Cyber East

Welcome to Cambridge

Proudly sponsored by Cambridge Cyber Advisors

Welcome to Cyber East

Cyber East is an industry body that works alongside the UK Government to develop the cyber security industry in the UK.

Our aim is to partner with cyber security businesses in the East of England and provide a platform for collaboration and growth within the Cyber Security industry.

Antony Gouldstone

Director

Agenda

1545-1600 – Registration
1600-1615 - Open & Welcome, Antony Gouldstone,
1615-1645 - Speaker #1 – Daniel Versace
1645-1715 - Speaker #2 – Tony Smith
1715-1745 - Speaker #3 – iuliana Silvason
1745-1800 - Q&A Panel with all speaker
1800-1810 – Prize Draw & Closing Thoughts
1810-1900 – Networking & Pizza

Daniel Versace

Senior Security Architect
BBC

SECURITY ARCHITECTURE

Daniel J Versace PGDip Cyber (Open), CISSP, CCSP, MCIIS

Daniel J Versace PGDip Cyber(Open)

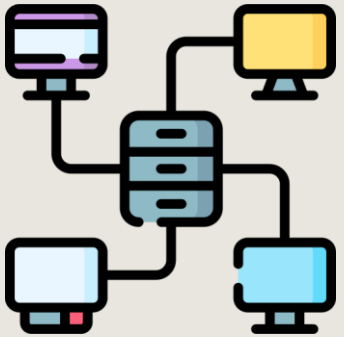
- Security+
- Network+
- ISO27001 Lead Implementer
- CISSP
- CCSP
- Cisco Certified Network Associate Cyber Ops
- Security Manager
- Security Architect

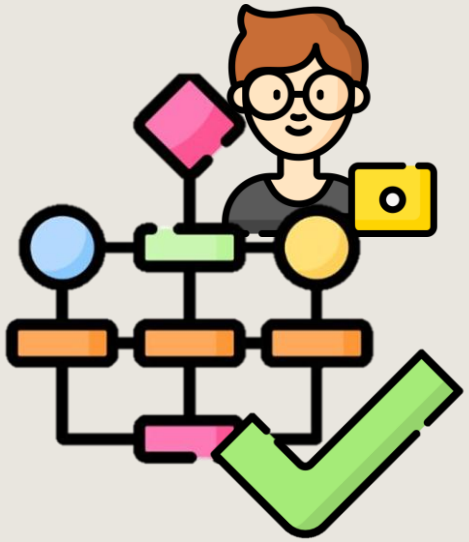
WHAT IS A SECURITY ARCHITECT?

- Software Development
- Security Testing
- System Design
- Code Review
- Network Design/Security
- Threat Modelling
- Cryptography

IT'S A TECHNICAL ROLE

- Security Architect
- Systems Architect
- Application Architect
- Cloud Architect
- Software Architect

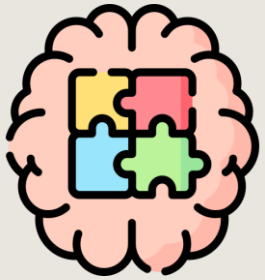




A DAY IN THE LIFE OF AN ARCHITECT

What do you get up to?

- Research
- Plan
- Design
- **Upskilling**
- Test
- **Threat Modelling**
- **Educating**
- Diagrams, Threat Models, UMLs, Activity Diagram
- Co-operate with other specialists
- Advise business leaders
- Align systems with business requirements
- **Securing systems**
- Handle compromise
- Defending decisions



SKILLS OF AN ARCHITECT

- Drive to learn & keep learning
- Find documentation relevant to security issues
- Software Development Life Cycle
- Communication
- Build, experiment, test
- Bridging the Gap
- Web Security – *for me, you might need network security or hardware security.*

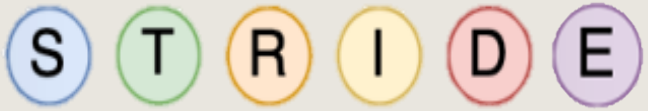
PRIMARY ROLE IS TO EDUCATE

CIA

- Confidentiality
- Integrity
- Availability

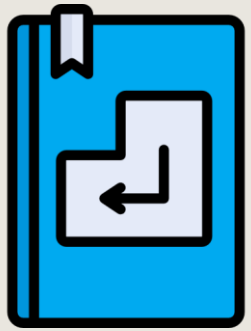
Risk

- MTD
- RPO
- Adopt a Risk Mentality
- Registering Risks
- **Risk Assessments**



Threats

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege



Incident Response

- Runbooks
- Escalation plans
- Out of hours contacts
- System documentation

WHAT'S THE FIRST STAGE OF INCIDENT RESPONSE?

PREPARATION

INFORMATION SECURITY PRINCIPLES

- **Principle of Least Privilege**
- **Disable Unused Services**
- **Logging**
- Alerting
- **Response Plans**
- **Patch Management**
- **Vulnerability Scanning**
- GDPR

- Treat security as an integral part of overall system design
- Protect information while being processes, in transit and in storage
- Implement layered security
- Authenticate users and processes ensuring appropriate access control decisions
- Strive for simplicity
- Ensure developers are trained in how to develop secure software
- **Reduce risk to an acceptable level to the business**
- Design security to allow for regular adoption of new technology and systems
- Develop and exercise contingency or disaster recovery procedures
- Design accountability and traceability into systems and services

