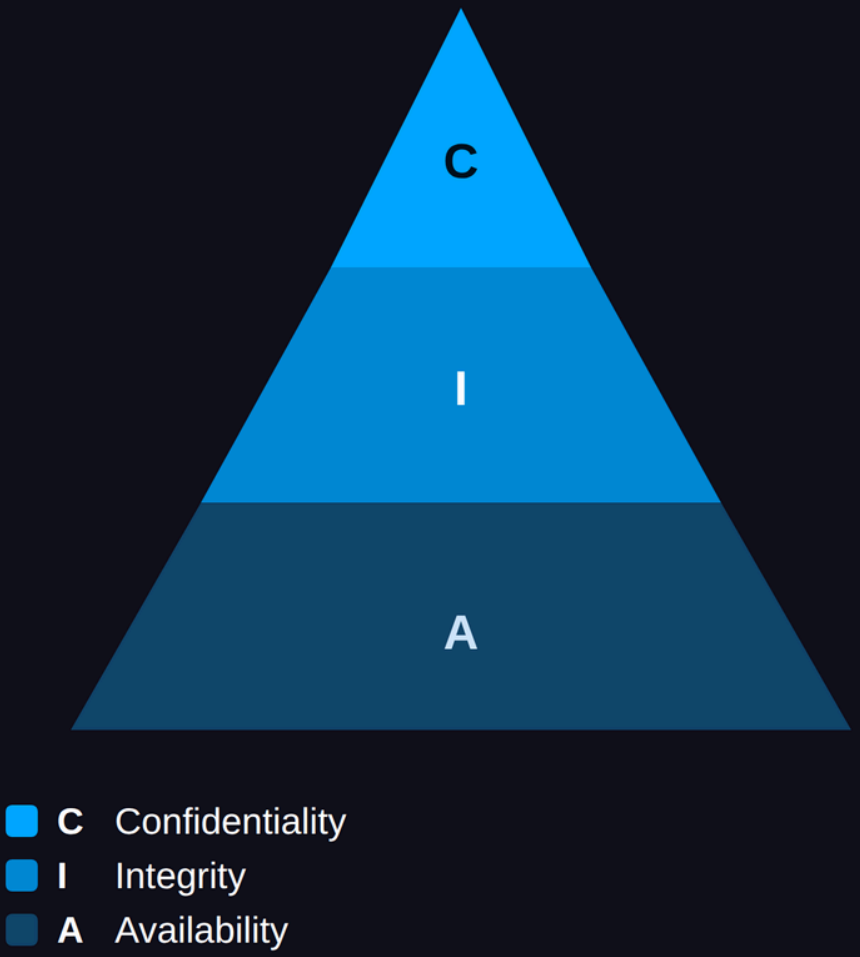
C Confidentiality
I Integrity
A Availability

IT ranks them **Confidentiality first**.

IT ranks them C → I → A

- Confidentiality **first** — a data leak is the worst outcome
- A five-minute outage is forgotten by lunchtime
- So IT's instinct: patch hard, lock data down

> **Hold that order — a building inverts it.**



IT ranks them **Confidentiality first**.

How a building network is actually built

Top to bottom

The internet is at the **top**; your fire panel is at the **bottom**

The Purdue model

The standard map is the **Purdue model** — Levels 0–5

The boundary

Security is the story of the **boundary** between them

MODULE 1

How a building network is actually built — the Purdue model

The internet is at the top. Your fire panel and chiller controller are at the bottom. Security is the story of the boundary between them.

LEVEL 4 – 5 **Enterprise IT**	Internet · corporate email · cloud apps · staff laptops — where IT security lives (CIA: confidentiality first)	IT ZONE
LEVEL 3.5 · DMZ **The IT / OT boundary**	**Firewall · jump host · the one controlled crossing point.** Cross it and you're inside the building. Target (2013) crossed it through an HVAC vendor's remote access.	⟷
LEVEL 3 **Operations**	BMS servers · historian · engineering workstation	OT ZONE
LEVEL 2 **Supervisory**	BMS head-end (Niagara / Desigo / Metasys) · SCADA / HMI · operator screen	OT ZONE
LEVEL 1 **Basic control**	DDC controllers · PLCs · JACE · lift controllers · ⚠ fire panel	OT ZONE
LEVEL 0 **Physical process**	Chillers · AHUs · fans · dampers · lifts · sensors & actuators **BACnet / Modbus** speak here — no authentication. Reach the wire, command the device.	OT ZONE

A hacked building is a life-safety problem — because the attack ends at Level 0, on real machines.

SRP > CIA · segment the zones · watch the boundary

Level 4–5 · Enterprise IT

What's here

Internet, email, cloud, staff laptops

IT security

This is where **IT security** lives (CIA, confidentiality-first)

Top of stack

The top of the stack — the least physical

Level 3.5 · the IT/OT boundary (DMZ)

One crossing

The **one controlled crossing point** — firewall + jump host

Cross it

Cross it and you're inside the building

Target 2013

Target (2013) crossed it through an HVAC vendor's remote access

> **Almost every building attack is a story about crossing this line.**

Levels 2–3 · Supervisory & Operations

L3
BMS servers, historian, engineering station

L2
the BMS head-end (Niagara/Desigo/Metasys), SCADA/HMI, the operator screen

Trust the screen
If you can't trust the screen, you can't run the building

Levels 0–1 · Control & the physical process

L1

DDC controllers, PLCs, JACE, lift controllers, the **fire panel**

L0

chillers, AHUs, fans, dampers, lifts, sensors

The end

The attack ends **here**, on real machines

Two facts fall out of the picture

No authentication

The bottom protocols (**BACnet/Modbus**) have **no authentication**

Can't patch

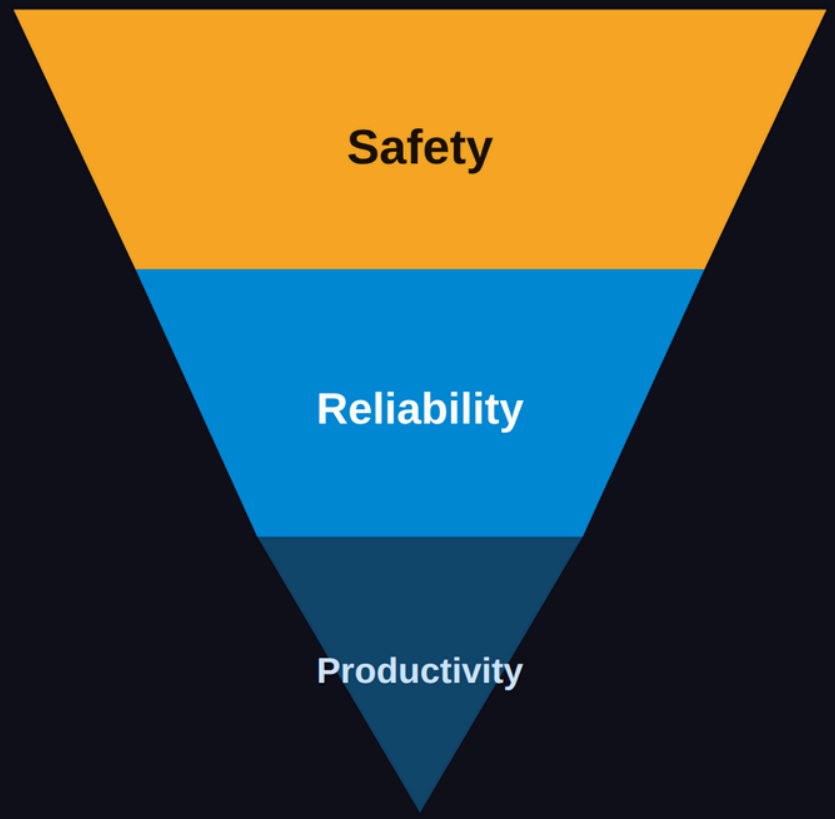
The bottom systems **can't be rebooted or patched** like a laptop — they're a live process

