AusCERT Cyber Leaders' Network (CLN)
Cyber Culture Metrics

Tim Lane
AusCERT Cyber Leaders Network
May 2026

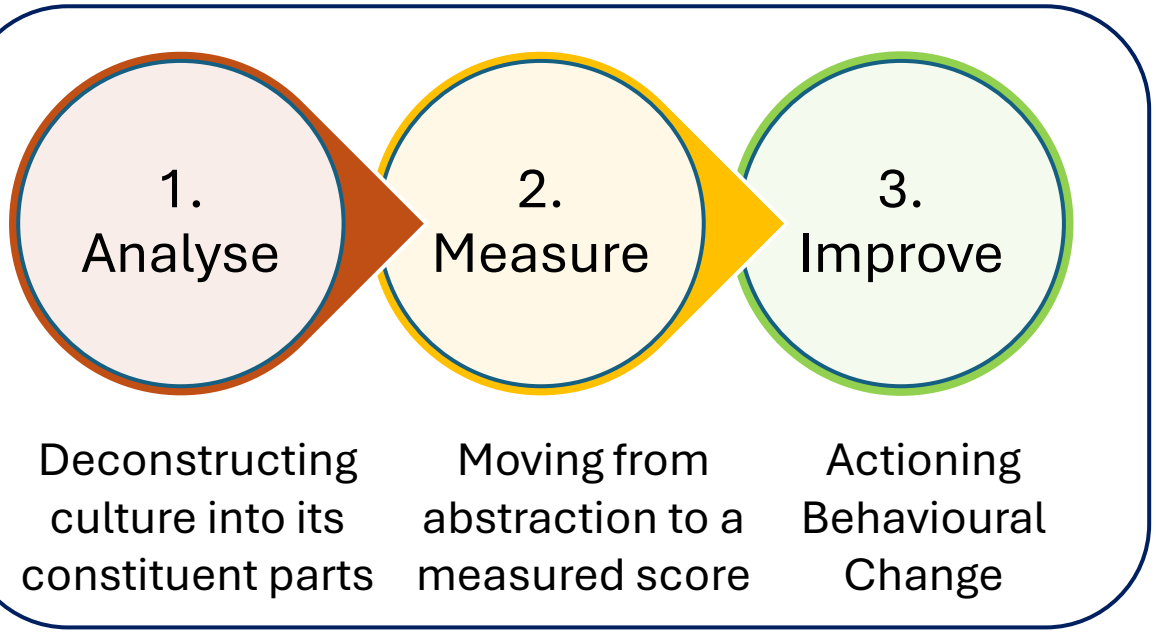
Introduction

Scope

- Focus on understanding existing cyber culture frameworks
- Helping bridge the gap between theoretical frameworks, current literature, and best practice models
- Practical measurement of cyber culture (human cyber risk)

Roadmap Approach

Cyber Security Culture Toolkit



The Cyber Culture Toolkit includes:

(1) Key Cyber Culture Guiding Principles and a simple theoretical Framework (CMDF)

(2) Customisable instrument to measure metrics and help drive improvements in organisational security behaviours

(3) Cybersecurity Culture Maturity Model (CCMM)

Cyber Culture – Why does it matter?

The Problem

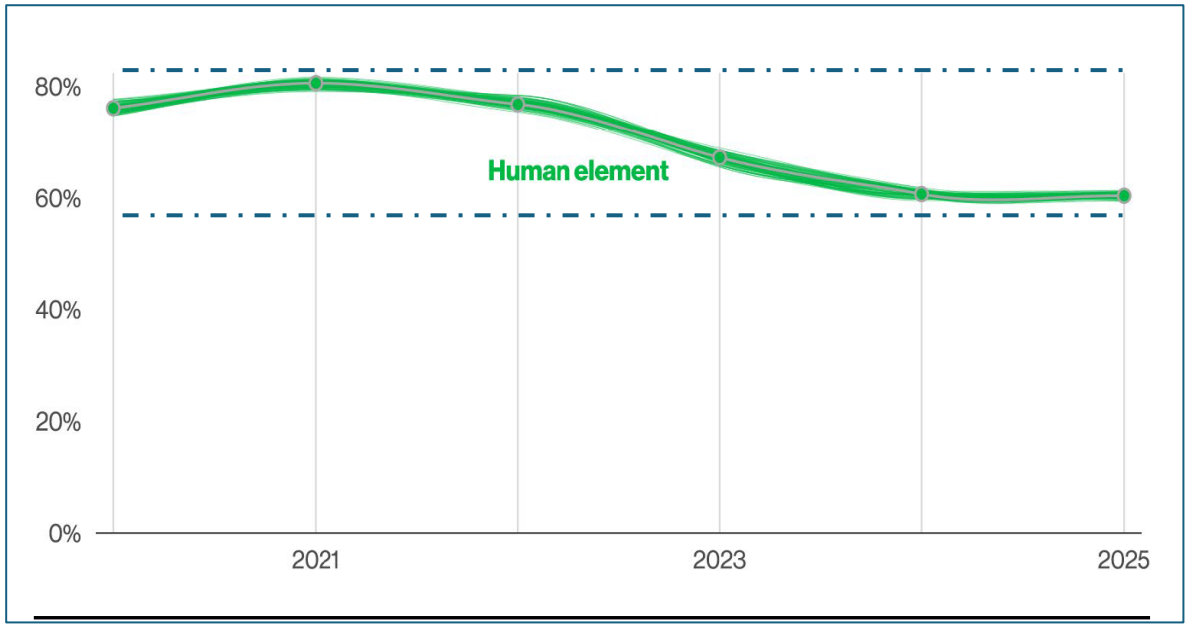


Figure 1 - Human element involvement over time in breaches – Verizon DBIR Report 2025