RESOURCES WE BUILT THE PRINCIPLES ON

ISO27002

OWASP

- Secure by Design principles

National Cyber Security Centre

Summary

NIST

SP 800-160

Business Growth Lead
Cydea

Tony
Smith

Always start with clean SOCs

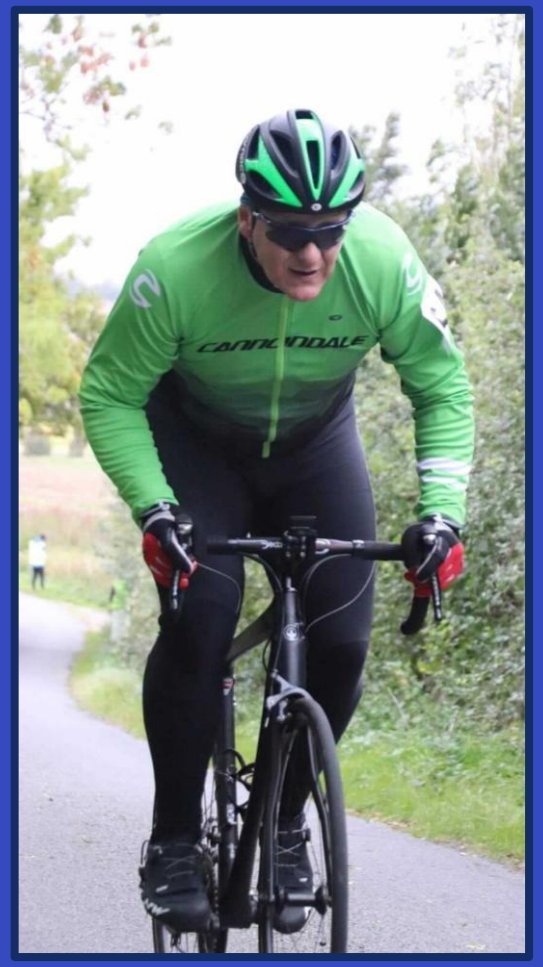
Stories and images that connect cyber security and the world of sport

Tony Smith – June 2026

Agenda

- Introduction
- The SOCs’ Mission
- Stories From The Front Line
- What You Do Is Not a Spectator Sport!
- Close

A self-confessed sports nut...



... and I also love my day job!

”chief cheerleading officer”
and
cyber security evangelist


COMING
SOON

MISSION:ALLPOSSIBLE

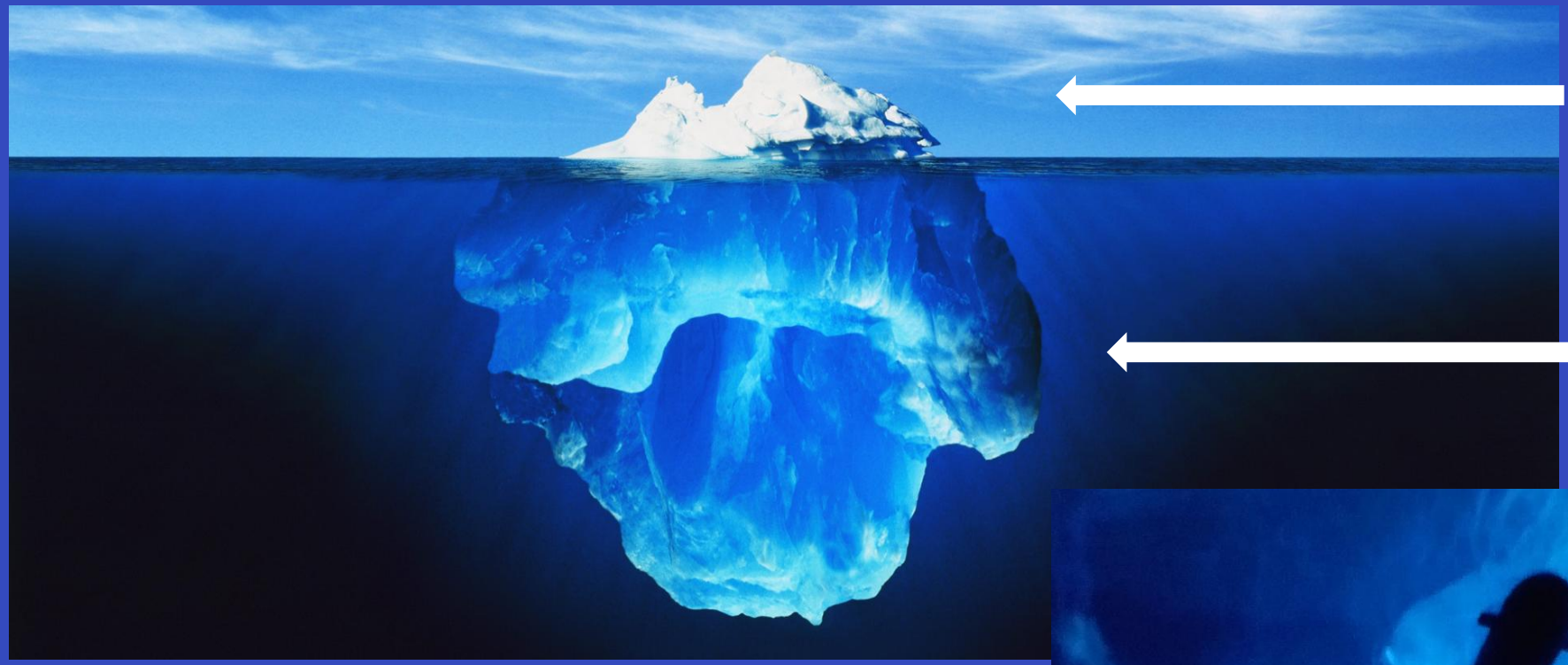
TAKEBACK

Your Mission… choose to accept it!

Effective security is invisible

The haystack!

What SOCs do is difficult !



What the world sees

What they really do

And beneath the surface lurks the threats!

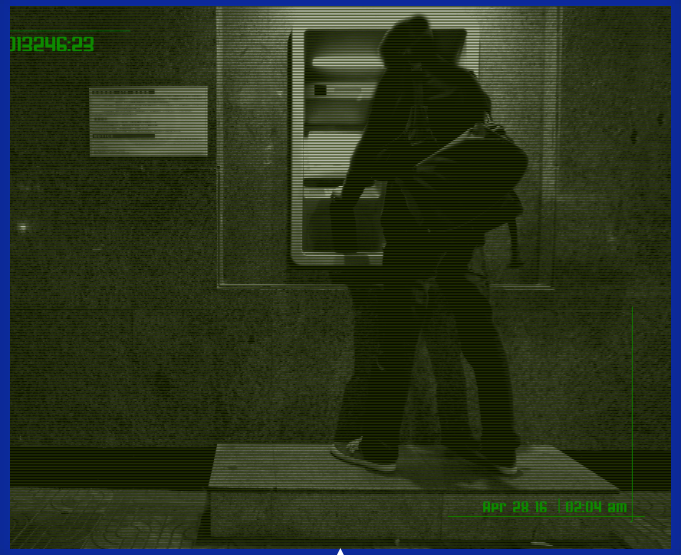
WHAT GOOD IS REGULATION?


