Octave

When Systems Fail

Resilience by Design: Leading Through Risk in an Intelligent, Interconnected World

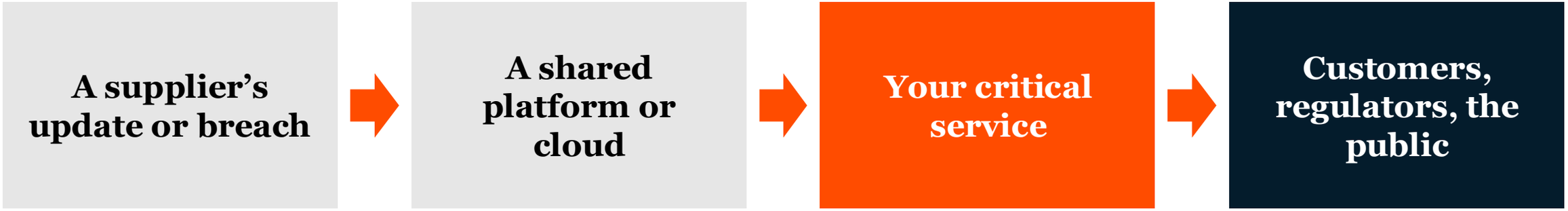
Presenter: Niel Harper

Technology • Cybersecurity • Leadership • Organisational resilience



"I'm no expert, but I think it's some kind of cyber attack!"

A failure rarely stays where it starts



Quiet. Trusted. Unreviewed.

One fault, many tenants

Your name is on it now

Trust is lost in hours

Resilience is designed before the failure, not discovered during it.

Five lenses on resilience

Critical infrastructure	Where a technical failure becomes public harm
Cybersecurity leadership	Decisions and decision rights, not just defences
AI governance	New capability, new exposure, new accountability
Regulation	Obligations are converging on resilience
Organisational resilience	Designing the whole organisation to recover

The threat has changed shape

Apr 2026

Joint US advisory: Iranian-affiliated actors exploiting PLCs across water, energy and local government

CISA, FBI, NSA et al.

80–90%

Share of intrusion tasks reportedly run by AI in a state-sponsored campaign against ~30 organisations

Anthropic disclosure, Nov 2025

May 2026

Poland's ABW warns attacks are shifting from data theft toward physical disruption

Polish ABW

Entry is often basic: exposed systems, default passwords, thin defences at smaller operators.

Critical infrastructure is a web of risk

Energy

Powers every other sector; exposed OT

Telecoms

Carries every sector’s traffic

Water

Small utilities, thin defences

Financial services

Cloud, cards, third-party concentration

Ports and shipping

Trade chokepoints; exposed OT

Health

Life-safety systems, supplier chains

What recent failures have taught us

Incident	What happened	Leadership lesson
Colonial Pipeline (2021)	Ransomware hit business IT; operations were halted as a precaution	IT/OT coupling sets your blast radius
CrowdStrike update (Jul 2024)	One faulty update crashed ~8.5M Windows devices	A trusted supplier is a single point of failure
Change Healthcare (2024)	Ransomware disrupted claims processing across US health	Concentration risk becomes systemic risk
Stryker wiper attack (Mar 2026)	Destructive attack wiped systems; offices stopped (Iran-aligned group)	Plan for destruction, not just theft

19 JULY 2024 · CROWDSTRIKE OUTAGE

One faulty update.
8.5 million machines down.

Airlines, banks, hospitals and broadcasters stopped in a single morning. The cause was a trusted security supplier, not an attacker.

Source: Microsoft, 20 July 2024

Resilience by design: four goals



Anticipate

Know your critical services, threats and dependencies



Withstand

Keep delivering under attack: segment, diversify, degrade gracefully



Recover

Restore minimum service fast: tested backups, runbooks, manual modes



Adapt

Learn and change after every incident and exercise

From defending systems to owning risk

From: security as technology

- Reports on tools and alerts
- Measures vulnerabilities closed
- Engaged after the system is built
- Escalates when something breaks