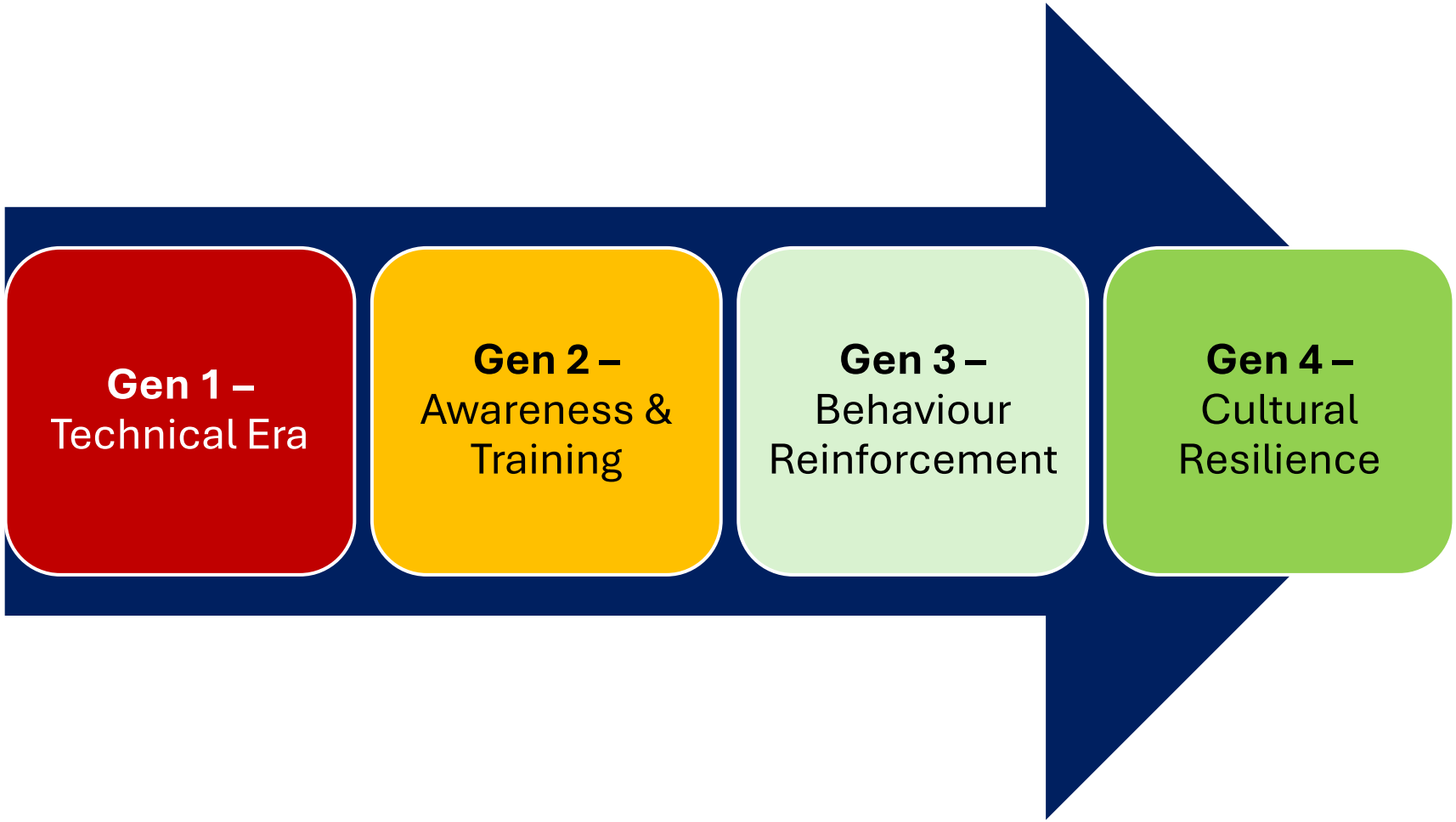
Key Points

- The human element is still causal in the majority of cyber incidents
- Ultimately, it is a change of behaviour that is needed to shift the dial
- The most effective lasting behaviour is achieved through embedded culture

To defend against modern threats, it's necessary to transition from **periodic compliance** to an **embedded cyber culture**.