COMPLIANCE IS ONLY A STARTING POINT
While Crossing

Stories from the Front Line

The Good Samaritan

We want your money



Real case !!

Cyber Security is NOT a spectator sport!

Cyber Security is a lot like...

...GOLF !

The right tools, in the wrong hands

The Importance of Partnership

22 x career doubles titles
(incl 14 x Grand Slams and 3 x Olympic 🥇)

Serena W
Singles – 73 x titles, 🥇
Doubles – 23 x titles, 🥇 🥇 🥇

Venus W
Singles – 49 x titles, 🥇
Doubles – 22 x titles, 🥇 🥇 🥇

61 x career doubles titles
(incl 11 x Grand Slams and 1 x Olympic 🥇)

Mark W
Singles – 4 x titles
Doubles – 67 x titles

Todd W
Singles – 2 x titles
Doubles – 83 x titles

Process – Consistency and Repetition

Muttiah Muralidaran*

800 Test Wickets (#1) 44,039 balls and 534 ODI Wickets (#1) 18,811 balls

(*spelled the way he likes it)

Every team needs a LIBERO

The Defensive Specialist – the normal rules don't apply (court position and movement, defending and attacking options)

Incident Readiness – Match-fit MVP

Tom Brady

LeBron James

Best defence always wins!

Pieter-Steph du Toit

2019 Rugby World Player of the Year

2024 Rugby World Player of the Year

Best defence always wins!

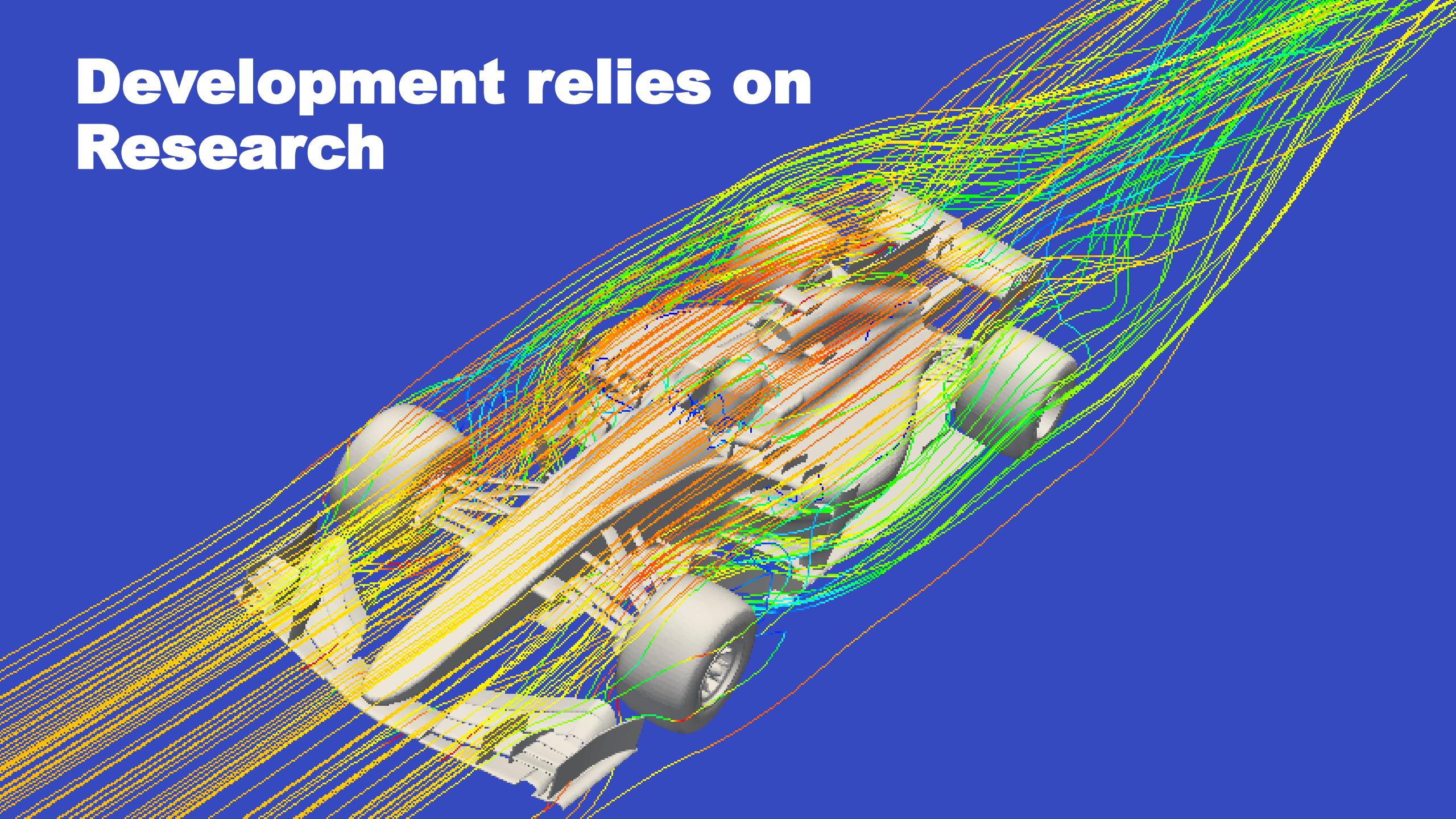
What is your next move ?

Knowing your next move (and the one after that) is essential to your chance of survival/success.

Front Foot, not Chin-music

Sachin Tendulkar
15,921 Test Runs (51 x 100's)
18,426 ODI Runs (49 x 100's)

Development relies on Research



Built/Completed September 2024

Precision relies on Practise

Hope is NOT a tactic !

