PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING

2025
EUROPE
COMMUNITY
MEETING

Compliance as a Consequence:

Unlocking PCI to Empower Your Business

PCI Security Standards Council®

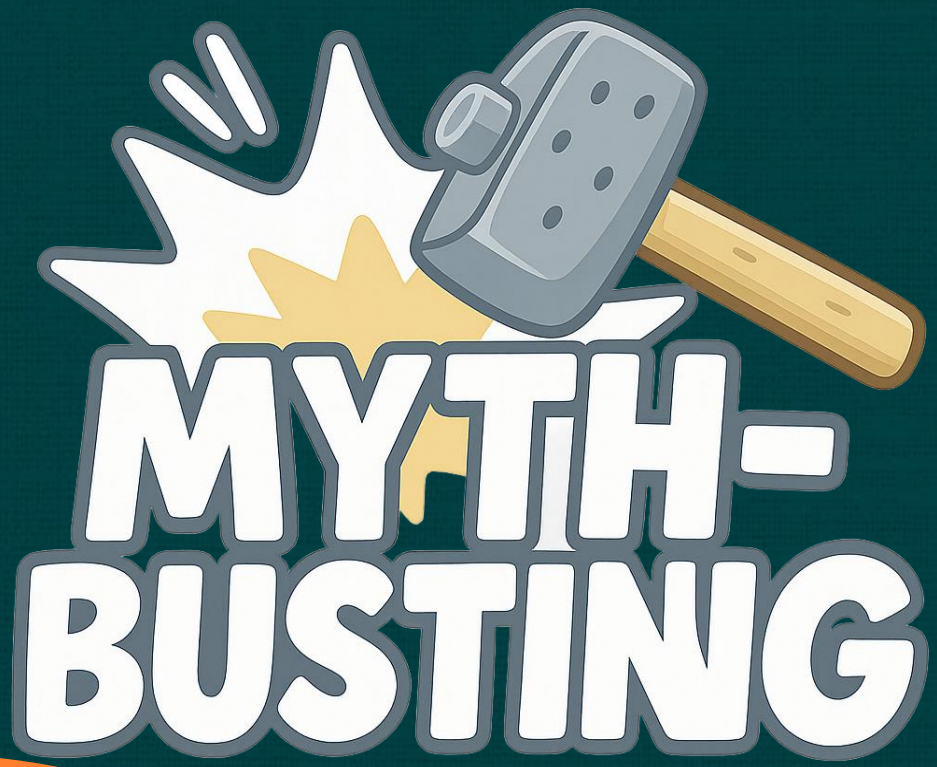
Joanna Katherine Vane

Information Security Director
Checkout.com

Simon Turner

CISSP, CISM, CISA, VPC, PCI ISA
Head of Governance & Compliance
British Telecommunications (BT Group)

PCI Security Standards Council



Myth-Busting: The Dangers of Checkbox Compliance

❑ Common Misconceptions:

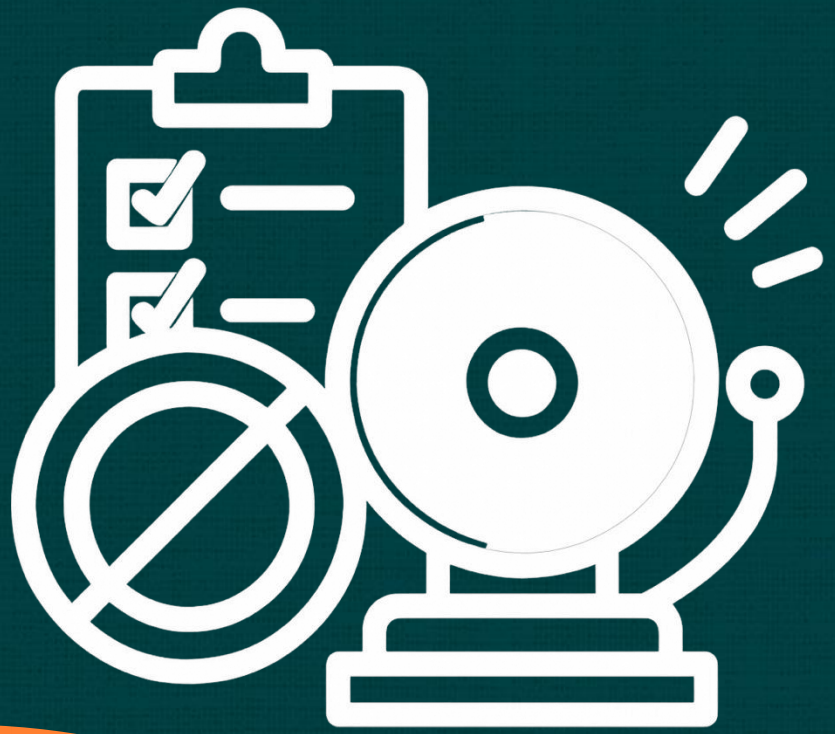
- 'If we're compliant, we're protected.'
- 'Passing audits means we're secure.'