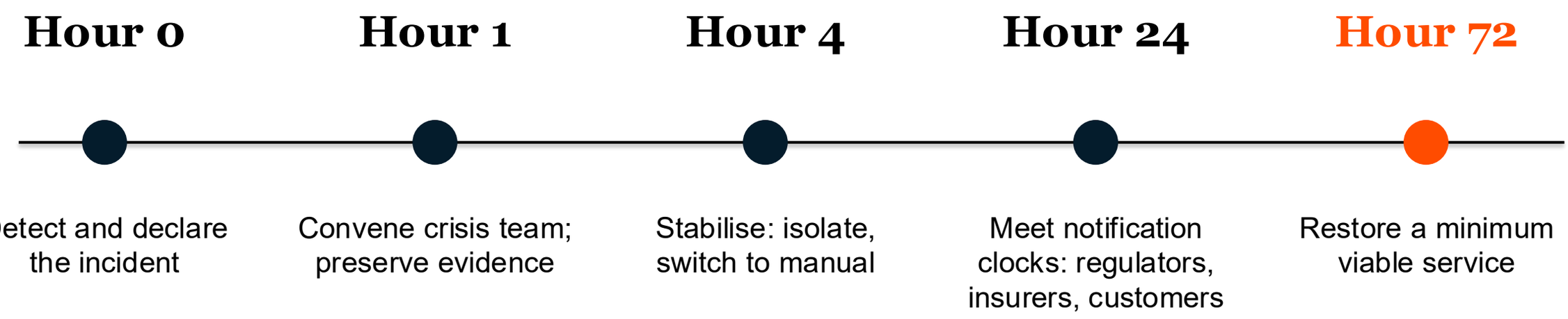
To: security as business risk

- Reports on business impact and risk appetite
- Measures time to recover critical services
- Designs in from the first conversation
- Rehearses decisions before the crisis