Practice, practice, practice

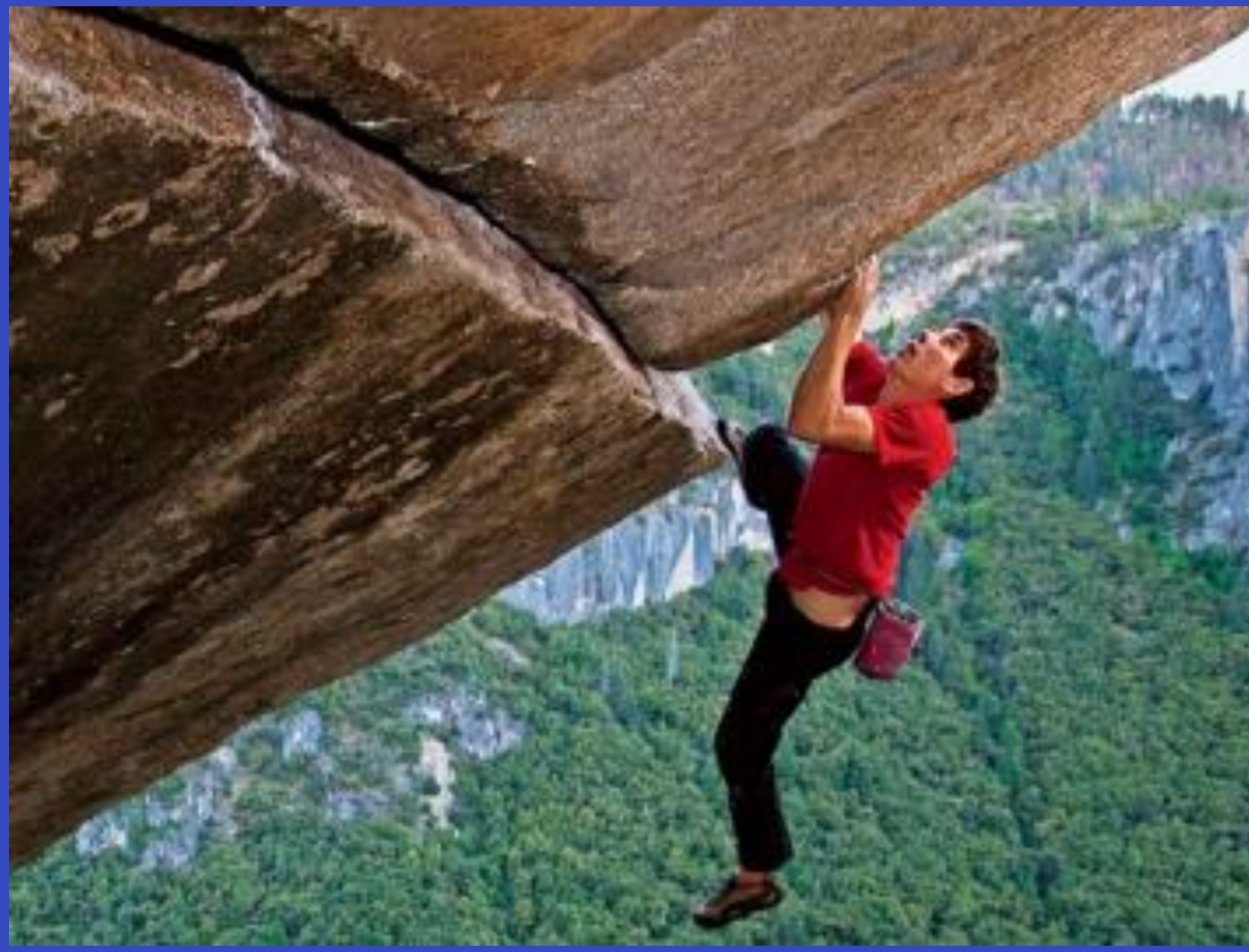
“The more I practice, the luckier I get.” ***Gary Player***

Cyber Security is TEAM sport!

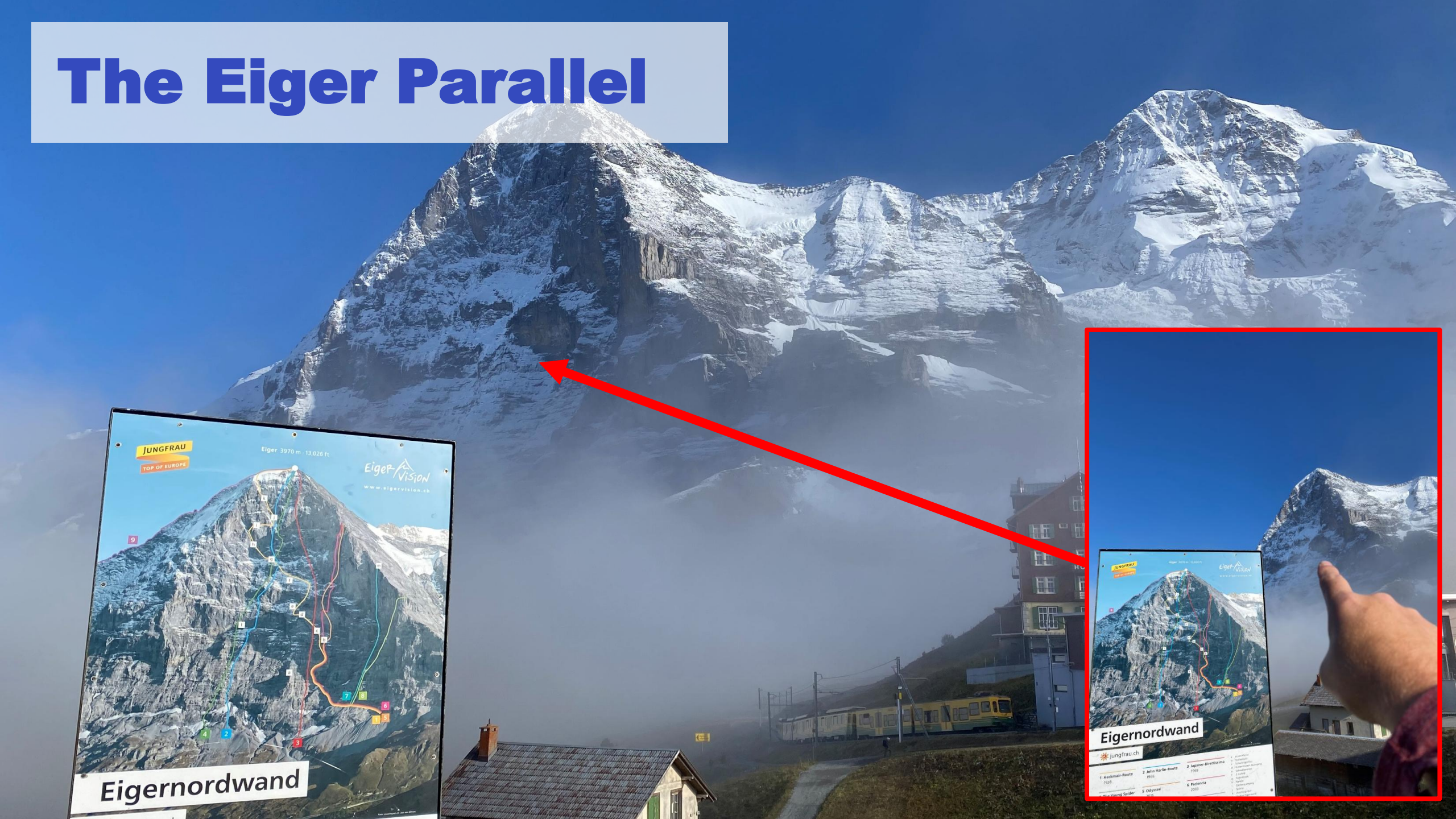
It all comes down to ...