Why it's different

These two facts are **why** building security is different

So a building inverts the triad — SRP

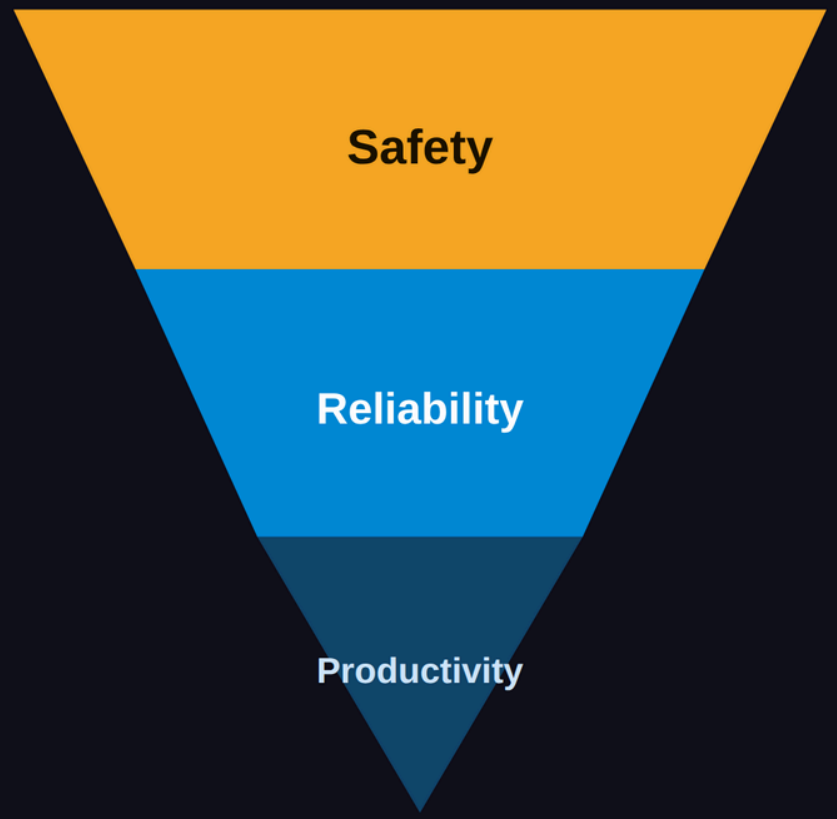
- At L0–L2 the system **is** the physical process
- Availability + safety **dominate**; the order flips
- **S**afety → **R**eliability → **P**roductivity



Safety first — Confidentiality drops to last.

Safety (1st)

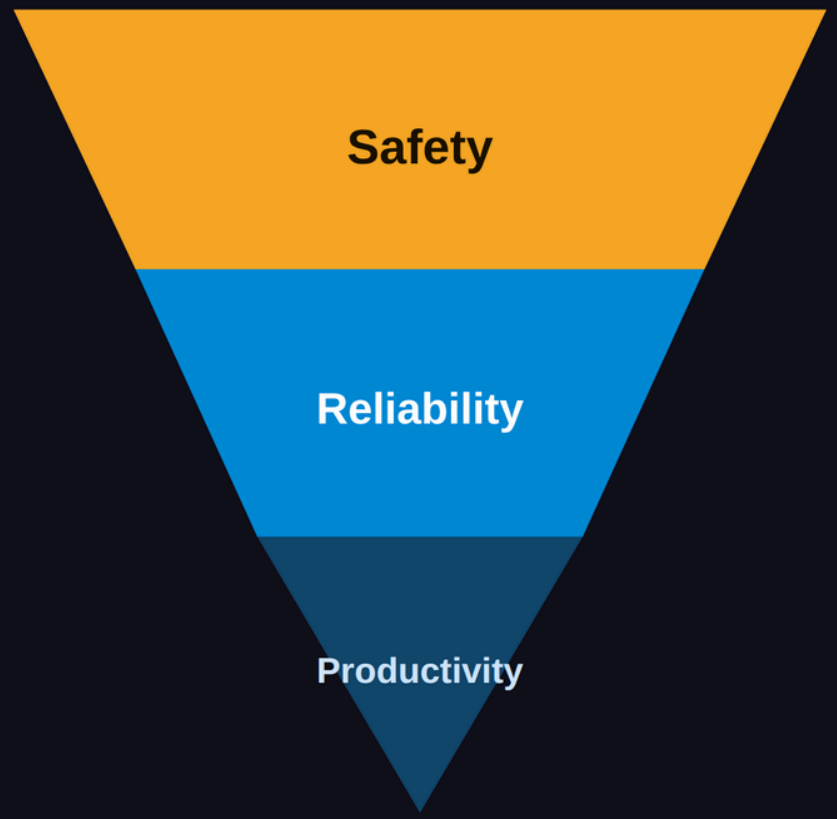
- Fire detection & suppression, smoke control, lift release, emergency power
- The protection of **human life** — non-negotiable
- Never let a security control touch a life-safety sequence



Safety first — Confidentiality drops to last.

Reliability (2nd)

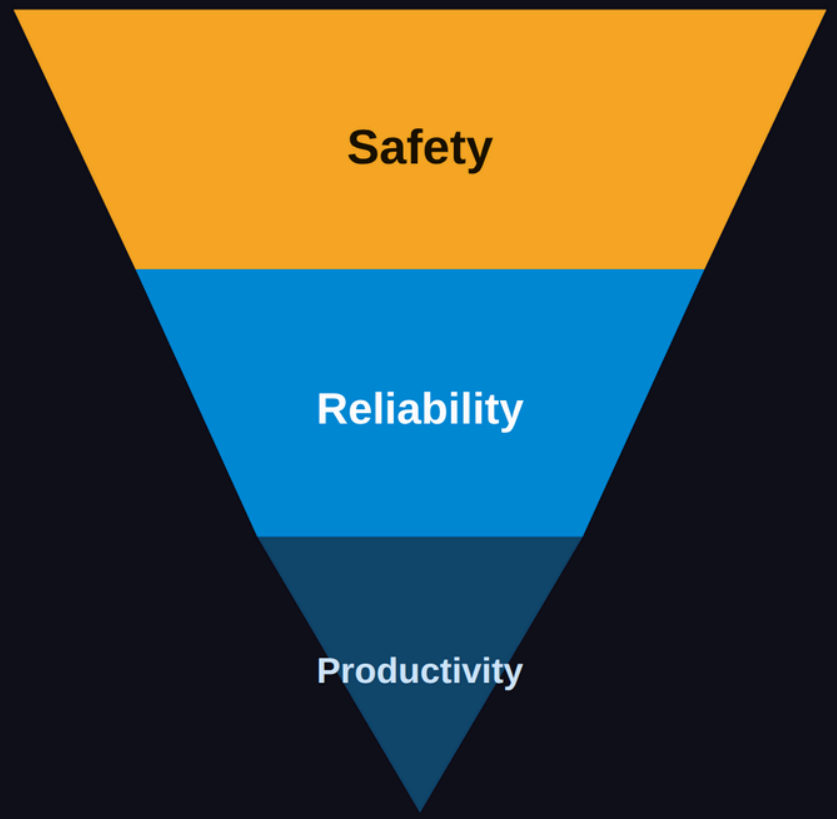
- Continuity: cooling for data halls & hospitals, tenant SLAs, lift uptime
- A dropped chiller in a data hall = millions/hour
- Keeping the process running



Safety first — Confidentiality drops to last.