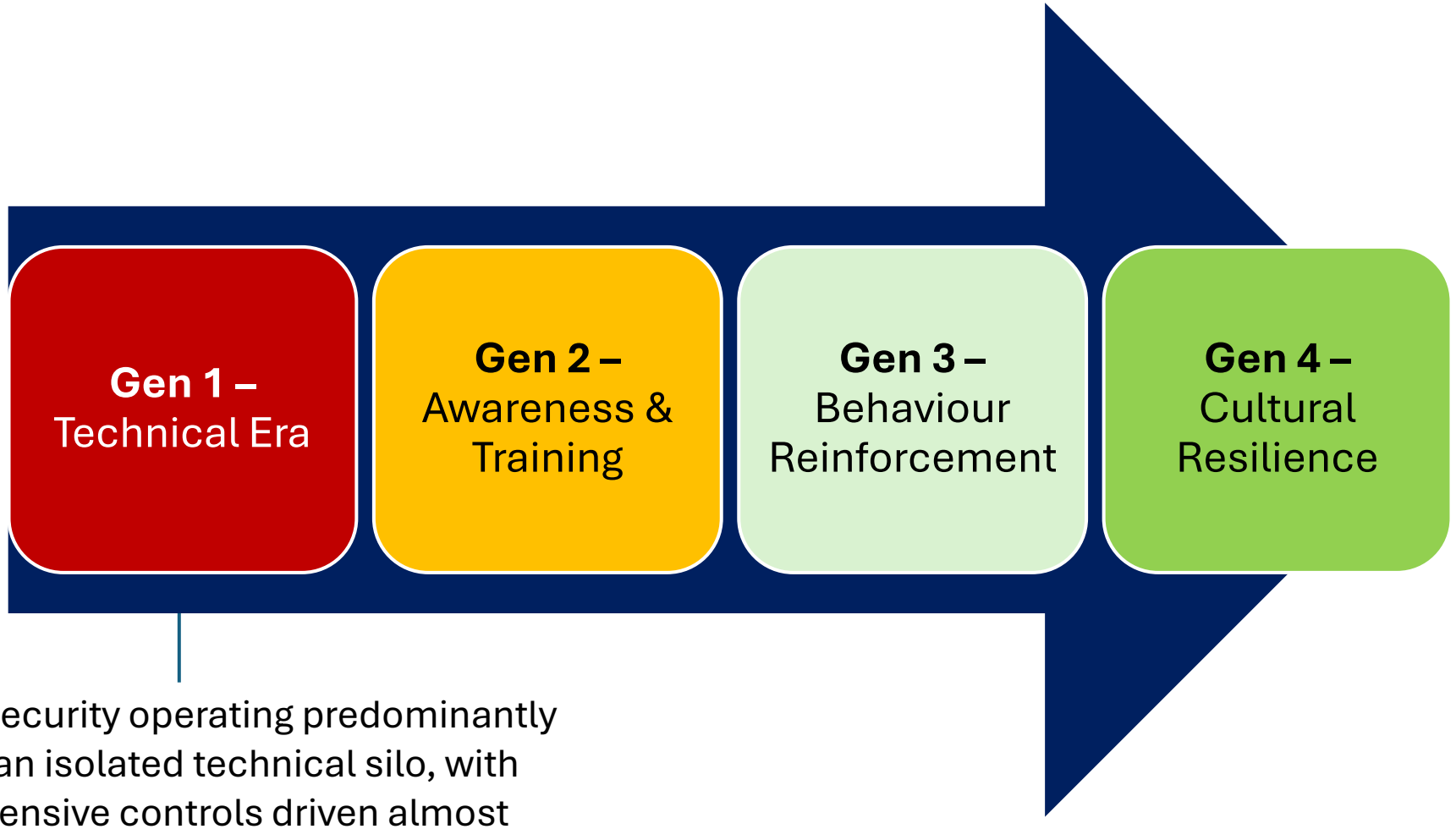
Cyber Culture Evolution

Cyber Cultural Evolution



Cyber Culture Evolution

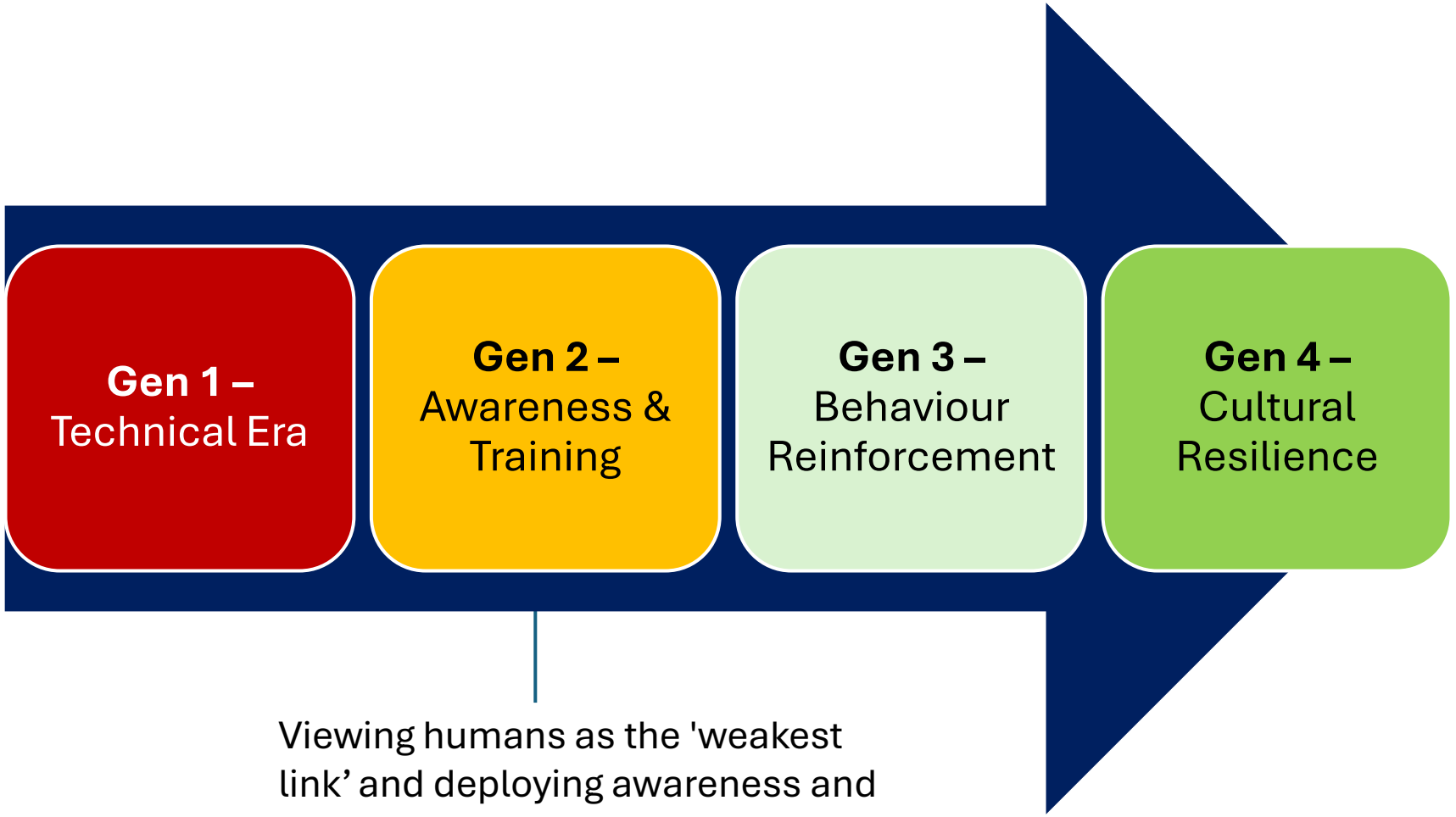
Cyber Cultural Evolution



IT security operating predominantly as an isolated technical silo, with defensive controls driven almost exclusively by technology.