❑ Cost of Failure:

- Fintech A: Passed audit, breached 3 months later.
- Fintech B: Data leak due to overlooked internal process.

True security requires depth, not just compliance.

PCI Security Standards Council



Compliance ≠ Security

"We live in a world where compliance is mandatory, but compliance alone won't keep us safe."

- Cybercrime is projected to cost the world $12.2 trillion annually by 2031.
- Compliance is baseline, not a safeguard.
- **Risk:** *Viewing InfoSec as a checkbox leaves blind spots.*

PCI Security Standards Council

InfoSec as Excellence

- **Define InfoSec Excellence:**
  - Proactive, integrated, cultural.
- **Why It Matters:**
  - Trust
  - Resilience
  - Competitive Advantage
- **Elevate the Bar:**
  - From necessary evil to strategic enabler.

PCI Security Standards Council

Core Principles of InfoSec Excellence

- ❑ Culture-First Mindset: Leadership sets the tone.
- ❑ Employee Empowerment: Awareness, responsibility, and vigilance.
- ❑ Continuous Adaptation: Risk landscapes evolve—so must we.

PCI Security Standards Council

Build InfoSec in Your Company's DNA

- ❑ **Layered Defense:**
  - Network, endpoint, identity, data, user behavior.
- ❑ **Key Programs:**
  - Security awareness training
  - Incident response readiness
  - Threat monitoring and hunting
- ❑ **Empowered Teams:**
  - Cross-functional collaboration
  - Shared accountability

PCI Security Standards Council

Leadership’s Role in InfoSec Excellence

- ❑ **Ripple Effect**: Culture cascades from the top.
- ❑ **Invest in Talent**: Hire, nurture, retain top security professionals.
- ❑ **Accountability:**
  - KPIs: Phishing click rates, patching timelines, time to detect/respond.

PCI Security Standards Council

Case Study: From Compliance to Culture

- Initial State: Audit-driven, low awareness.
- Transformation:
  - Security built into onboarding
  - Quarterly training gamified
  - Transparent metrics reported to leadership
- Outcomes:
  - 40% reduction in incidents
  - 2x faster response times
  - 95% employee engagement in security programs

PCI Security Standards Council

The Psychology of Security Behavior

- Understanding Motivation: Fear-based training vs. purpose-driven engagement.
- Triggering Ownership: How we aligned security with personal accountability.

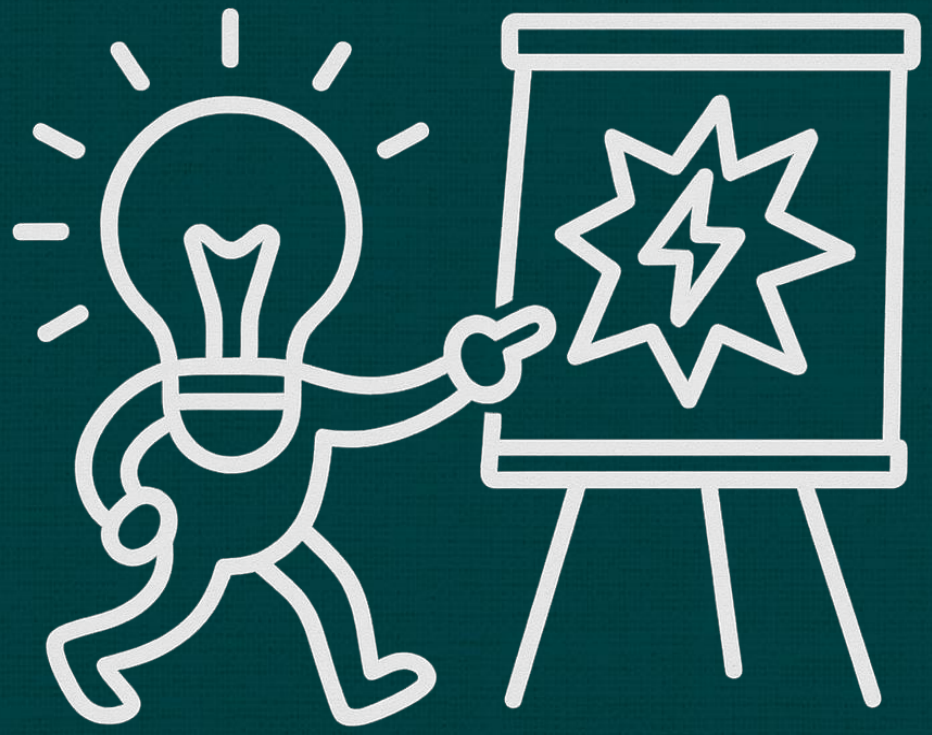
Balancing Speed and Security in Product Delivery

- **Myth:** Security slows you down.
- **Reality:** Integrated security accelerates delivery.
- **Practice:** Secure SDLC, threat modeling sprints, security in PR reviews.