Productivity (3rd)

- Energy, predictive maintenance, green-mark, asset value
- Confidentiality doesn't vanish — it just stops being **first**
- A stolen temperature log is survivable; a stalled smoke fan isn't



Safety first — Confidentiality drops to last.

The gate question

The question

Ask of any system: **"Does this control a physical process?"**

Always yes

For a BMS the answer is **always yes** — so SRP is always on

OT not IT

That test tells you when to think OT, not IT

Sell in SRP order

Safety first

Open on **safety & continuity**; close on cost — never the reverse

The line

"The fire matrix runs on the same network you're asking us to secure."

Not price-first

Feature-and-price-first is what makes you sound like every other vendor

The building's Crown Jewels

The physical process and what commands it — **not** the data. Name them, and you know what to protect first — each maps to a Pillar.

Fire & life-safety

Detection, suppression, smoke control, lift-release — the crown itself.

The head-end

The BMS supervisory brain — sees and commands everything below it.

Field controllers

The DDCs/PLCs that actually drive the plant — the hands.

Lifts

Their own controllers and safety circuits — people-movement.

Access & CCTV

The keys to the doors and the eyes on the building.

Power

Electrical distribution the whole building rides on.

The key ring — remote access

Runs no process itself, but it can reach every jewel above. Guard it hardest.

Crown Jewels (1/2)

Fire & life-safety
the last barrier before casualties

BMS head-end
the trusted screen you run the building from

Controllers & lifts
the physical actuators

Crown Jewels (2/2)

Access control & CCTV
one credential owns the fleet (Verkada)

Power
loses everything above it

The remote-access layer
the #1 attack path (Target)

Degraded-mode operation

The question

Can the building run its life-safety functions **without** the BMS?

Manual fallback

Operators keep it safe manually if the digital brain is down

The reassurance

"If the digital brain is offline, your building still runs safely."

ACTIVITY · W1

Profit-Centre Map

- Map each function — power, cooling, access, lifts, fire — to what the **owner** pays to protect
- Circle the one that hurts most if it fails

Every technical system ties to a business outcome — **that mapping is your sell.**

MODULE 2

Selling into Governed Clients

CCoP without the fear — your biggest clients are the ones it governs.

CCoP — what it is

Cybersecurity Code of Practice

Singapore's mandatory cyber code

Issued by CSA

Issued by **CSA** under the Cybersecurity Act (2018, amended 2024)

Structured

A structured code, not a mood

CII — what it is

Critical Information Infrastructure

systems whose loss cripples an essential service

CSA designates

CSA **designates** the operators; obligations follow

CCoP binds

CCoP binds designated CII

The essential-services sectors

Critical sectors

Healthcare · transport · energy · water

More sectors

Banking & finance · government · infocomm

Your accounts

Your key accounts live here

Your key accounts ARE these operators

The operators

Hospitals · MRT/rail · airports · data centres · utilities · government buildings

The implication

Selling a chiller plant into a hospital = walking into a CCoP-governed requirement

Fluency wins

Fluency wins; silence disqualifies

The 30-second check — the tells

Pass/fail section

A dedicated, **pass/fail** cyber section

The keywords

Words: **segmentation, MFA, asset inventory, incident reporting, hardening**

The references

A vendor security questionnaire; references to **CSA / the Act / IEC 62443**

What CCoP asks for — the lifecycle

- Structured as **Govern** → **Identify** → **Protect** → **Detect** → **Respond** → **Recover**
- The same backbone as the NIST CSF
- Know the shape and a dense section stops being scary

CCoP is a **structured lifecycle** — it repeats.

What CCoP asks for — the control families

- Access control & MFA · network segmentation · logging & monitoring
- Incident reporting to CSA within set timelines
- Audits, risk assessments, secure hardening

> **Every family maps to a Pillar in Module 4.**

1. **Govern**
2. **Identify**
3. **Protect**
4. **Detect**
5. **Respond**
6. **Recover**

CCoP is a **structured lifecycle** — it repeats.

IEC 62443 — the OT standard tenders point to

The standard

The standard behind "align to recognised OT-security principles"

Zones & conduits

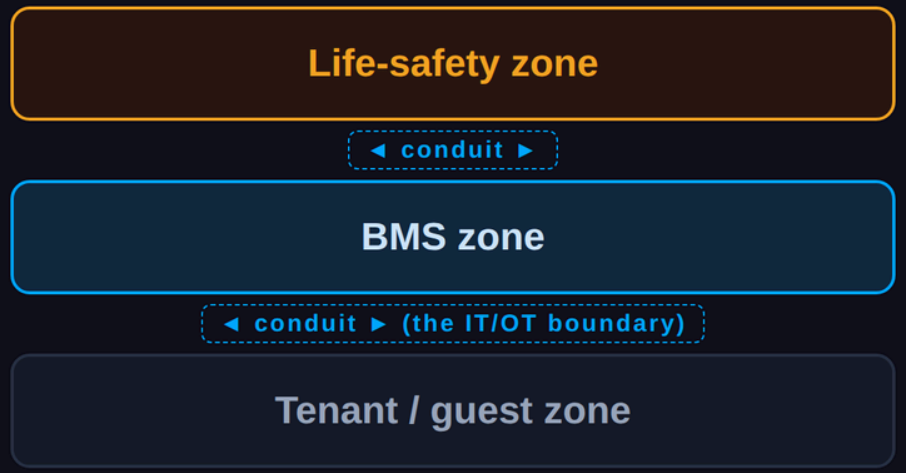
Its core idea: **zones and conduits**

The vocabulary

Recognising the vocabulary signals real competence

Zones

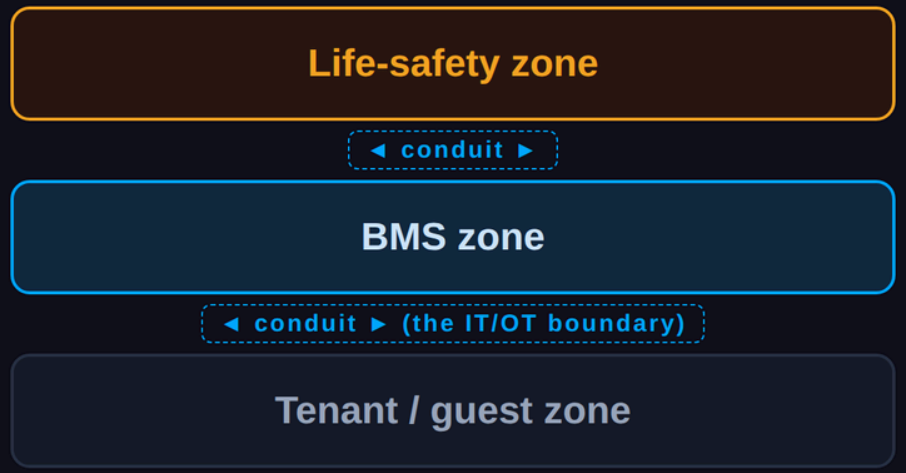
- Group assets by **risk and trust**: a life-safety zone, a BMS zone, a guest zone
- Everything in a zone shares a security level
- This **is** the Purdue picture, formalised



Group by risk into **zones**; control every **conduit**.