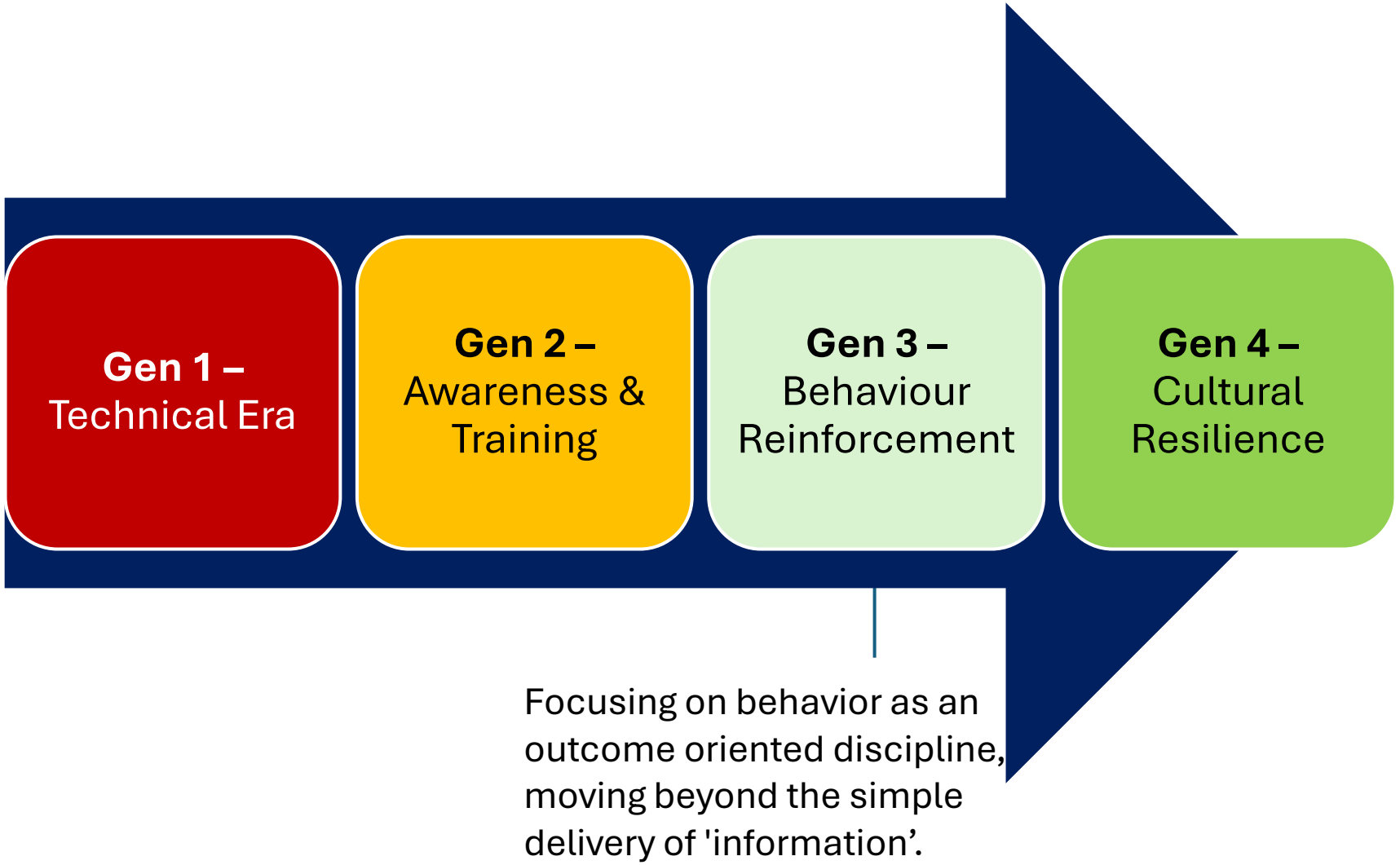
Cyber Culture Evolution

Cyber Cultural Evolution



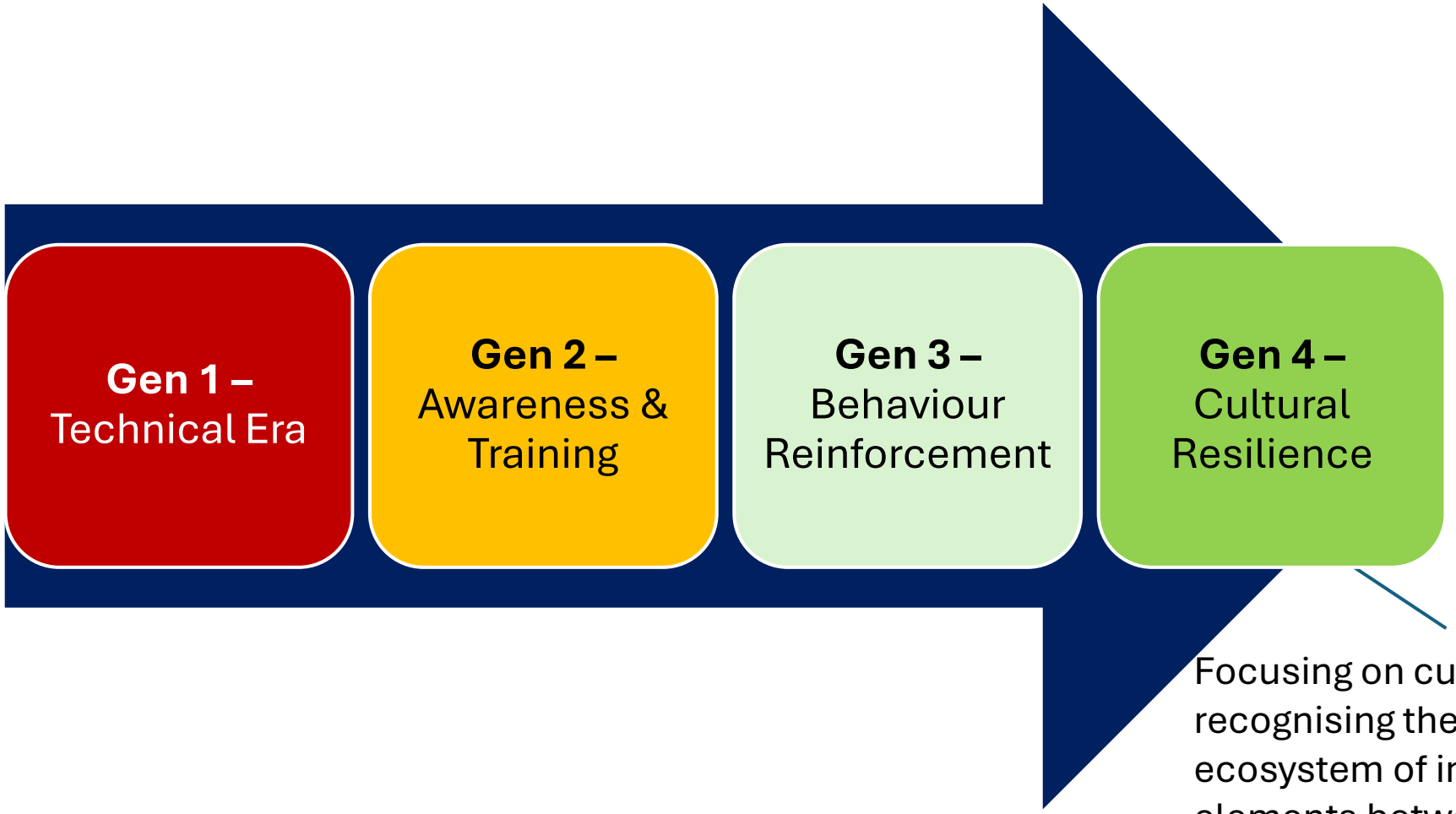
Cyber Culture Evolution

Cyber Cultural Evolution



Cyber Culture Evolution

Cyber Cultural Evolution



Focusing on cultural resilience: recognising the complex ecosystem of interacting elements between people and the organisation that determine actual security resilience.

Cyber Culture Evolution

Cyber Cultural Evolution

1 - Key Cyber Culture Guiding Principles

ENISA Cyber Security Culture Framework

ENISA's work on cyber security culture is widely recognised as a pre-eminent European reference point for integrating behavioural science, awareness, governance and organisational culture into cybersecurity strategy.

ENISA provides a highly influential framework, but does not provide a cyber culture scoring model.

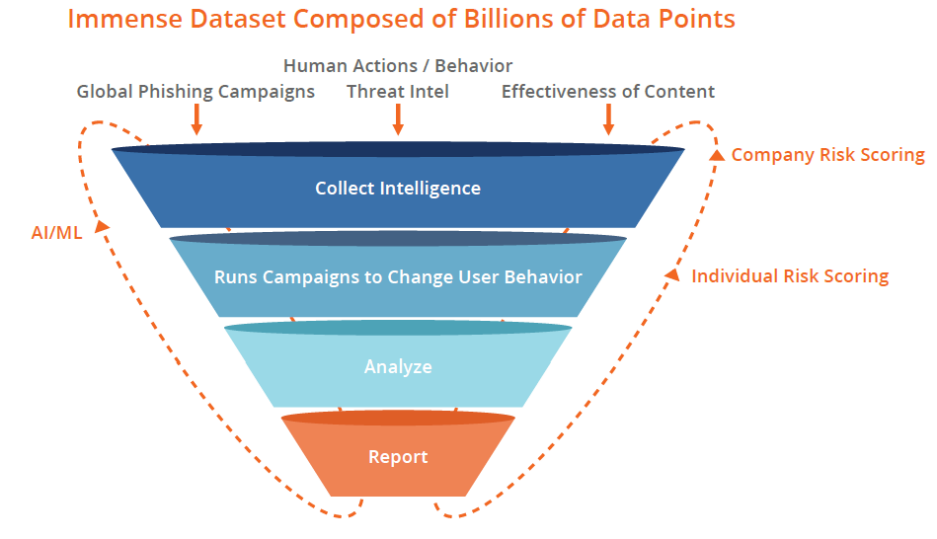
NIST - Creating a Culture of Security

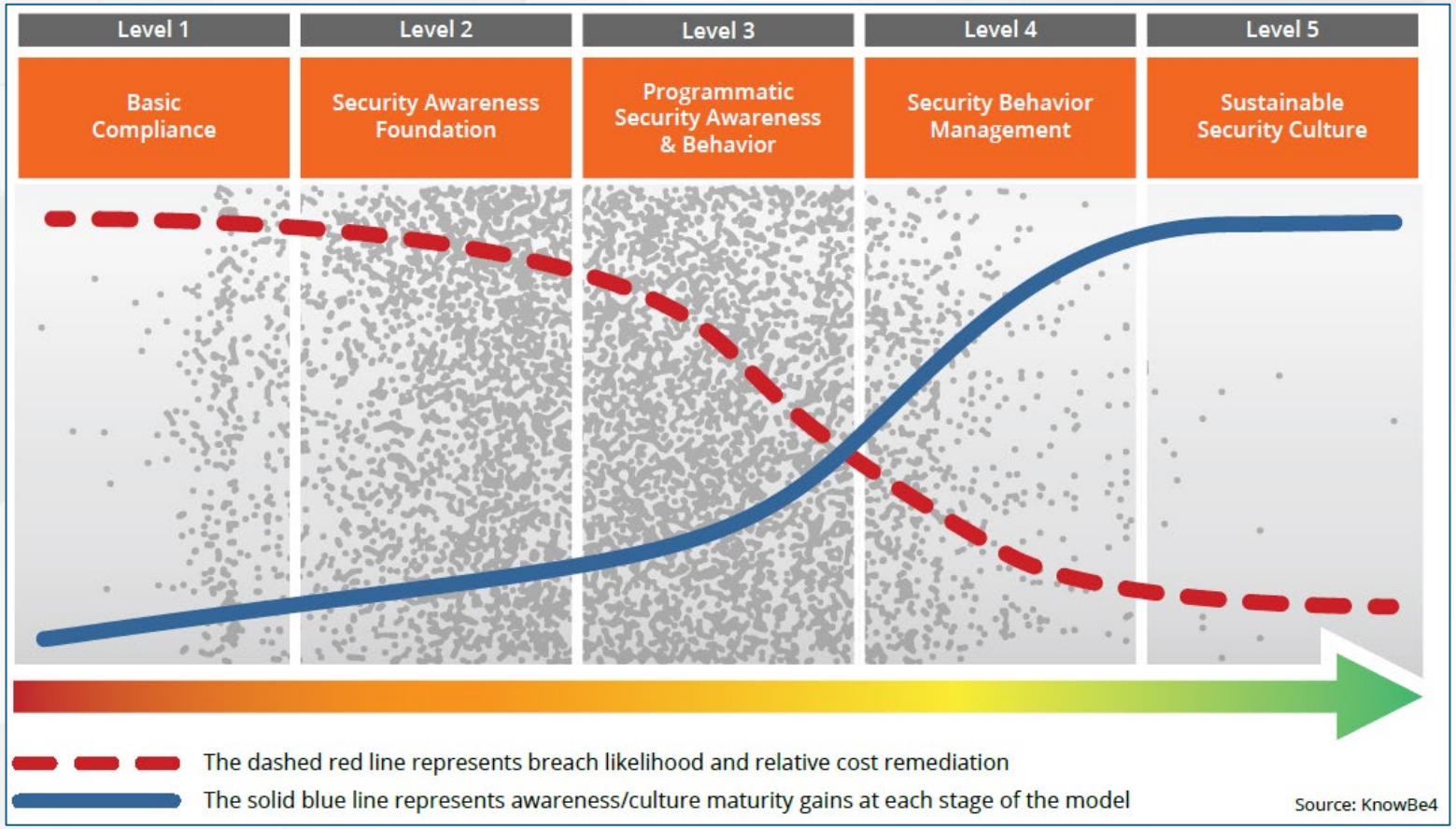
Leverages Socio Technical Systems (STS) Theory and Human Centered Design (HCD)
NIST CSF 2.0 (Cybersecurity Framework) – The Structural Mandate
NIST SP 800-55 Rev. 2: Measurement Guide for Information Security
NIST SP 800-50 & SP 800-16: Building an Information Technology Security Awareness and Training Program
NIST Human Factors in Cybersecurity