TRUST

n. **a firm belief in the reliability, truth or ability of someone or something**



The Eiger Parallel



Trust at 13,000 feet

Let's Connect

Tony Smith

Senior Compliance & Information Security Manager DSP

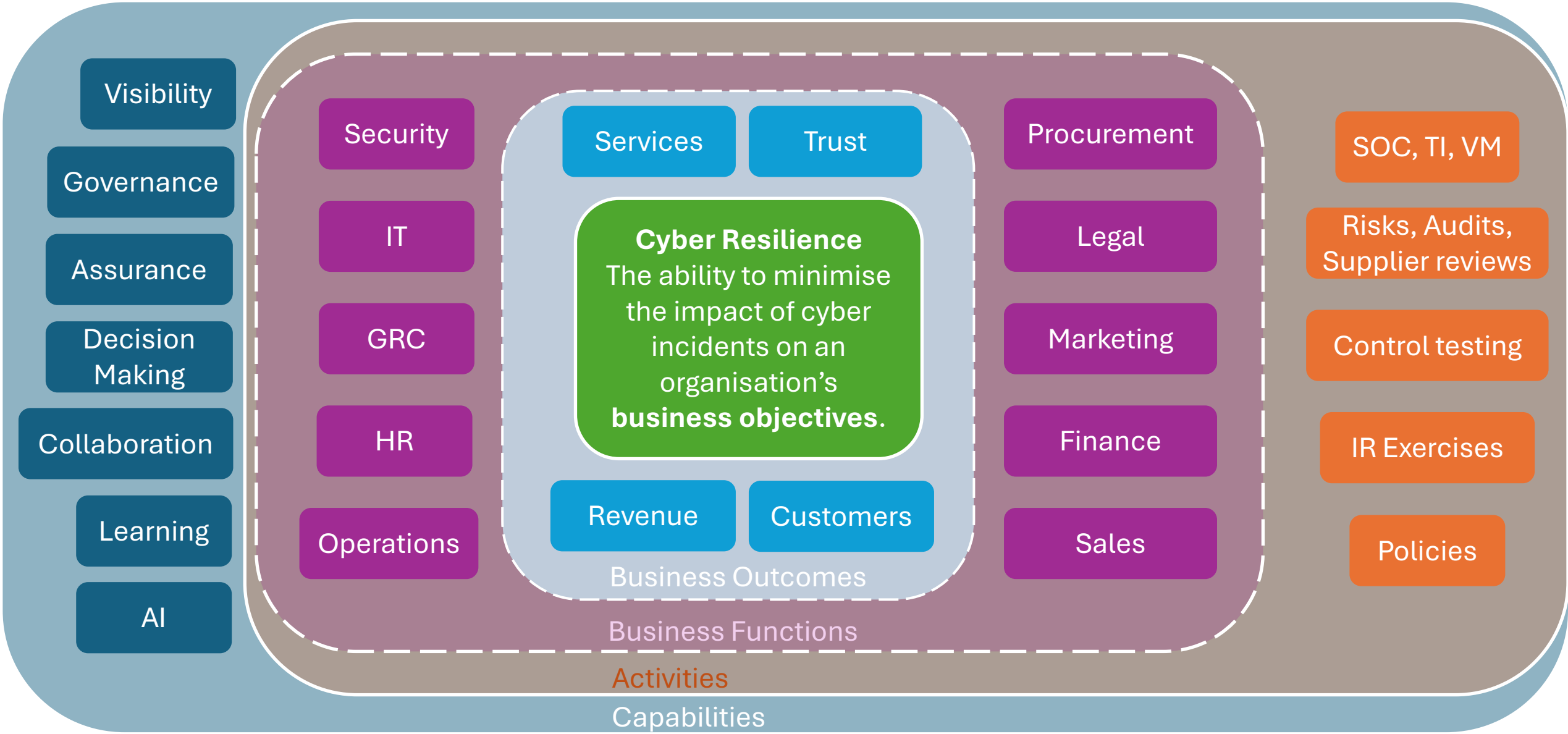
iuliana Silvasan

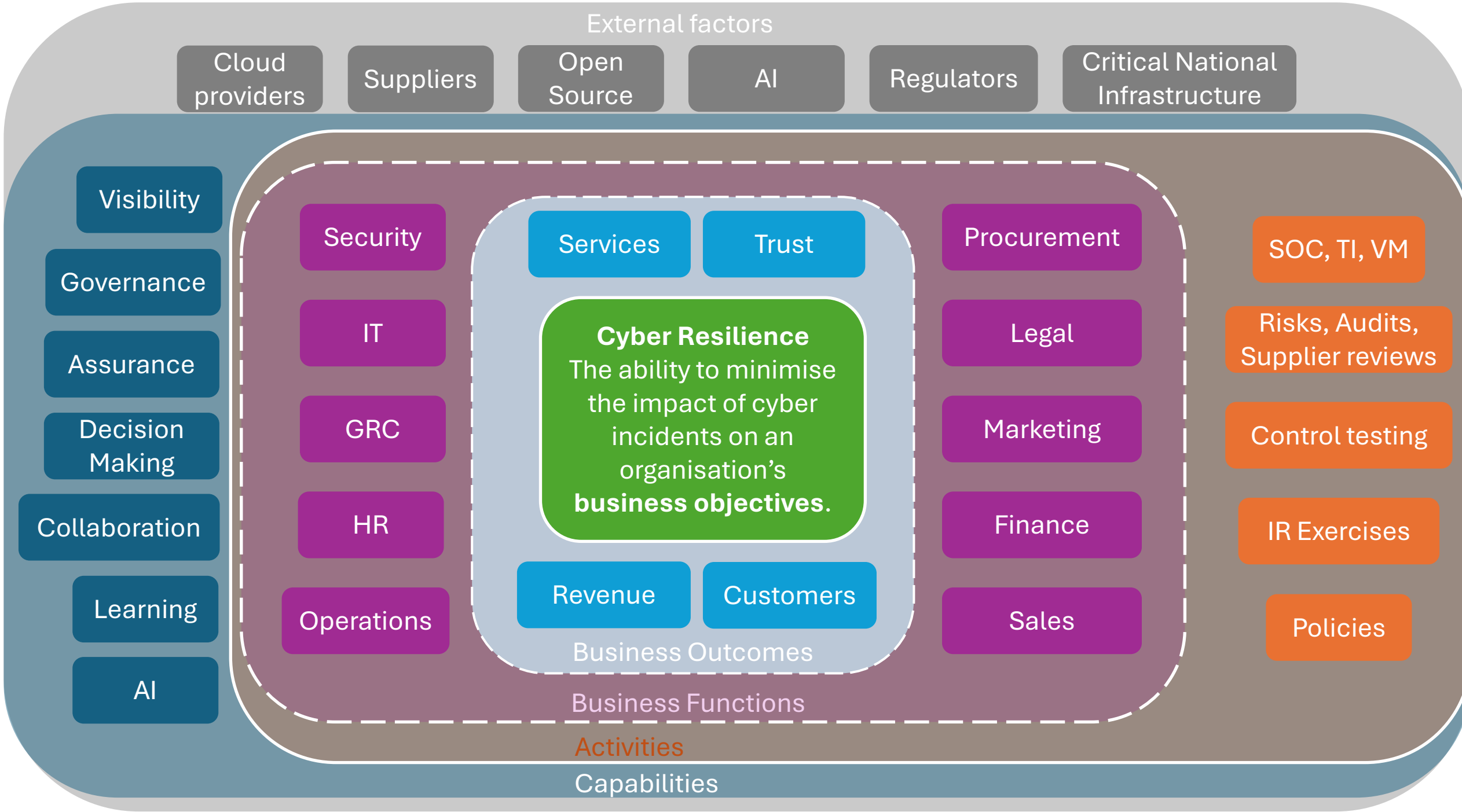
A Systems View of Cyber Resilience

iuliana Silvasan

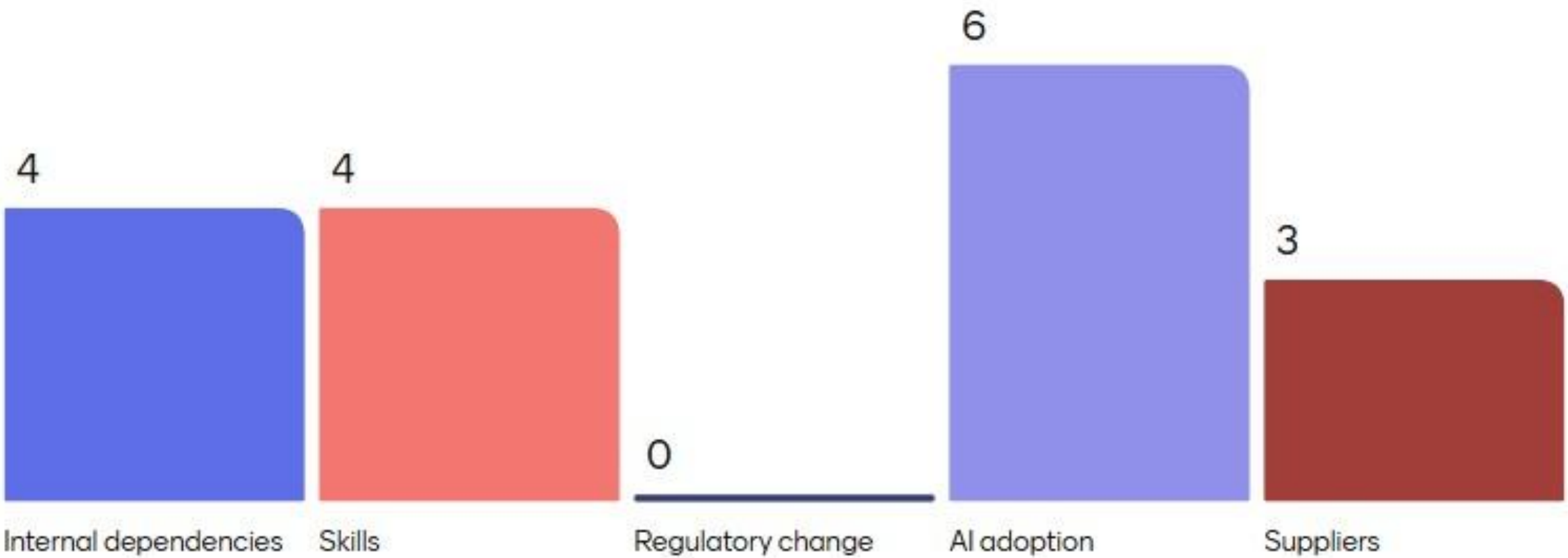
Senior Compliance and Information Security Manager @ DSP

The ecosystem of cyber resilience




External factors
Cloud providers
Suppliers
Open Source
AI
Regulators
Critical National Infrastructure
Visibility
Governance
Assurance
Decision Making
Collaboration
Learning
AI
Security
IT
GRC
HR
Operations
Services
Trust
Cyber Resilience
The ability to minimise the impact of cyber incidents on an organisation's business objectives.
Revenue
Customers
Business Outcomes
Procurement
Legal
Marketing
Finance
Sales
Business Functions
SOC, TI, VM
Risks, Audits, Supplier reviews
Control testing
IR Exercises
Policies
Activities
Capabilities

Which factor worries you the most?