Conduits

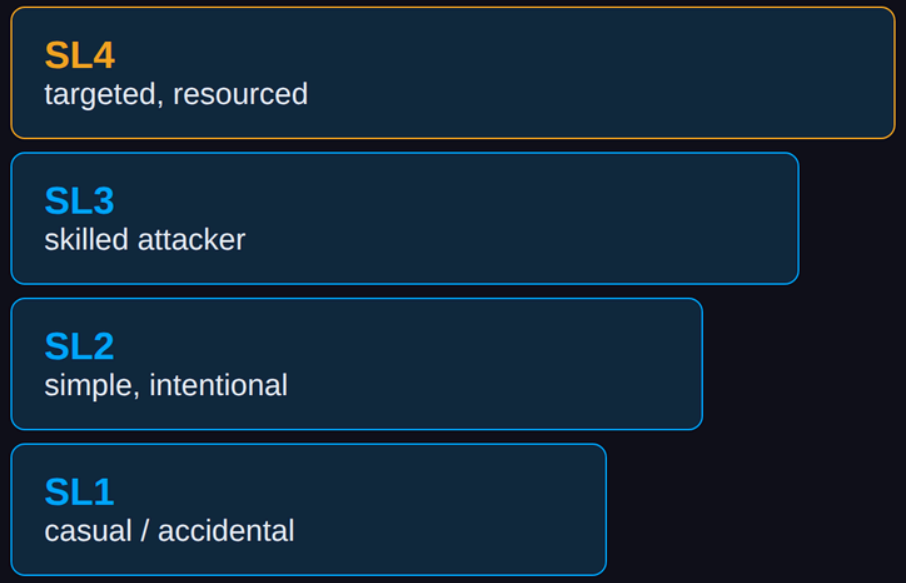
- Every **connection between zones** is a conduit — identified and controlled
- The **IT/OT boundary is the most important conduit**
- Control the conduit, contain the blast radius



Group by risk into **zones**; control every **conduit**.

Security Levels SL1–SL4

- A rating of the **attacker** a zone is protected against
- **SL1** casual/accidental → **SL4** targeted, skilled, well-resourced
- "Align to 62443" means: zones, conduits, and a stated SL



Security Levels rate the **attacker** you're protected against.

The supply-chain cascade

Legally accountable

A CII operator is **legally accountable** — so it pushes obligations **down** through the contract

What cascades

Vendor remote-access, segmentation, asset inventory, incident reporting

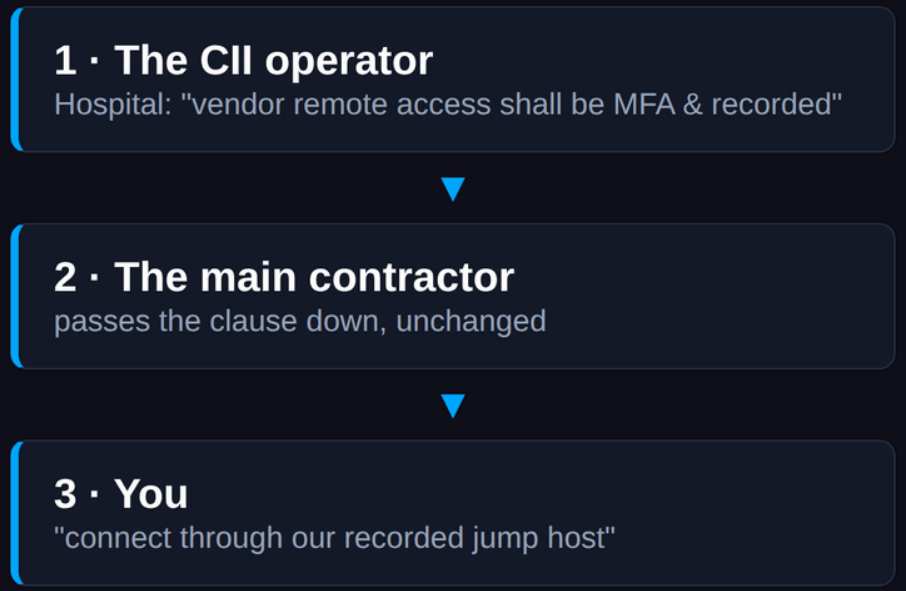
You inherit it

You inherit it, named in the Act or not

The cascade in three hops

- **Hop 1** — a hospital (CII): **"vendor remote access shall be MFA and recorded."**
- **Hop 2** — the main contractor passes it down unchanged
- **Hop 3** — it lands on you: **"connect through our recorded jump host."**

> **You never signed the Act — but you're delivering to it.**



One obligation, **three hops** — you deliver to the Act.

The precision guardrail

Know who

Know **exactly** who CCoP binds

Don't overclaim

Never tell a non-CII landlord "you're legally mandated" — the overclaim kills credibility

Precision

Precision **is** the expertise

When the client isn't CII — the other hooks

Insurance

insurers demand cyber controls

Tenant clauses

MNC & government tenants require them

More hooks

SCDF/BCA (life-safety), **PDPA** (CCTV/access data), **green-mark / asset value**

Sell these — real, and defensible.

ACTIVITY · W2 · GOVERNED-CLIENT DETECTOR

Spot the Governed Client

- Six briefs: CII / cascade-exposed / not governed
- Argue the two judgment cases: the bank-tenant tower & the clinic-in-a-mall

Web: **Governed-Client Detector** — recognise → read the clauses → answer in building-safety language.

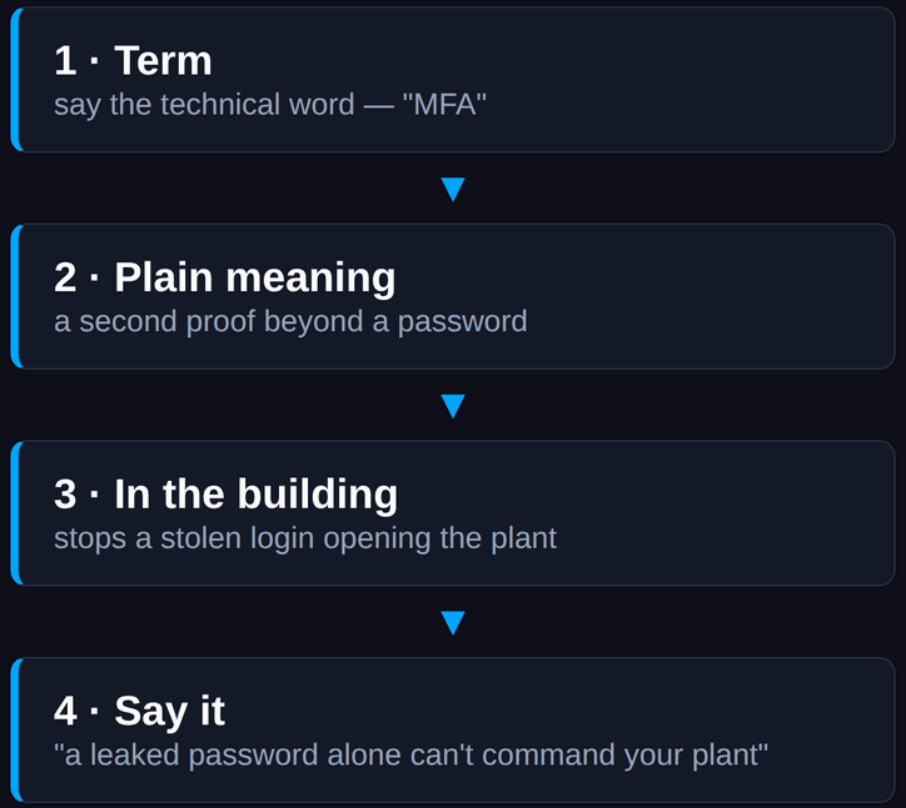
MODULE 3

The "Babel Fish"

Every cyber term is a building-safety promise in disguise. Translate it.