KnowBe4 Implementation

7 Focus Areas

1. Attitudes
2. Behaviours
3. Cognition
4. Communication
5. Compliance
6. Norms
7. Responsibilities

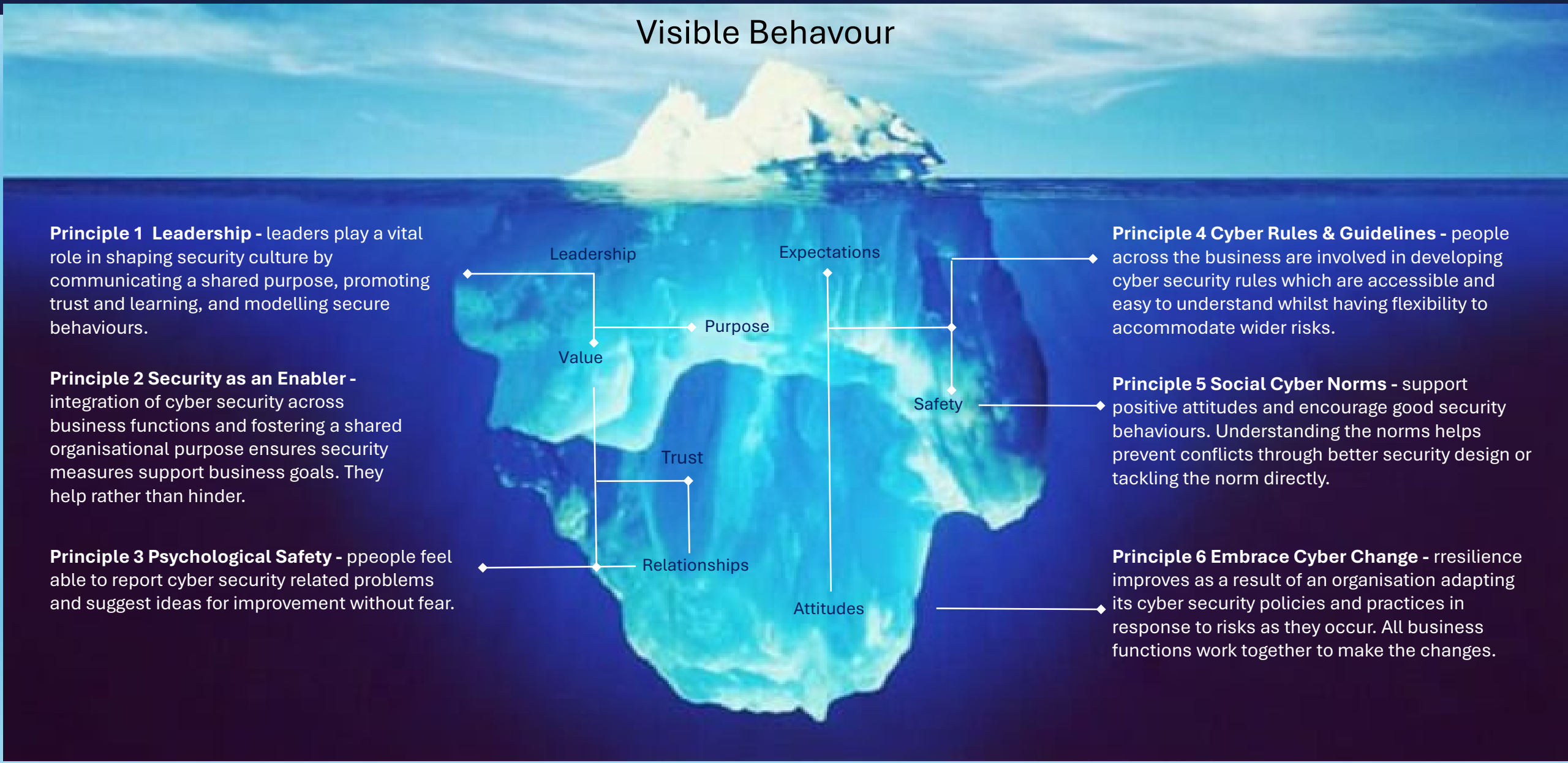




The Cyber Security Culture Iceberg

AUSCERT

The cyber security culture iceberg provides a visual aid to identify principles that help create, as well as demonstrate, a strong cyber culture.



Principle 1 Leadership - leaders play a vital role in shaping security culture by communicating a shared purpose, promoting trust and learning, and modelling secure behaviours.

Principle 2 Security as an Enabler - integration of cyber security across business functions and fostering a shared organisational purpose ensures security measures support business goals. They help rather than hinder.

Principle 3 Psychological Safety - ppeople feel able to report cyber security related problems and suggest ideas for improvement without fear.

Principle 4 Cyber Rules & Guidelines - people across the business are involved in developing cyber security rules which are accessible and easy to understand whilst having flexibility to accommodate wider risks.

Principle 5 Social Cyber Norms - support positive attitudes and encourage good security behaviours. Understanding the norms helps prevent conflicts through better security design or tackling the norm directly.

Principle 6 Embrace Cyber Change - rresilience improves as a result of an organisation adapting its cyber security policies and practices in response to risks as they occur. All business functions work together to make the changes.

Topic 2 – CCMM Measurement Instrument

CCMM Reference

The CCMM measurement instrument provides a:

1. Diagnostic Tool (6 dimensions aligned with NCSC Iceberg model, 5 questions each)
2. Linkage to Theoretical Foundation
3. Cyber Culture Measurement Score
4. CCMM Reference for Improvements

Instrument Validity:

Ensuring a rigorous validation process for the survey instrument:

- Review of published models and frameworks
- Leverage of the NCSC Iceberg model into six dimensions to measure both explicit security behaviours and implicit cultural values
- Use of AI assisted cognitive interviews with Staff personas to evaluate question comprehension, mitigate response bias, and ensure construct validity across target audiences
- Developed a dimensional scoring system that maps metrics directly to the capability maturity model levels.

CCMM Reference

#	Leadership	Security as an Enabler	Psychological Safety	Cyber Rules & Guidelines	Social Cyber Norms	Embrace Cyber Change
1	Resourcing	Strategic Enabler	Incident Reporting	Accessibility	Positive Reinforcement	Continuous Improvement
2	Commitment	Behaviour Linkage	Security Response	Ease of Understanding	Cultural Embedding	Change Adaptation
3	Prioritisation	Work Practice Consideration	Incident Disclosure	Relevance and Currency	Social Expectation	Agility
4	Role Modelling	Safe Adoption of Technology	Trust in Human Intent	Balancing Innovation and Risk	Behaviour Modelling	Rationale for Change
5	Cyber Risk Treatment	Cyber Built In Alignment	Work Impact Disclosure	Consistency in Practice	Decision Integration	Empowerment

CCMM Reference

AUSCERT

#	Leadership	Security as an Enabler	Psychological Safety	Cyber Rules & Guidelines	Social Cyber Norms	Embrace Cyber Change
1	Resourcing	Strategic Enabler	Incident Reporting	Accessibility	Positive Reinforcement	Continuous Improvement
2	Commitment	Behaviour Linkage	Security Response	Ease of Understanding	Cultural Embedding	Change Adaptation
3	Prioritisation	Work Practice Consideration	Incident Disclosure	Relevance and Currency	Social Expectation	Agility
4	Role Modelling	Safe Adoption of Technology	Trust in Human Intent	Balancing Innovation and Risk	Behaviour Modelling	Rationale for Change
5	Cyber Risk Treatment	Cyber Built In Alignment	Work Impact Disclosure	Consistency in Practice	Decision Integration	Empowerment