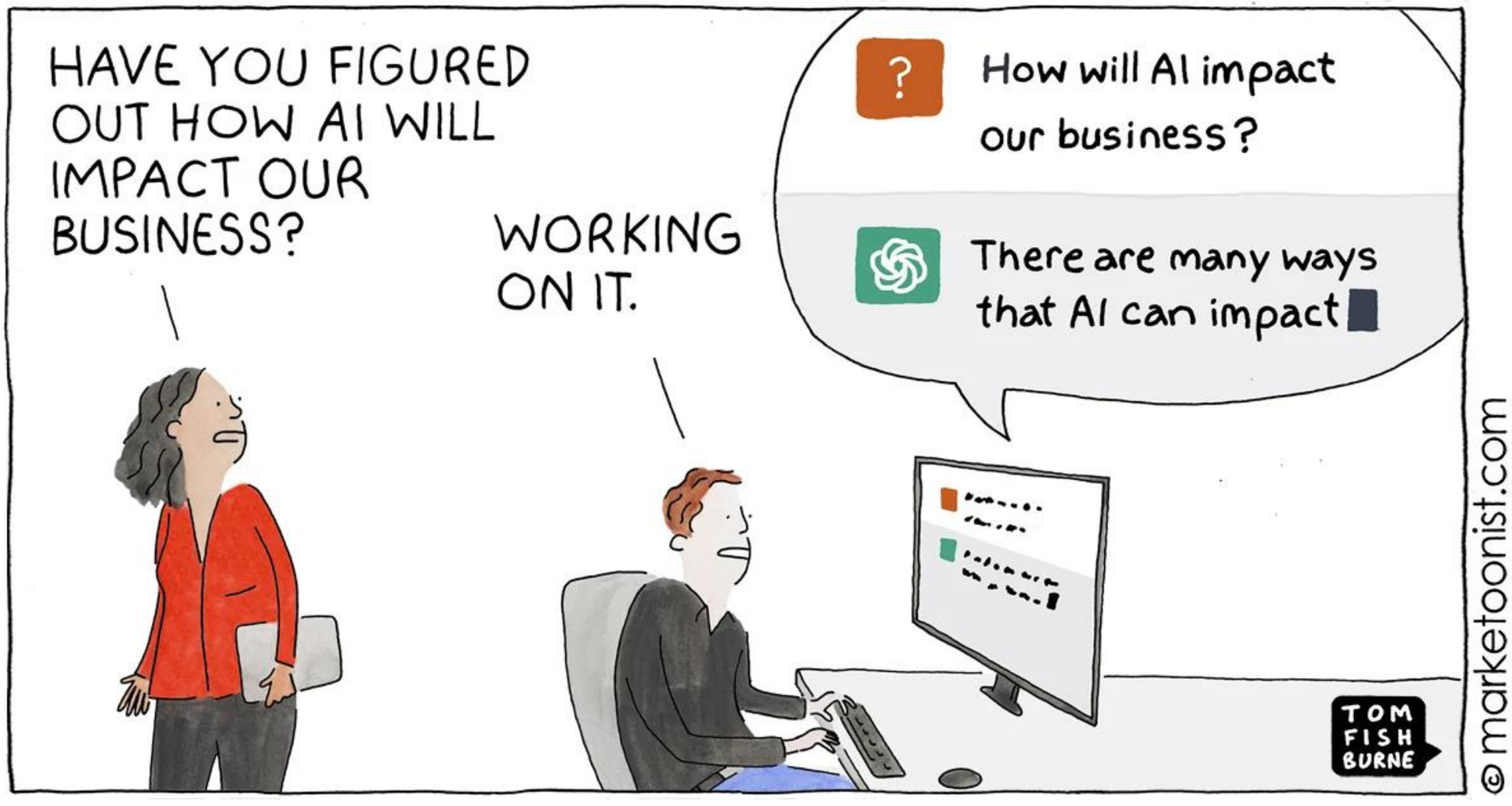
Five questions every board should ask

1. Which services can we not afford to lose, and for how long?
2. What do we depend on that we do not control?
3. Have we practised recovery, and what broke when we did?
4. In hour one, who decides, who speaks, and who can shut things down?
5. Where is AI already in use, and who owns that risk?

Leading through the first 72 hours



Agree decision rights, communications, and restoration priorities before the incident.


HAVE YOU FIGURED OUT HOW AI WILL IMPACT OUR BUSINESS?
WORKING ON IT.
How will AI impact our business?
There are many ways that AI can impact
TOM FISH BURNE
© marketoonist.com

AI cuts both ways



In the attacker's hands

- Faster reconnaissance and phishing at scale
- Automated intrusion steps
- Lower skill needed to probe OT systems



Inside your enterprise

- Shadow AI and data leakage
- Agents with real permissions; prompt injection
- Over-trust in wrong answers; model concentration

The question for both: what can this system do, and what happens when it is wrong?

AI governance that works in practice

Anchored in NIST AI RMF (Govern, Map, Measure, Manage) and ISO/IEC 42001.

1 Inventory

Every model, agent and AI feature, including shadow AI

2 Classify

By impact: who is affected if it is wrong?

3 Own

A named executive owner for each use

4 Test

Red-team for misuse, injection and drift

5 Monitor

Log, review, and set human override points

6 Retire

Decommission models and data on schedule



"I need someone who is comfortable in the regulatory jungle."

Regulation is converging on resilience

Regime	What it demands	Where it stands
EU AI Act	Risk-based duties for AI systems; documentation, oversight, monitoring	High-risk dates delayed: 2 Dec 2027 (Annex III), 2 Aug 2028 (Annex I)
NIS2 (EU)	Risk management, supply-chain security, incident reporting	In force; applied through national law
DORA (EU finance)	ICT risk, resilience testing, third-party oversight	Applying since January 2025
SEC rules (US)	Disclose material cyber incidents within four business days	In effect since December 2023

EU AI Act dates reflect the 2026 Digital Omnibus agreement and Parliament vote (16 Jun 2026), pending final adoption.

Home ground: Trinidad and Tobago

What is in place

- Computer Misuse Act 2000
- Data Protection Act 2011, partly in force
- TT-CSIRT national response team
- TATT telecom cybersecurity framework (Jan 2026)

What is still open

- Information Commissioner not yet established
- No national cyber agency established in law
- Cybercrime Bill, first tabled in 2014, still not enacted

A legal gap is not a risk gap: partners and insurers apply global standards anyway.

Know your minimum viable company

Tomorrow you can keep only four things running. Which four?



Map critical services and name an owner



Trace dependencies: suppliers, cloud, people



Define manual fallbacks and impact tolerances



Prove it with exercises, not documents

Measure what matters

Leading: how prepared are we?

- Critical services with tested recovery
- Critical suppliers assessed, with exit plans
- Executive exercises held each year
- AI systems inventoried and owned

Lagging: how did we perform?

- Time to detect
- Time to restore, against target
- Customer-visible downtime
- Notifications met on time

Your first 90 days

Days 1–30: See

- Name critical services and owners
- Inventory AI use and key suppliers
- Confirm incident decision rights

Days 31–60: Prove

- Tabletop a supplier failure with executives
- Restore one critical service end to end
- Log and close the gaps

Days 61–90: Embed

- Report resilience metrics to the board
- Build requirements into procurement and AI approvals
- Schedule the next exercise cycle

Resilience is a leadership decision

- Design for failure before it happens
- Govern what you depend on: suppliers, platforms, AI
- Practise until recovery is routine

Questions and discussion