The translation method

- **Term → plain meaning → what it protects → the sentence you say**
- Four steps for any acronym a tender throws at you
- The heart of the whole course



The **Translator** move — for any acronym.

Use the term AND define it

Don't dumb down

Don't dumb cyber down — **translate** it

Explain it

Say "MFA", then explain it in one breath

Earns trust

The owner trusts you **more**, not less — that's the respect move

Why building protocols have no security

No authentication

Modbus/BACnet read & write device registers with **no authentication**

Reach = trust

Whoever reaches the wire is trusted to command the equipment

The heart

This is the technical heart of building cyber

Why — they were built for isolated networks

Built isolated

Designed in the 1980s–90s for **physically isolated**, trusted networks

Now false

That assumption is now false — they touch IT and the internet

Can't retrofit

But you can't retrofit auth onto the installed base

You can't patch it — so build the boundary

Architectural fix

The fix is **architectural**: segment so nothing untrusted reaches the wire

Monitor

for anomalous commands

FrostyGoop

needed no exploit — it just spoke Modbus

Jargon — Authentication

Plain meaning
proving you are who you say

In the building
the login before anyone changes a setpoint

> *Say it: "every command is tied to a named, proven identity."*

Jargon — MFA

Plain meaning
a second proof beyond a password

In the building
stops a stolen contractor login opening the chiller plant

> *Say it: "a leaked password alone can't command your plant."*

Jargon — SSO

Plain meaning

one managed identity; revoke once, revoke everywhere

In the building

a leaver's access dies with their account

> *Say it: "when someone leaves the project, their access ends that day."*

Jargon — PAM

Plain meaning

tight control + recording of admin access

In the building

governs who can rewrite fire logic and setpoints

> *Say it: "the powerful changes are gated and recorded."*

Jargon — RBAC

Plain meaning

access by job role, not person-by-person

In the building

an operator operates; only an engineer reprograms

> *Say it: "people get exactly the access their role needs."*

Jargon — Shared account

Plain meaning

one login many people use — a known risk

In the building

"BMS_Operator" on a sticky note

> *Say it: "we remove shared logins so every action traces to a person."*

Jargon — EDR

Plain meaning

a guard on each computer watching behaviour

In the building

watches the BMS workstation

> *Say it: "your BMS workstation is monitored, not fitted and forgotten."*

Jargon — Patching / firmware

Plain meaning

fixing known holes in device software

In the building

controllers on years-old, unsupported firmware

> *Say it: "we track firmware & support status per controller."*

Jargon — Default credentials

Plain meaning
the factory admin/admin

In the building
controllers & cameras shipped with public passwords

> *Say it: "we change every factory password before handover."*

Jargon — Asset inventory

Plain meaning
a live list of everything connected

In the building
most buildings can't produce one

> *Say it: "visibility is the first deliverable, not an afterthought."*

Jargon — Segmentation

Plain meaning

isolated network zones

In the building

keeps tenant/guest/CCTV away from fire & lift controllers

> *Say it: "life-safety on its own island."*

Jargon — Micro-segmentation

Plain meaning

fine-grained, device-by-device zoning

In the building

each critical system walled off from the next

> *Say it: "even inside, systems can't freely reach each other."*

Jargon — Flat network

Plain meaning

everything sees everything — the bad default

In the building

the lobby Wi-Fi can reach the fire panel

> *Say it: "that's how a tenant laptop ends up at the chiller."*

Jargon — IT/OT boundary

Plain meaning

the monitored gate between office IT and controls

In the building

where email/internet meets the BMS

> *Say it: "one controlled crossing, and it's watched."*

Jargon — Zero Trust

Plain meaning
never trust by location; verify every access

In the building
being "inside" the network grants nothing

> *Say it: "being on the network isn't a key."*

Jargon — Air-gapped

Plain meaning
no internet path at all

In the building
a control network physically isolated

> *Say it: "the attack surface simply isn't there."*

Jargon — Remote access

Plain meaning

logging in from off-site to support the system

In the building

how the integrator services the BMS

> *Say it: "convenient — but the #1 way buildings get breached."*

Jargon — VPN & jump host

VPN
an encrypted tunnel in → "no always-on back-door"

Jump host
one monitored doorway for support

> *Say it: "we show you who connected and what changed."*

Jargon — Setpoint / fire matrix & backup

Setpoint / fire matrix
the values & life-safety logic → "we baseline and alert on change"

Backup / degraded-mode
restore, and run without the BMS

> *Say it: "an incident is a recovery, not a rebuild."*

ACTIVITY · BABEL FISH TRANSLATOR

The Translator Drill

- Draw a term; in 30 seconds give plain meaning + building example + the sales line
- Two rounds, table coaches

Web: **Babel Fish Translator** — the skill is saying it **cold**.