The Cyber Security Culture Iceberg

AUSCERT

Diagnostic Tool for Measurement of Cyber Culture						
1	Leadership	**Resource Commitment**	Leadership provides adequate time, budget, and people to manage cyber security risks effectively	5 = Strongly Agree	100	5
2		**Communication**	Leaders communicate regularly about cyber security risks and expectations.	5 = Strongly Agree	100	5
3		**Prioritisation**	Leadership demonstrates that cyber security is important to achieving business goals	5 = Strongly Agree	100	5
4		**Role Modelling**	Senior leaders are held to the same cyber security standards and rules as everyone else	5 = Strongly Agree	100	5
5		**Cyber Risk**	Leaders raise and address cyber security concerns when risks are identified	5 = Strongly Agree	100	5

Cyber Culture Determinants Framework

Cyber Culture Determinants Framework (CMDF)

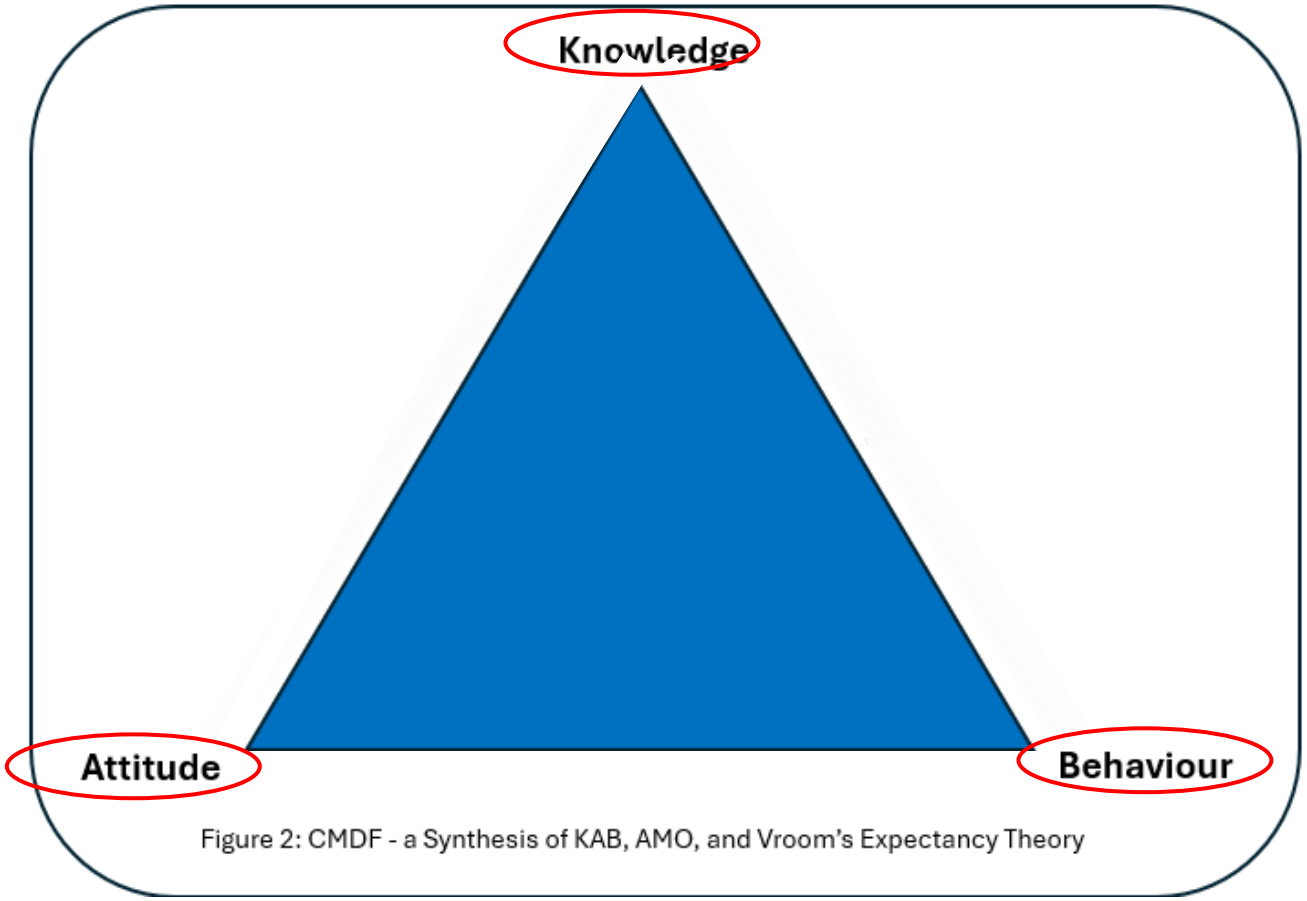


Figure 2: CMDF - a Synthesis of KAB, AMO, and Vroom's Expectancy Theory

KAB - understanding the psychological journey. Do Staff know risks and rules (***Knowledge)*** ? Do they believe it matters ***(Attitude)***? Do they actually follow it? (***Behaviour***)

Cyber Culture Determinants Framework

Cyber Culture Determinants Framework (CMDF)