Cross-Functional Collaboration Wins

- ❑ **Bridging Gaps:** Embedded security roles in engineering and product.
- ❑ **Co-ownership of Risk:** Security metrics in team dashboards.
- ❑ **Examples:** Co-led incident simulations, joint backlog prioritization.

Lessons from Incidents



- ❑ **Learning Culture:** From blame to blameless postmortems.
- ❑ **Visibility:** Sharing near misses as learning moments.
- ❑ **Change:** Incident response drills, public RCA reviews.

Metrics That Matter

- **Shift:** From check-the-box stats to behavior-driven metrics.
- **Sample KPIs:**
  - Time-to-detect and time-to-contain incidents
  - Phishing simulation reporting rate
  - Patch velocity across environments

Securing AI and Emerging Tech

- **Emerging Risks:** AI hallucinations, prompt injection, model theft.
- **Approach:** Guardrails for development, shadow AI scanning, AI governance council.

PCI Security Standards Council

Training That Sticks

- **Fail Fast, Learn Fast:** From theoretical to experiential learning.
- **Tools:** Gamified phishing campaigns, red team “capture the flag” days.

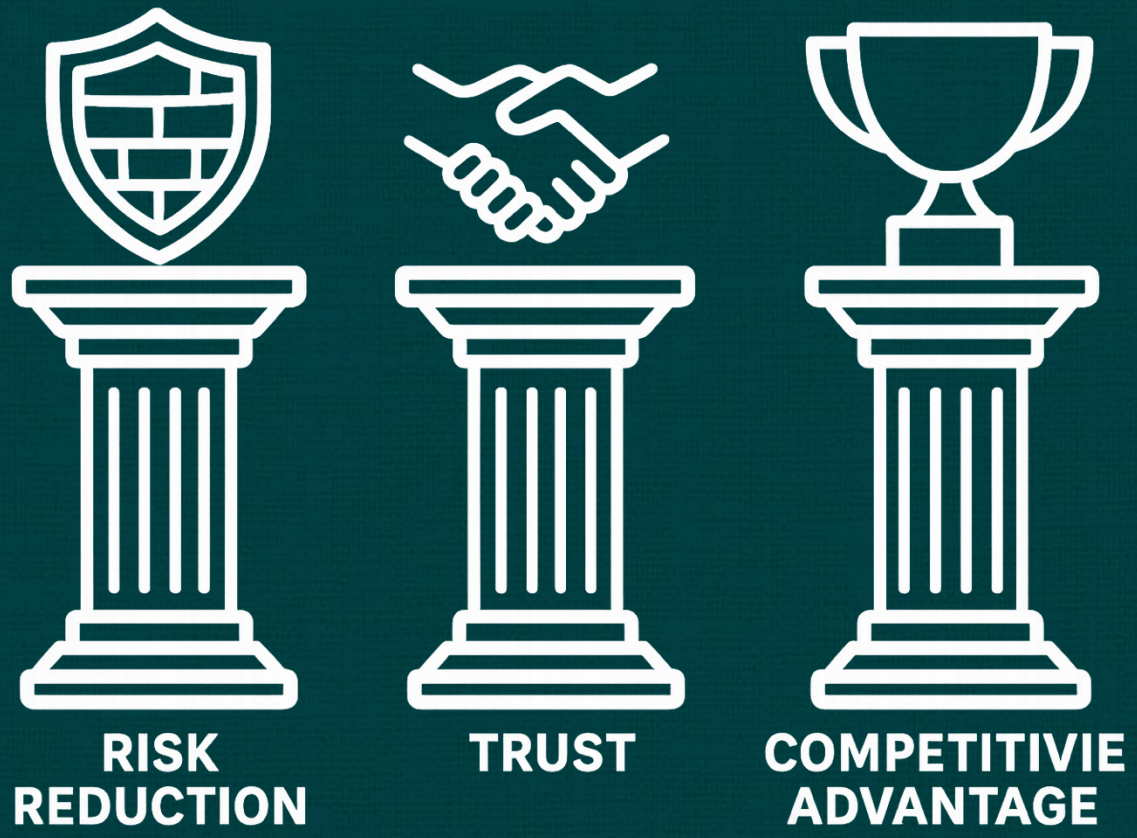
Sustaining The Momentum

- **Beyond the Audit:** Maintaining energy year-round.
- **Practices:** Quarterly themes (e.g., “Spring Clean Your Access”), recognition programs

PCI Security Standards Council

Benefits Beyond Compliance

- Risk Mitigation:
  - Predictive threat modeling
  - Faster containment
- Brand Trust:
  - Market differentiation
  - Regulatory goodwill
- Competitive Edge:
  - Preferred partner status
  - Leadership in security innovation



Final Thoughts

- Conclusion: "Compliance is the floor, not the ceiling. Our goal is excellence."

- Call to Action:
  - Rethink InfoSec as an enabler
  - Foster continuous improvement

- What's next: Let's share, challenge, and learn from each other.

PCI Security Standards Council