MODULE 4

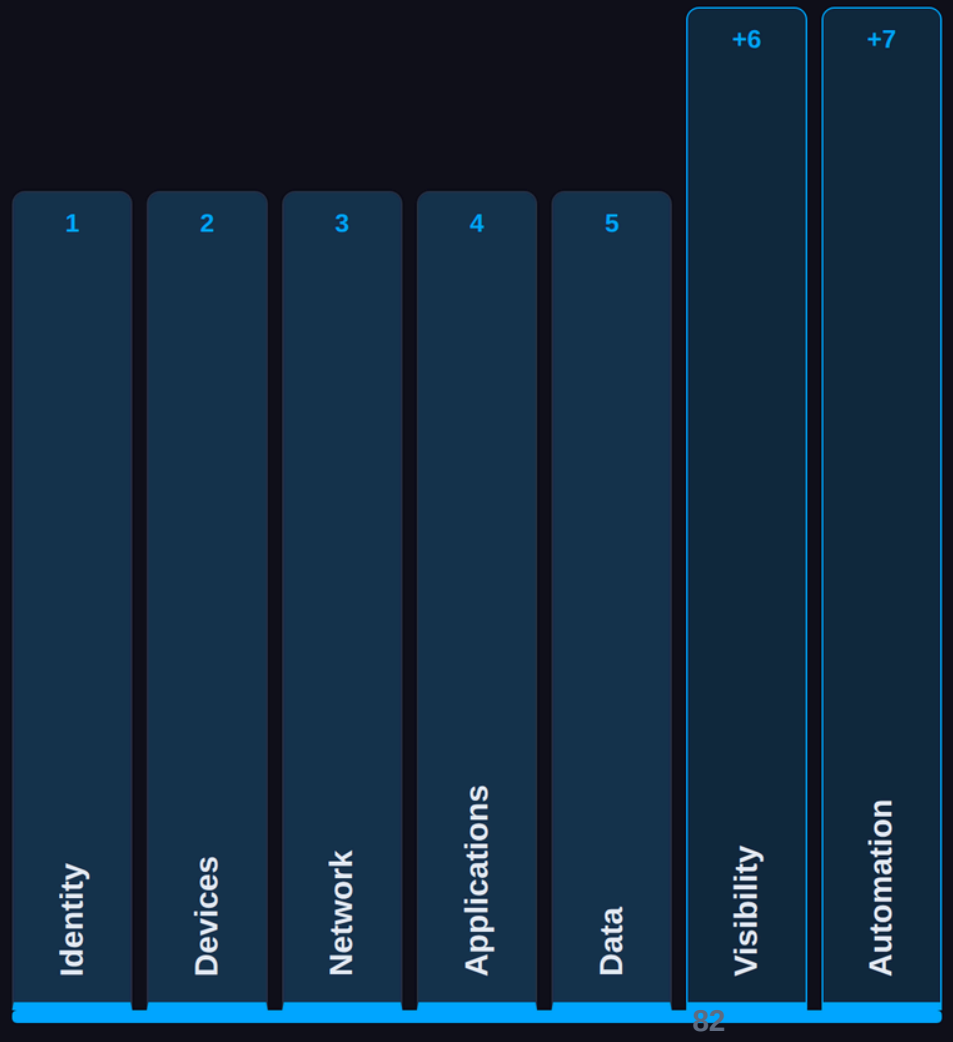
The 5 (+2) Pillars

Turn "cybersecurity" into seven concrete diagnostic questions.

Five pillars, plus two rooms for buildings

1 Identity | 2 Devices | 3 Network | 4 Applications | 5 Data | +6 Visibility | +7 Automation

- Each pillar = **one diagnostic question** you ask an owner
- **"You don't fix the firewall — you ask the right question."**



Each pillar = **one diagnostic question**.

Pillar 1 · Identity

The leader's question

"Who can command the building, and can you name them?"

The 80/20 move

MFA on remote access; kill shared logins; a named vendor list

> *Say it: "remote access is per-engineer, MFA and logged."*

Pillar 2 · Devices

The leader's question

"What % of controllers run software no one patches?"

The 80/20 move

asset register + firmware status; change default creds

> *Say it: "you get a live asset register on day one."*

Pillar 3 · Network

The leader's question

"How many hops from the lobby Wi-Fi to the fire panel?"

The 80/20 move

segment life-safety/BMS/tenant/guest; a monitored IT/OT gate

> *Say it: "your fire system lives on its own island."*

Pillar 4 · Applications

The leader's question

"Who is remotely connected right now?"

The 80/20 move

vendor access via a recorded jump host, time-limited, MFA

> *Say it: "request-based, recorded support — no standing back-door."*

Pillar 5 · Data

The leader's question

"Would you know if a setpoint or fire sequence changed by a fraction?"

The 80/20 move

config backups; setpoint/change alerting; baselines

> *Say it: "a quiet tamper won't stay quiet."*

Pillar 6 · Visibility

The leader's question

"Show me the asset inventory. When was it last updated?"

The 80/20 move

passive discovery; keep the register live through the contract

> *Say it: "you can't protect a building you can't see."*

Pillar 7 · Automation

The leader's question

"What acts on its own, and what waits for a human?"

The 80/20 move

AI/automation may advise; humans approve life-safety actions

> *Say it: "fast where it's safe, a person where it isn't."*

Pillars ↔ Purdue zones ↔ IEC 62443

- The seven pillars are a **sales-friendly repackaging** of the same ground
- 62443's foundational requirements cover identity, use control, integrity, confidentiality, data-flow, response, availability
- Showing the mapping earns credibility with a technical buyer

PILLAR	PURDUE	62443
Identity	all levels	ID & auth
Network	the conduits	zones/conduits
Devices	L0–L1	system integrity
Data	L1–L2	data confidentiality
Visibility	whole stack	timely response

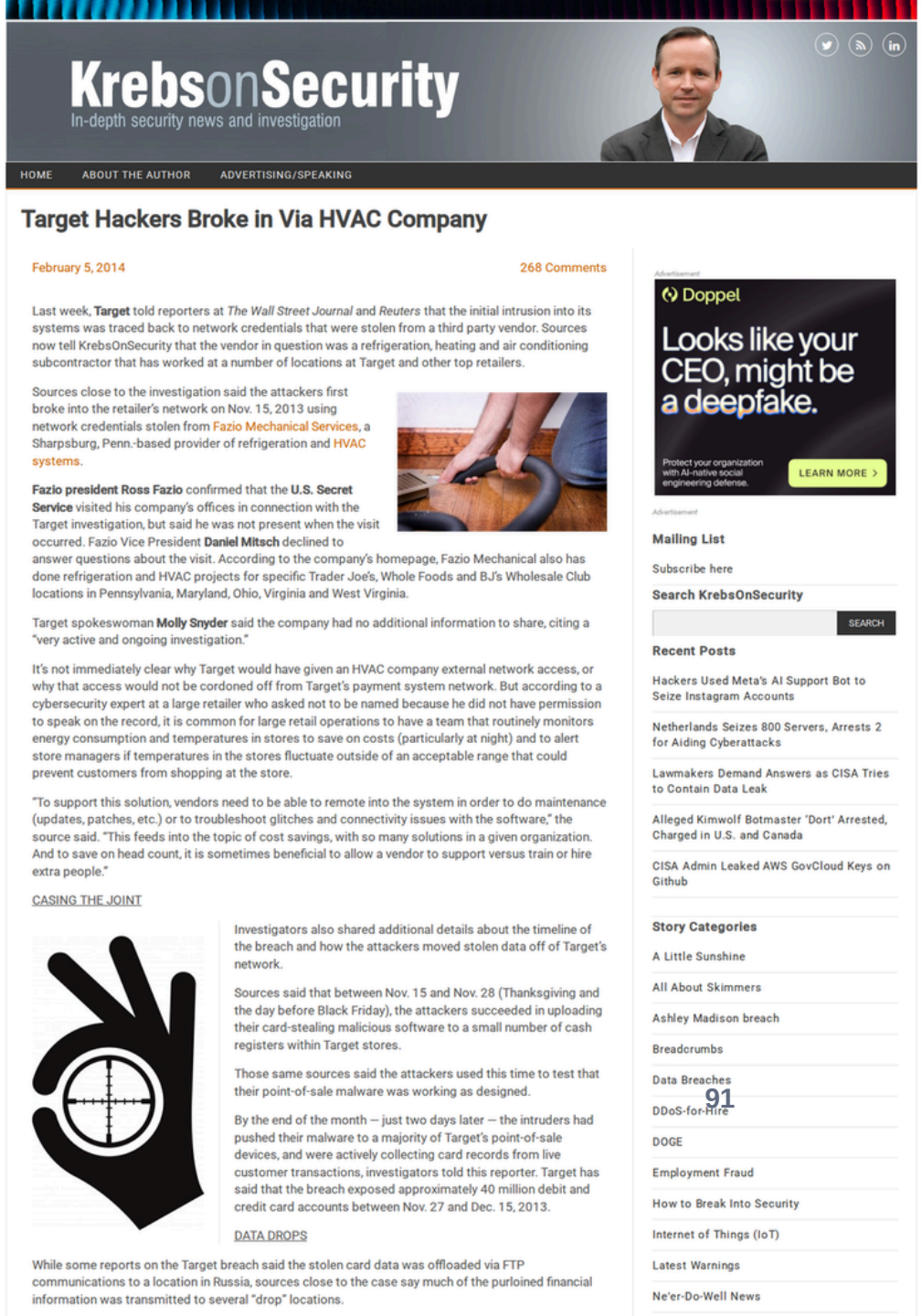
The Pillars **repackage** the same ground.