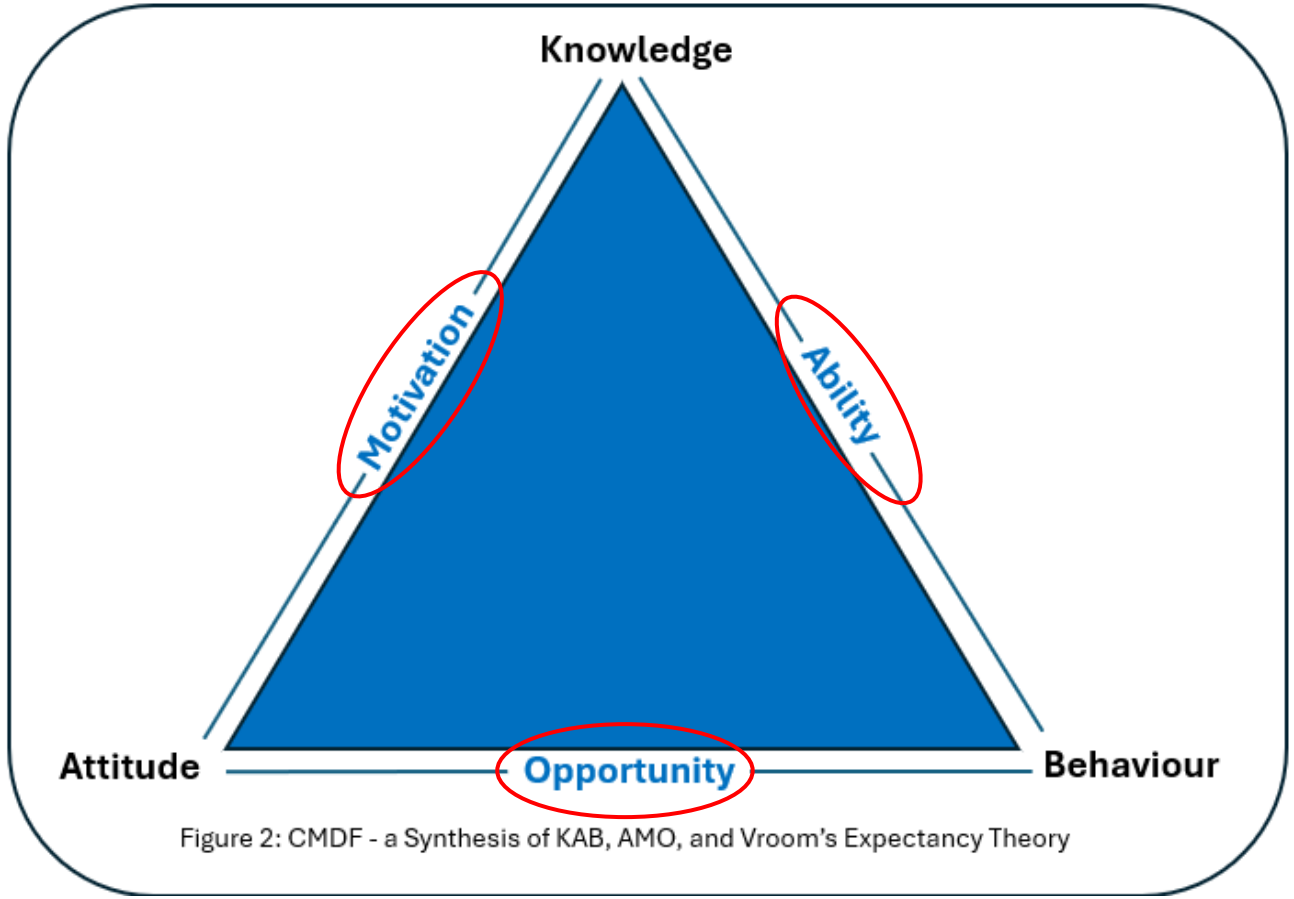


Figure 2: CMDF - a Synthesis of KAB, AMO, and Vroom's Expectancy Theory

AMO - the organisation and the individual – does the organisation provide Staff the ***Ability*** (training), the ***Motivation*** (recognition), and the ***Opportunity*** (frictionless processes) to be secure?"

Validation and Theoretical Justification

KAB/AMO Foundation	Theoretical Foundation	Justification
KAB (Behavior) (Organisational) - Leadership's physical actions in funding security. **AMO** (Opportunity) - Allocation of budget, time, and people directly provides the resources (opportunity) employees need to act securely.	Schein's Model of Organizational Culture (Edgar Schein)	Culture is influenced by what leaders fund, measure, and personally model.
KAB (Knowledge) (Attitude) - Regular messaging builds threat awareness and reinforces that cyber safety is an organisational priority. **AMO** (Motivation) (Extrinsic) - Transparent communication from leadership creates top-down accountability and a compliance mindset.		
KAB (Attitude) - Shifting the perception of cyber risk from an isolated IT issue to a core business priority. **AMO** (Motivation) - Board-level prioritisation establishes institutional urgency and strategic buy-in.		
KAB (Attitude) (Behavior) - Personnel mirror executive actions, where visible compliance by leaders fosters a positive cultural attitude. **AMO** (Motivation) - Eliminates double standards, increasing the willingness of staff to follow established rules.	Transformational Leadership Theory (Bass & Avolio)	
KAB (Behavior) - Active escalation and management of security concerns by leaders as a visible governance practice. **AMO** (Ability) (Opportunity) - Management actively challenging risk provides a structured pathway and support for staff to flag issues.		

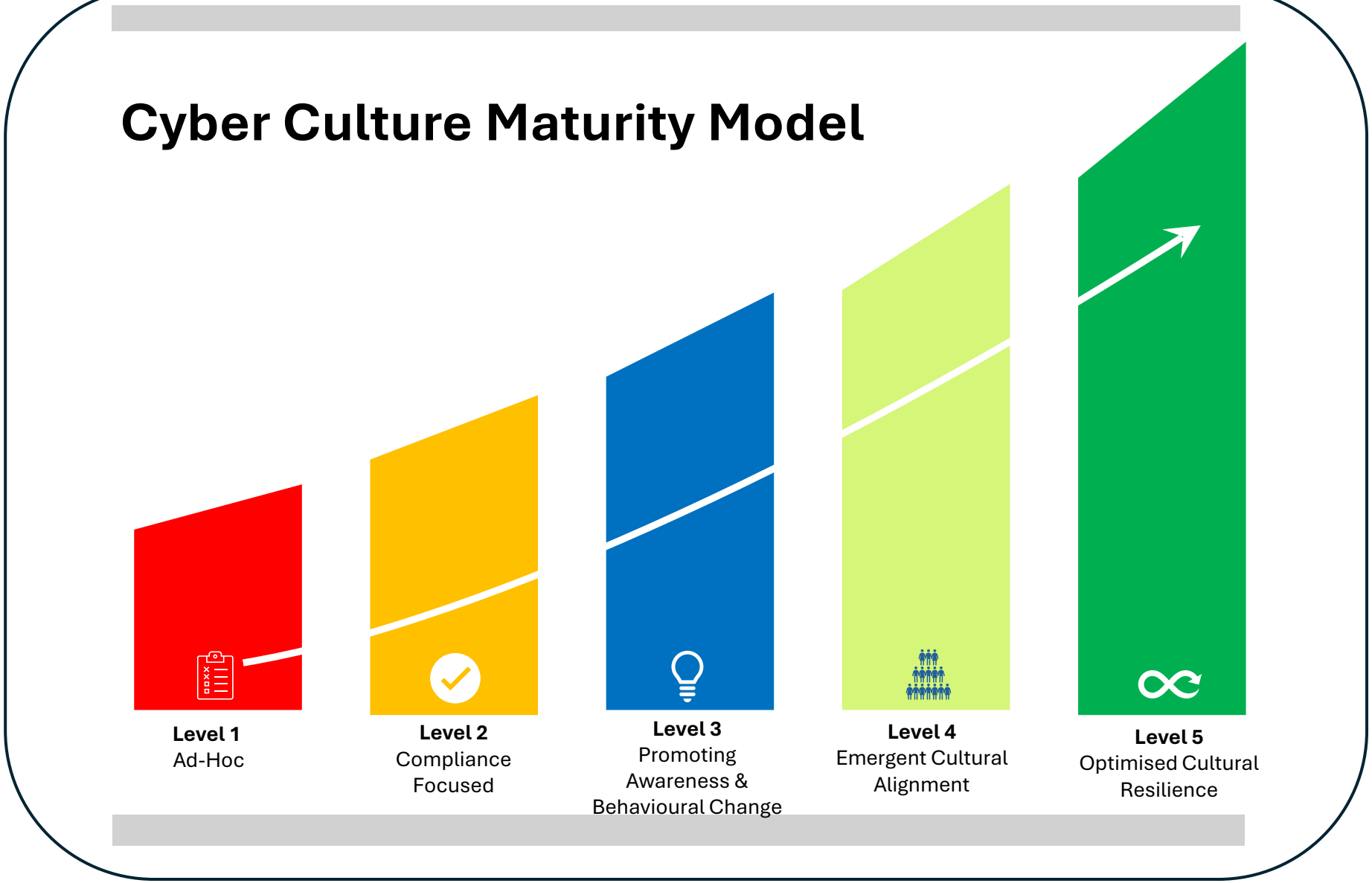
3 – CCMM Capability Maturity Model

The Cyber Security Culture Maturity Model

Figure 3 – The Cyber Culture Maturity Mode Illustrates an organisation's progression from having Ad Hoc culture to achieving an embedded, proactive and self sustaining security culture.

