

From Power to Supply Chains: Sustainability Is Security

Why resilience starts before the firewall

Codemash, 16 January 2026

Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

Set the frame: this is a security talk, not a sustainability sermon.



Matt "Kelly" Williams

I ask inconvenient questions about software, power, and how resilient systems really are.

Founder, Sustainable IT Manifesto Foundation • Founder, Making Software Greener • Green Computing Foundation advisory board member

kelly@makingsoftwaregreener.com |
LinkedIn: [@mattkwilliams](#)

Sustainable IT Manifesto Foundation



SustainableITManifesto.org

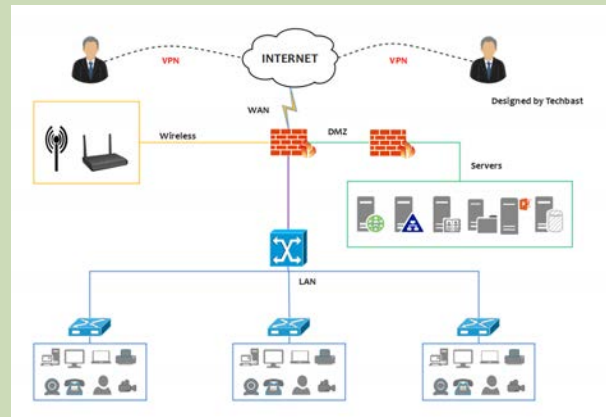
(also I give silent talks about confidence and leaving variables intentionally undefined)

Cybersecurity is about ensuring systems remain reliable and trustworthy, not just when things go right, but when they go wrong.

Sustainability is the practice of designing and operating systems so they remain secure, reliable, and supportable over time—without creating hidden dependencies, fragile supply chains, or risks that only appear under stress.

From a security perspective, sustainability means reducing long-term exposure by building systems that can be powered, maintained, updated, and trusted even as conditions change.

Security doesn't start at the firewall



Speaker focus:

Security assumptions depend on power, hardware, and logistics working.

If a system only works when everything goes right,
it isn't secure.

Resilience by design means planning for power
loss, supply shocks, human error, and change—
before they become incidents.

Hidden Assumptions

What we assume will always be there

- Power
- Hardware
- Bandwidth
- Vendors
- Time

Speaker focus:

Security models quietly assume stability.

**Failures don't
arrive one at a time**



Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

Cascading failures = security incidents.

Power Is a Security Dependency

Power = Availability + Integrity



Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Energy resilience is security resilience

Speaker focus:

Power loss isn't just downtime—it's risk.

Energy-Hungry Systems Fail Harder

Efficiency reduces blast radius

Speaker focus:

High draw → heat → throttling → failure → rushed fixes.

Climate as a Threat Multiplier

Weather now affects threat
models



Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

**This is already happening,
not hypothetical.**

Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Colorado - winds -> fires

Cost Pressure Is a Security Pressure

Rising energy costs change behavior

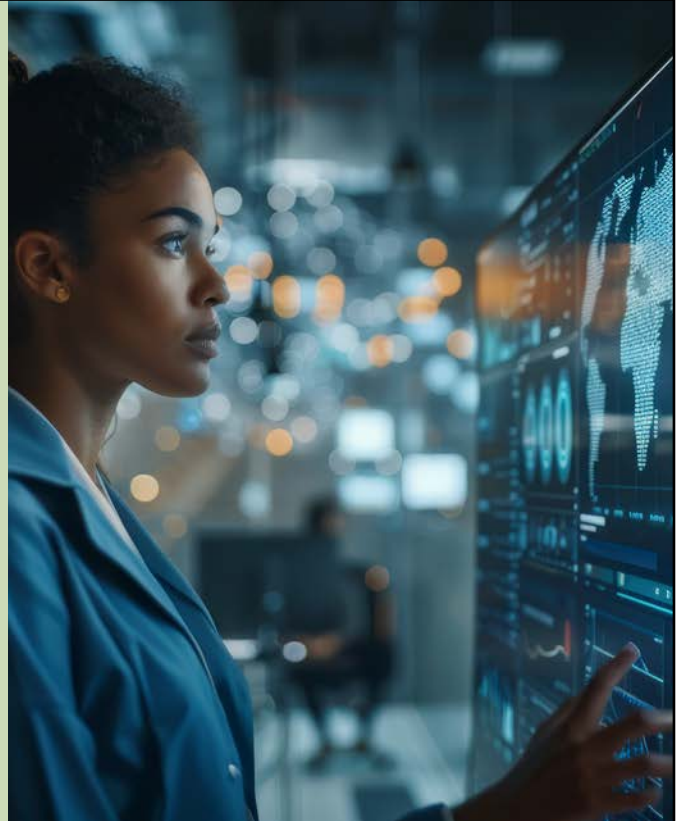
Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

Deferred upgrades, disabled controls, risky optimizations.

**Efficient systems
fail more gracefully**



Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

This will echo throughout the talk.

Software Efficiency as Defense

Waste Is a Vulnerability

Inefficiency expands attack surface



Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

More code, more services, more risk.

Scaling Hides Problems

Scaling Hides Problems **(Until it suddenly can't)**

Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

Cloud masks inefficiency—until budgets or limits hit.