Why cyber resilience matters more and more

More dependence – e.g. Suppliers, Cloud, SaaS, AI

More regulation – e.g. DORA, NIS2, UK Cyber Security and Resilience Bill

More disruption – e.g. (AI driven) Cyber attacks, outages, supplier incidents

More expectations – Customers, regulators, boards

Organisational success increasingly depends on systems we do not fully control.

A ransomware incident quickly goes from a technology incident to an enterprise coordination problem.

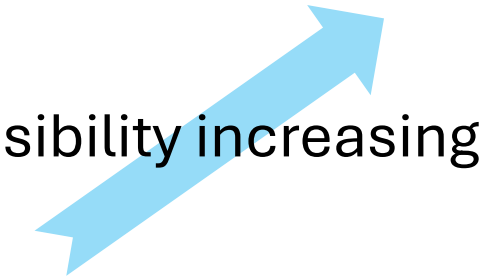
The Visibility Paradox

More monitoring

More dashboards

More frameworks

More audits



The Board Ask

Are we affected?

Can we recover?

What are we dependent on?

Are we ready?

Confidence

UK's Cyber Governance Code of Practice for Boards and Directors

(A) Risk Management

(B) Strategy

(C) People

(D) Incident planning, response and recovery

(E) Assurance and oversight

- Self-assessment and Board training can highlight areas for improvement.

Visibility → Understanding

(A) Risk Management

Risk creates focus

- What are the top five risks most likely to stop the desired business outcomes?
- Focus effort where it creates the greatest value.

Lesson learned: Move discussion from vulnerabilities to business disruption, customer trust, supplier failure, key system and person dependency.

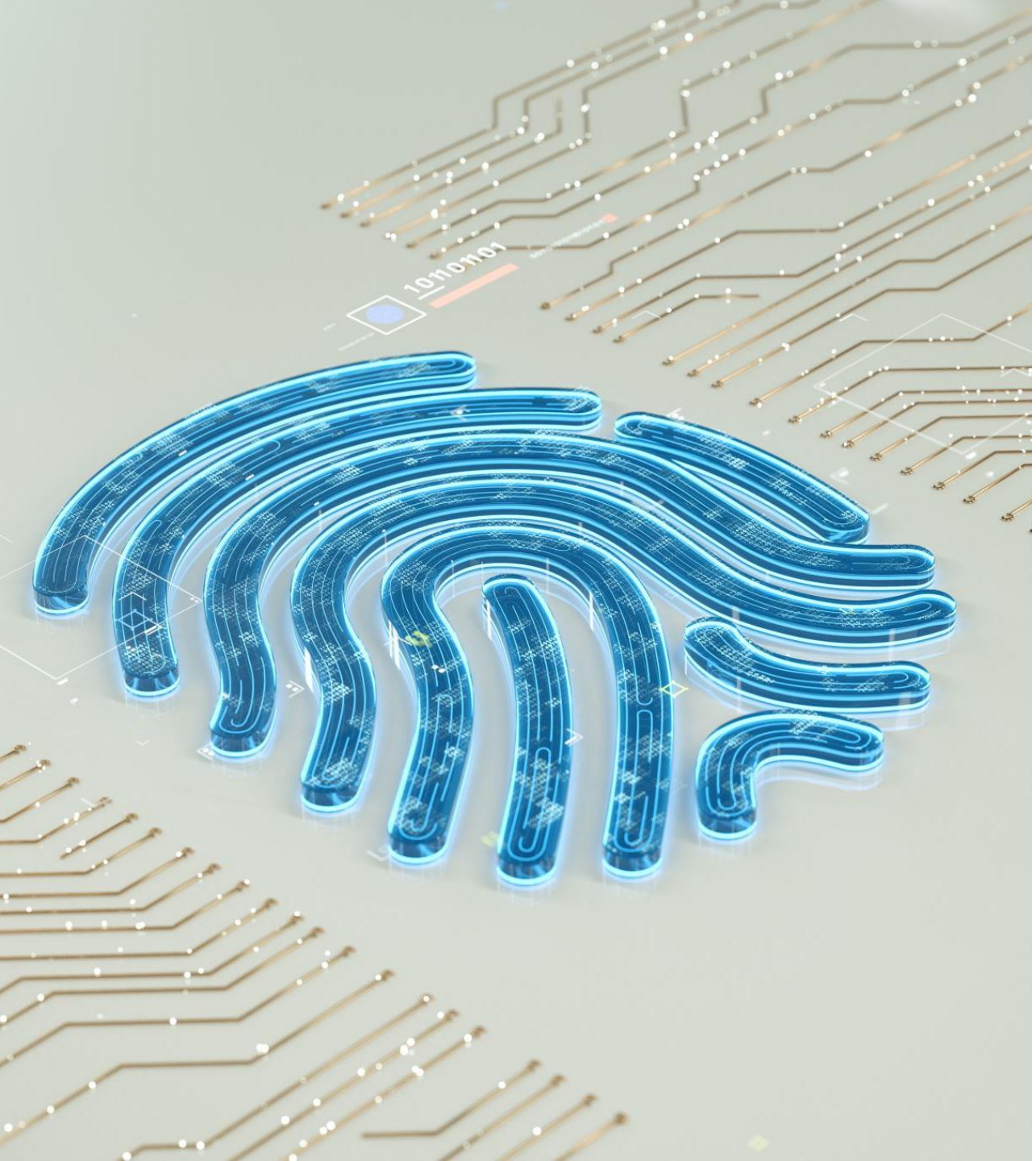
Understanding → Investment

(B) Strategy

Strategy creates alignment

- When *organisational strategy* embeds cyber security strategy across its entire ecosystem, cyber resilience increases.
- Which business objective is your cyber programme protecting?
- Are we investing in the right things?