TARGET · 2013 · IDENTITY + NETWORK

source: krebsonsecurity.com →

The building-systems vendor was the front door

- **1** phish the HVAC vendor · **2** cross the boundary
- **3** pivot on a flat network · **4** exfiltrate — **~40M cards**
- **You are the vendor with the account.**



KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Target Hackers Broke in Via HVAC Company

February 5, 2014 268 Comments

Last week, **Target** told reporters at *The Wall Street Journal* and *Reuters* that the initial intrusion into its systems was traced back to network credentials that were stolen from a third party vendor. Sources now tell KrebsOnSecurity that the vendor in question was a refrigeration, heating and air conditioning subcontractor that has worked at a number of locations at Target and other top retailers.

Sources close to the investigation said the attackers first broke into the retailer's network on Nov. 15, 2013 using network credentials stolen from Fazio Mechanical Services, a Sharpsburg, Penn.-based provider of refrigeration and HVAC systems.

Fazio president Ross Fazio confirmed that the **U.S. Secret Service** visited his company's offices in connection with the Target investigation, but said he was not present when the visit occurred. Fazio Vice President **Daniel Mitsch** declined to answer questions about the visit. According to the company's homepage, Fazio Mechanical also has done refrigeration and HVAC projects for specific Trader Joe's, Whole Foods and BJ's Wholesale Club locations in Pennsylvania, Maryland, Ohio, Virginia and West Virginia.

Target spokeswoman **Molly Snyder** said the company had no additional information to share, citing a "very active and ongoing investigation."

It's not immediately clear why Target would have given an HVAC company external network access, or why that access would not be cordoned off from Target's payment system network. But according to a cybersecurity expert at a large retailer who asked not to be named because he did not have permission to speak on the record, it is common for large retail operations to have a team that routinely monitors energy consumption and temperatures in stores to save on costs (particularly at night) and to alert store managers if temperatures in the stores fluctuate outside of an acceptable range that could prevent customers from shopping at the store.

"To support this solution, vendors need to be able to remote into the system in order to do maintenance (updates, patches, etc.) or to troubleshoot glitches and connectivity issues with the software," the source said. "This feeds into the topic of cost savings, with so many solutions in a given organization. And to save on head count, it is sometimes beneficial to allow a vendor to support versus train or hire extra people."

CASING THE JOINT

Investigators also shared additional details about the timeline of the breach and how the attackers moved stolen data off of Target's network.

Sources said that between Nov. 15 and Nov. 28 (Thanksgiving and the day before Black Friday), the attackers succeeded in uploading their card-stealing malicious software to a small number of cash registers within Target stores.

Those same sources said the attackers used this time to test that their point-of-sale malware was working as designed.

By the end of the month — just two days later — the intruders had pushed their malware to a majority of Target's point-of-sale devices, and were actively collecting card records from live customer transactions, investigators told this reporter. Target has said that the breach exposed approximately 40 million debit and credit card accounts between Nov. 27 and Dec. 15, 2013.

DATA DROPS

While some reports on the Target breach said the stolen card data was offloaded via FTP communications to a location in Russia, sources close to the case say much of the purloined financial information was transmitted to several "drop" locations.

Advertisement

Doppel
Looks like your CEO, might be a deepfake.
Protect your organization with AI-native social engineering defense.
LEARN MORE ›

Advertisement

Mailing List

Subscribe here

Search KrebsOnSecurity

SEARCH

Recent Posts

Hackers Used Meta's AI Support Bot to Seize Instagram Accounts

Netherlands Seizes 800 Servers, Arrests 2 for Aiding Cyberattacks

Lawmakers Demand Answers as CISA Tries to Contain Data Leak

Alleged Kimwolf Botmaster 'Dort' Arrested, Charged in U.S. and Canada

CISA Admin Leaked AWS GovCloud Keys on Github

Story Categories

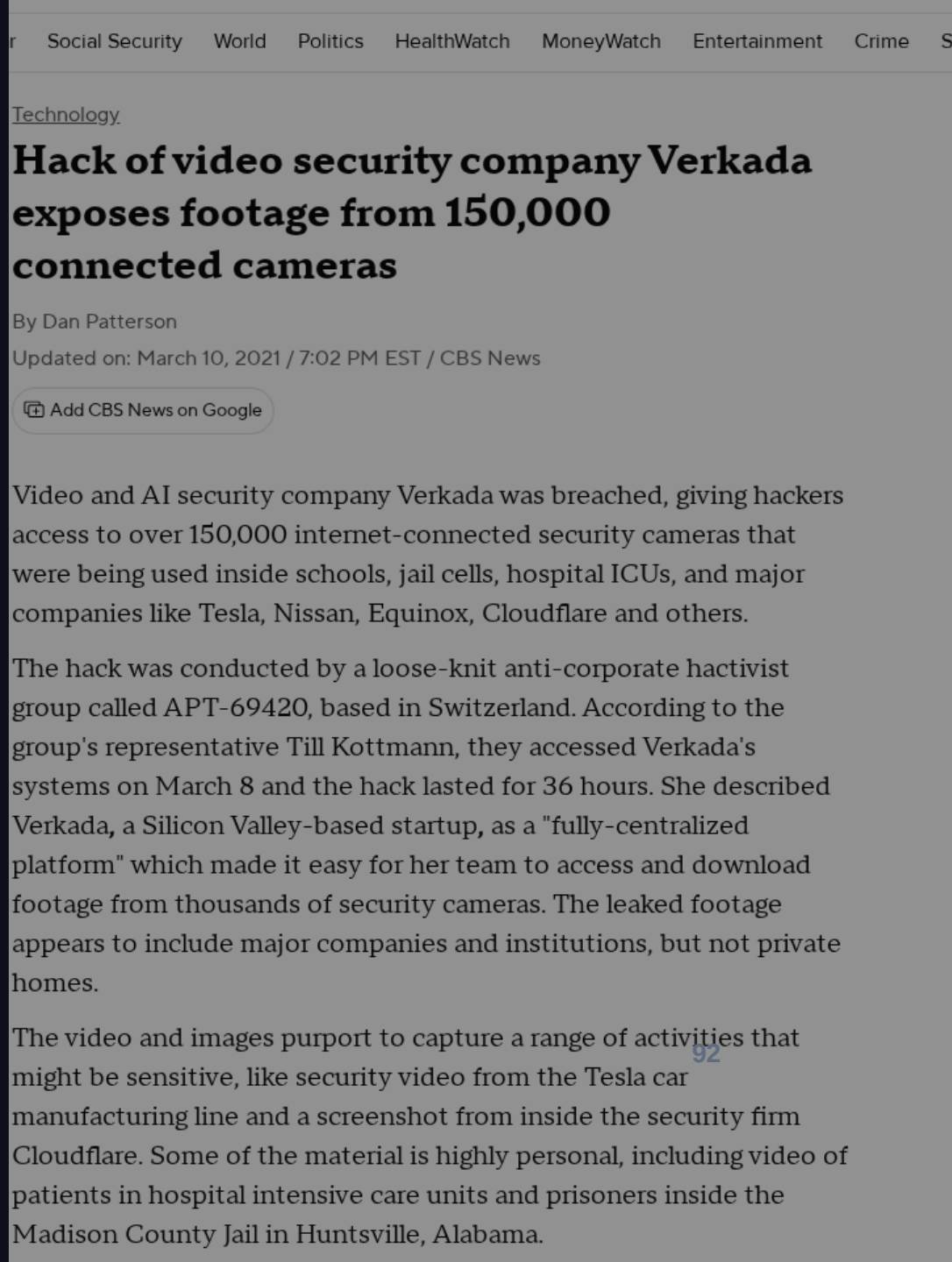
A Little Sunshine
All About Skimmers
Ashley Madison breach
Breadcrumbs
Data Breaches
DDoS-for-Hire
DOGE
Employment Fraud
How to Break Into Security
Internet of Things (IoT)
Latest Warnings
Ne'er-Do-Well News

