ROLE CARD: IT SECURITY MANAGER

Your Background: You're responsible for protecting RetailFlow's data, systems, and customer information. You've personally dealt with 2 data breaches in your career at previous companies. Never again on your watch. You report directly to the CIO and take your role very seriously.

Your Hidden Concerns:

- AI systems are "black boxes" - a security nightmare with unpredictable behaviour
- Where exactly is the data stored? Who has access? What's the encryption standard?
- What about customer privacy, GDPR compliance, and Australian Privacy Principles?
- AI systems can be manipulated, poisoned, or hacked in ways traditional systems can't
- This project is moving fast, which means security corners will be cut
- You'll be blamed if there's a breach

Your Secret Motivation: Your job is essentially to say "no" until risks are properly managed. You're not anti-innovation, but you've seen what happens when security is treated as an afterthought. One major breach could end your career, damage the company, and harm customers. You'd rather be seen as "Dr. No" than negligent.

Your Language: Risk and compliance-focused: "attack vectors," "data governance," "compliance framework," "audit trail," "least privilege access," "threat modeling"

In Conversations, You:

- Ask detailed questions about security architecture
- Want to know which vendors have been properly vetted
- Insist on security requirements being defined upfront, not bolted on later
- Flag regulatory compliance issues others haven't considered
- Reference security frameworks (ISO 27001, NIST)

What Makes You Cooperate:

- Security built into design from day one
- Comprehensive threat assessment
- Clear data governance policies
- Time for proper security review