With Great Power Comes Great Power Bills

-- Tom Smith, *The Last Hero on Earth*

Least Privilege

(Applied to Compute)

**Do less.
Run less.
Store less.**

Speaker focus:

Security principle, sustainability outcome.

**Performance, cost, and
carbon are the *same* problem**

Speaker focus:

This is the unifying insight.

Software as Control Surface

Code choices shape resilience

Sustainable IT Manifesto Foundation

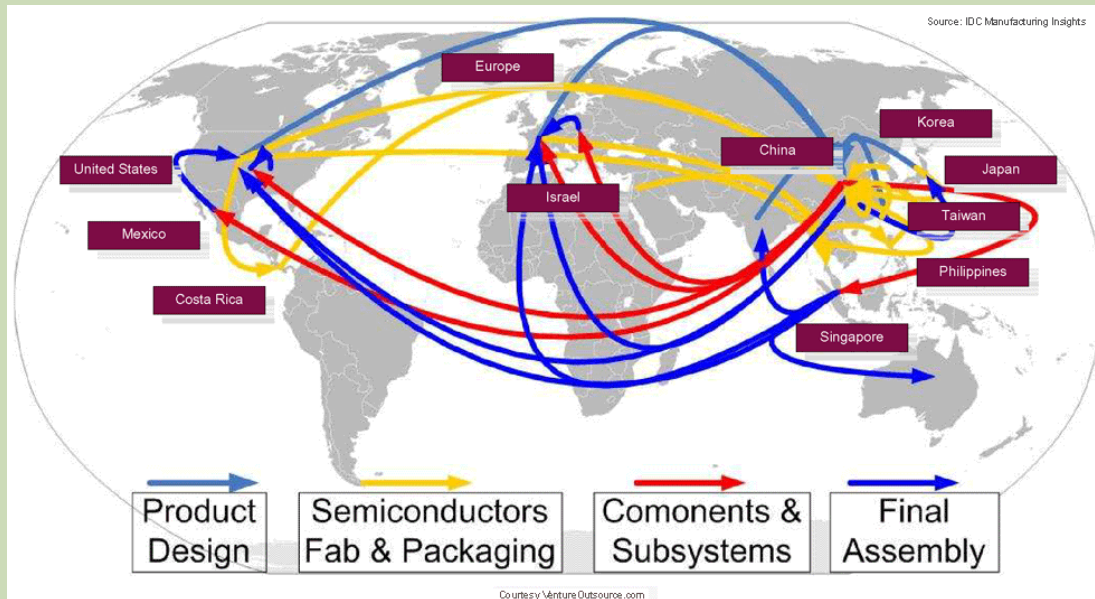
SustainableITManifesto.org

Speaker focus:

Architecture *is* policy.

Hardware & Supply Chains

Your Threat Model Is Bigger Than You Think



(It extends beyond your org chart)

Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

Vendors, sourcing, logistics all matter.

**Hardware Lifecycle
= Security Lifecycle**

**End-of-life devices don't stop
being dangerous**

Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

Unpatched firmware, shadow assets, forgotten gear.

Emergency Procurement Breaks Controls

Shortages force bad security decisions

Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

When the only option is “whatever we can get.”

“If you don’t know where your hardware came from, you don’t know who touched your security.”

Speaker focus:

Let it land.

Sustainability as Risk Reduction

This Isn't About Virtue

It's about exposure

Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

Speak to security leaders' language.

Converging Forces

Security teams are getting pulled into ESG

- Risk management
- Compliance
- Insurance
- Customer expectations

Speaker focus:

Whether they like it or not.

Sustainability Signals Maturity

Stable systems attract trust

Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

Auditors, insurers, customers notice.

Something You Can Do Tomorrow

No-New-Budget Improvements

Small changes, compounding impact

Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

This lowers resistance.

Four Lenses

Where to start

1. Power & infrastructure
2. Software efficiency
3. Hardware lifecycle planning
4. Culture & process integration

Speaker focus:

You don't have to do everything.

Start Where You Hurt

- Outages
- Incidents
- Near-misses

Speaker focus:

Retrospectives are gold mines.

“The easiest fixes are often the ones that make the biggest difference—because no one wanted to touch them.”

A Pattern You've Probably Noticed

Aware	What assumptions does this system depend on?
Conscious	What tradeoffs are we making—intentionally or not?
Enabled	Do our tools and processes support better choices?
Empowered	Can teams act before risk becomes an incident?

Say something like:

“I’m not proposing a new framework.

This is just a pattern I see in mature security organizations.

They don’t do everything at once — they get better at *seeing*, then *choosing*, then *enabling*, then *acting*.”

(This slide intentionally left blank)

Security isn't about building walls....

**It's about building systems that
keep working when the walls crack.**

Sustainable IT Manifesto Foundation

SustainableITManifesto.org

Speaker focus:

Bring it back to resilience.

Resilience is what organizations develop after enough things go wrong to start paying attention.

Q&A

When has sustainability already affected your security?

Sub-prompts (if needed):

An outage that changed behavior

A supply issue that forced risk

A cost decision that weakened controls

Speaker focus:

Invite stories, not hypotheticals.

**Security isn't just about stopping
bad things from happening.
It's about building systems
that keep working when
the world gets weird.**