Lesson learned: Map projects to outcome and risk appetite.



Vision

to **embed security** into the fabric of our culture **as a shared responsibility** built on **collaboration** and a genuine care **for doing the right thing**.

We **protect what matters**, maintain customer trust and **stay resilient** in the face of cyber threats, always **ready to scale** as we expand as a global player in the database managed services field.

Security that protects, empowers and scales.

Investment → Capability

(C) People

People create capability

- Cyber resilience depends on accountable, capable, cyber, data and AI-aware people across the organisation.
- Who owns cyber risk outside the security team?

Lesson learned: Cyber awareness is not the same as cyber accountability. People create resilience when they understand their role in the system.

What would be hardest if chat and email were unavailable for 24 hours?

What leaders should know before the incident

- The top 5 business services that matter most
- The systems and suppliers they depend on
- The departments needed to keep them running
- The manual workarounds available
- The decisions that would be hardest under pressure
- The communication channels available if normal tools fail
- The partners needed for recovery
- The evidence that controls and plans have been tested and assumptions identified

Capability → Confidence

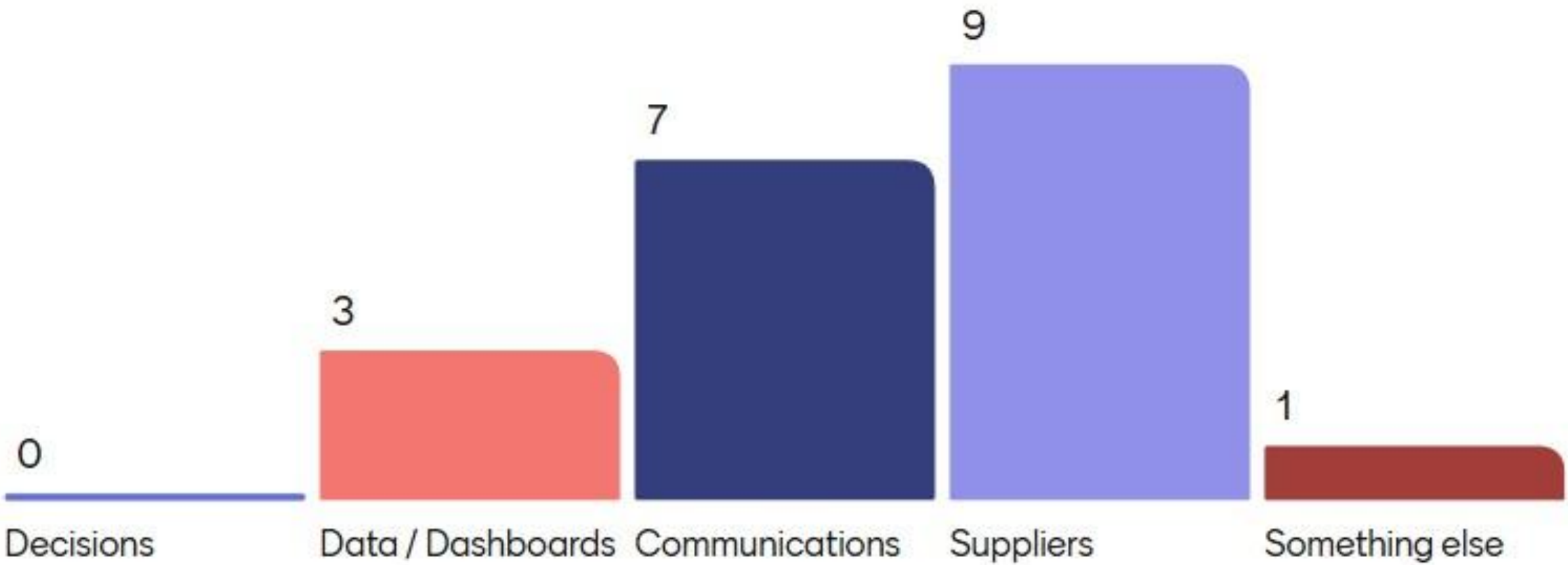
(D) Incident planning, response and recovery

Exercises create confidence

- People might know their tasks, but do they know their decisions?
- AI changes speed, scale, volume, whilst accountability and governance stay the same. If AI investigates incidents in minutes, can we make decisions in minutes?

Lesson learned: Relationships, judgement and practiced accountability matter more than roles on paper. Measure decision speed, recovery capability.

During a major incident, what would you trust least?



Data → Operational Truth

(E) Assurance and oversight

Assurance creates trust

- What evidence supports our confidence that the system works or is trustworthy?
- GRC creates the data layer that reflects reality.
- What would your teams stop trusting first?

Lesson learned: Identify what demonstrates a control works. Rank your controls for better focus. Ensure metrics demonstrate confidence, not activity. Ensure a single source of truth.

What is your biggest obstacle to cyber resilience?

Cyber Resilience is an emergent system property

Cyber resilience improves when leaders:

- Focus on the risks that matter most.
- Understand how the business creates value.
- Align cyber strategy across the whole organisation.
- Build capability through people, accountability and culture.
- Test the organisation, not just the technology.
- Seek assurance that reflects operational reality.
- Use governance to turn data into accountable decisions.
- Create learning systems that continuously improve resilience.

iuliana Silvasan, PhD

Govern risk, security and AI as they scale | GRC, security...

Thank you

Q&A Panel Discussion

Cyber East MEETS...

BECOME A CYBER AMBASSADOR IN YOUR LOCAL CITY

Why become a Cyber Ambassador?

- Share your skills and knowledge with our community
- Be at the heart of your local peer events
- Help us grow and engage our local communities
- Be part of a growing cyber cluster supporting the East region
- Represent Cyber East at events and trade shows

Contact info@cybereast.co.uk for more details

Thank you for joining us today.

Now for pizza – kindly provided by Tony Smith!