VERKADA · 2021 · DEVICES + IDENTITY

source: cbsnews.com →

150,000 cameras from one credential

- One **exposed admin credential** → the camera vendor's cloud
- **~150,000 cameras**, incl. building access
- Building security systems **are** IT systems



r Social Security World Politics HealthWatch MoneyWatch Entertainment Crime S

Technology

Hack of video security company Verkada exposes footage from 150,000 connected cameras

By Dan Patterson

Updated on: March 10, 2021 / 7:02 PM EST / CBS News

Add CBS News on Google

Video and AI security company Verkada was breached, giving hackers access to over 150,000 internet-connected security cameras that were being used inside schools, jail cells, hospital ICUs, and major companies like Tesla, Nissan, Equinox, Cloudflare and others.

The hack was conducted by a loose-knit anti-corporate hactivist group called APT-69420, based in Switzerland. According to the group's representative Till Kottmann, they accessed Verkada's systems on March 8 and the hack lasted for 36 hours. She described Verkada, a Silicon Valley-based startup, as a "fully-centralized platform" which made it easy for her team to access and download footage from thousands of security cameras. The leaked footage appears to include major companies and institutions, but not private homes.

The video and images purport to capture a range of activities that might be sensitive, like security video from the Tesla car manufacturing line and a screenshot from inside the security firm Cloudflare. Some of the material is highly personal, including video of patients in hospital intensive care units and prisoners inside the Madison County Jail in Huntsville, Alabama.

OLDSMAR WATER · 2021 · APPLICATIONS

source: cbsnews.com →

A hand on the controls via remote access

- Exposed **TeamViewer** → the plant's HMI
- Attacker moved a chemical setpoint **111×**
- Unwatched remote access = a hand on the process

CBS Evening News

Feds tracking down hacker who tried to poison Florida town's water supply

By Jeff Pegues

February 9, 2021 / 7:02 AM EST / CBS News

Add CBS News on Google

A shocking case of computer hacking has been uncovered in Pinellas County, Florida. Federal investigators are trying to hunt down the person who tried to poison a public water supply – remotely.

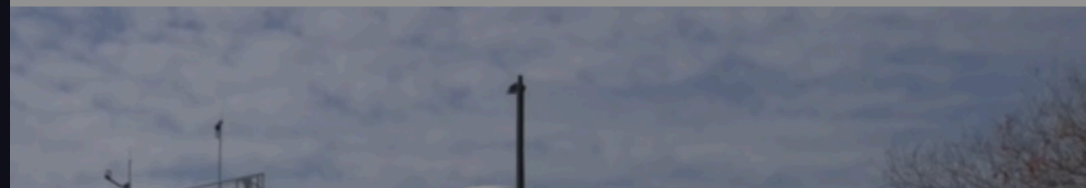
Investigators say a plant operator monitoring the water plant in the Tampa Bay city of Oldsmar noticed breaches starting Friday morning.

The hacker was controlling the computer system's mouse – opening various functions on the screen and changing the sodium hydroxide in the water supply from about 100 parts per million to more than 11,100 parts per million.

"This is obviously a significant and potentially dangerous increase," Pinellas County Sheriff Bob Gualtieri said. "Sodium hydroxide, also known as lye, is the main ingredient in liquid drain cleaners."

If ingested in large amounts, sodium hydroxide can cause vomiting, chest and abdominal pain, according to the Centers for Disease Control.

93



FROSTYGOOP · 2024 · DATA + NETWORK

source: dragos.com →

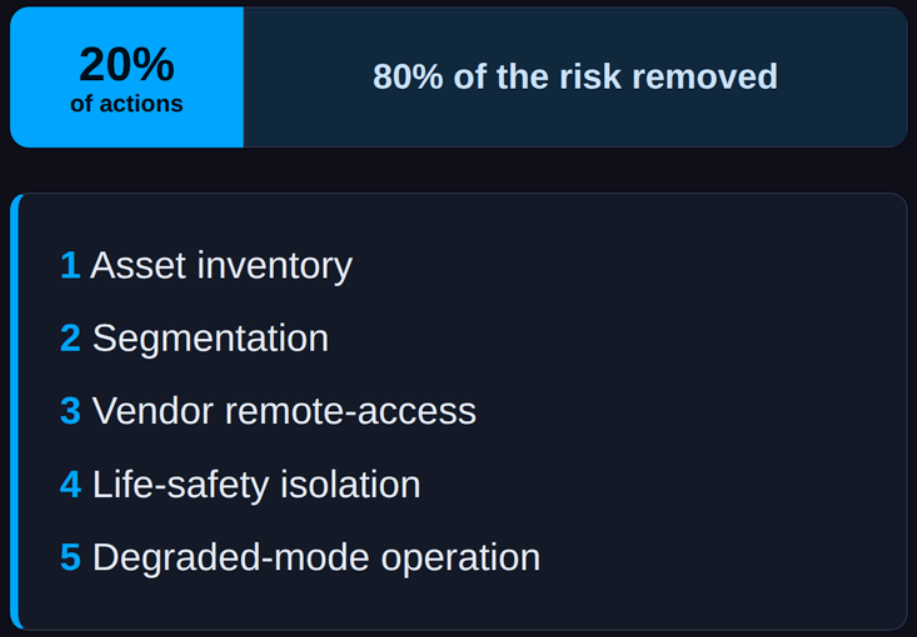
No exploit — it just spoke the protocol

- **Modbus TCP** commands straight to heating controllers
- **600+ apartments** lost heat, sub-zero, two days
- The only defence is the boundary

The 80/20 — the vital few

- **1** asset inventory · **2** IT/OT + life-safety segmentation
- **3** vendor remote-access control · **4** fire/life-safety isolation
- **5** manual / degraded-mode operation

> **Lead with these five, not a wish-list.**



Lead with the **vital few**, not a wish-list.

ACTIVITY · W4 · PILLAR TENDER SORTER

Sort the real Section 42

- 42.5 → Identity · 42.7 → Network · 42.9 → Devices · 42.10 → Data · 42.14 → Visibility
- Justify each — on a real tender, not a synthetic one

Web: **Pillar Tender Sorter** — the spine of tomorrow's lab.

You can read the building, spot a governed client, translate the jargon, and sort a real spec.

Day 2 → AI does the heavy lifting, safely — then you pitch.