As maturity increases, behaviour shifts from basic compliance toward optimised secure habits

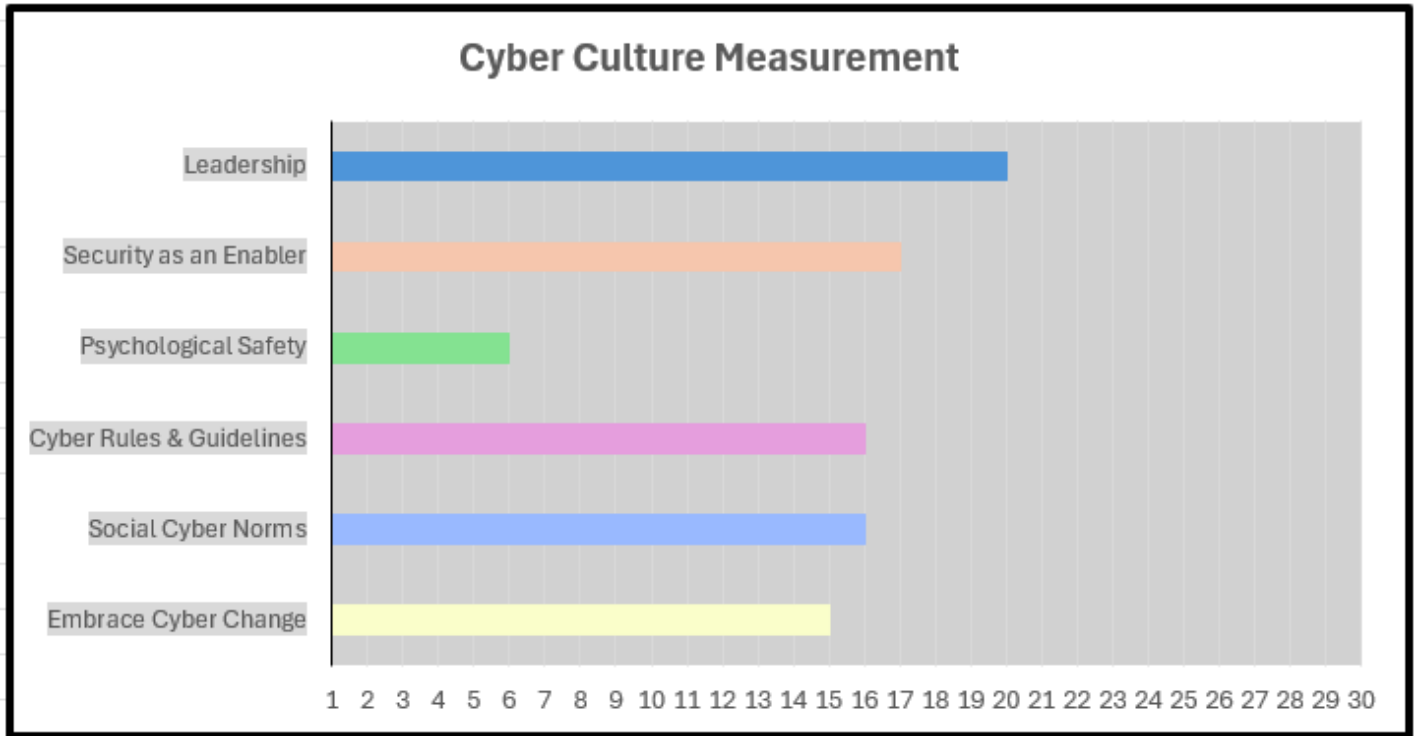
The Cyber Culture Metrics Assessment Tool is here

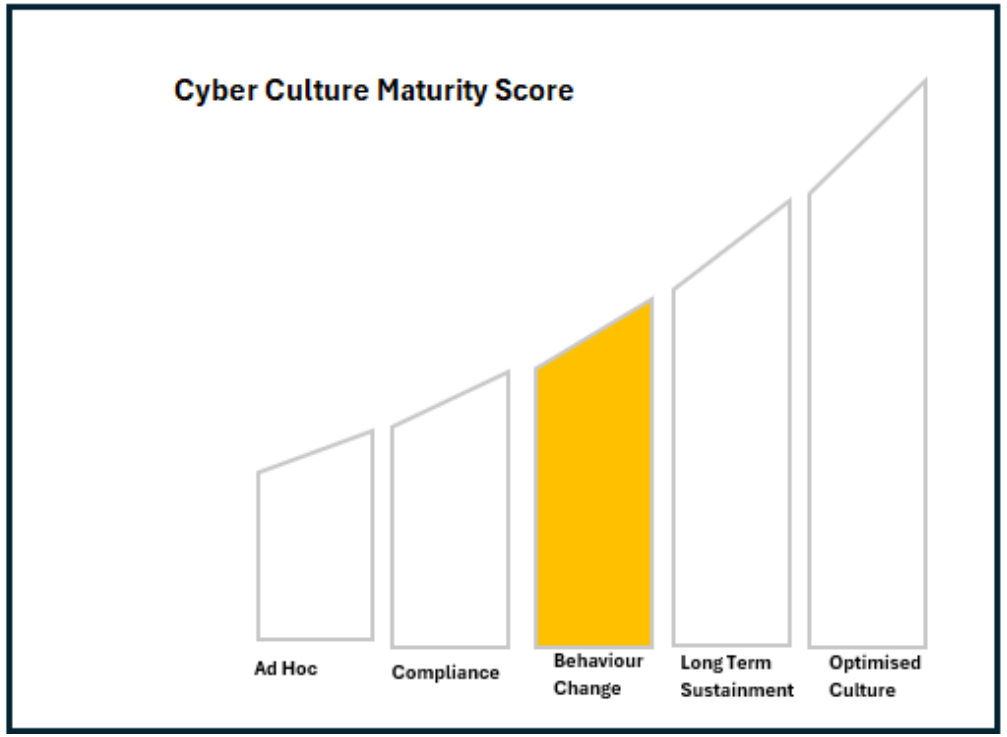


CCMM Measurement Score

AUSCERT

Total Score 90



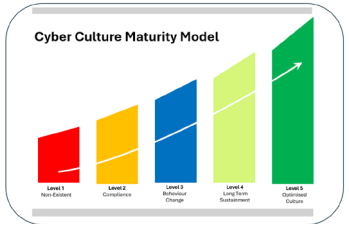


CCMM Reference

The CCMM reference provides a:

CCMM Label & Description, Value, Program & People Indicators, Behavioural Analysis and Steps to Next Level

Cyber Culture Maturity Model Reference					
Category	Level 1 Ad-Hoc	Level 2 Compliance Focused	Level 3 Promoting Awareness & Behavioural Change	Level 4 Long Term Cultural Change	Level 5 Optimised Culture and Resilience
Label	**Basic awareness foundation**	**Meeting minimum obligations**	**Reduced human risk**	**Security embedded into operations**	**Organisational resilience and measurable value**
Description	No formal security awareness program exists. Employees are largely unaware of cyber risks, expectations, or reporting responsibilities. Security communication and leadership support are largely absent.	Program exists primarily to meet audit or compliance requirements; training is often ad hoc or once a year with minimal expectations.	The program actively targets behavioural change by focusing on high risk behaviours and ongoing reinforcement. Security messaging becomes continuous and intentional.	Security awareness becomes embedded into organisational culture. Shared beliefs and expectations around security emerge, and cyber security becomes part of everyday decision making. focusing on shared beliefs and attitudes rather than just individual behaviours.	The most advanced level where the program is fully integrated into organisational strategy and shows clear, measurable impact. Security awareness and culture are fully integrated into business strategy. Leadership receives measurable insights linking culture, behaviour, and organisational resilience.
Value	Very limited value as the absence of a program creates significant risk and vulnerability to social engineering. High exposure to human related incidents and likely non-compliance with standards. The key potential value is in recognising the gap and creating a starting point for improvement.	Meets minimum compliance requirements and establishes basic program structure. Ensures regulatory obligations are met and establishes a basic structure for future strategic growth, and creating an opportunity to transition toward strategic risk reduction.	Demonstrable reduction in human related risk. Improved employee engagement, increased reporting, and early evidence of safer behaviour. Noticeable improvements in secure daily practices. Establishes foundations for culture change.	Security becomes proactive rather than reactive. Staff seek guidance early, secure behaviours become normalised, and trust between teams improves significantly. Security is integrated into daily decision making, technical controls become more effective.	Security culture becomes a strategic organisational asset. Awareness supports resilience, business priorities, and long term adaptability to evolving threats and regulatory changes. Leadership sees the direct connection between culture and risk reduction; the organisation adapts confidently to new threats.
Program Indicators	No formal program in place; security is not discussed or supported by leadership. No structured communications or training.	No strategic plan, limited leadership support, part time ownership and minimal collaboration with other areas of the business.	Leadership involvement. A full time program lead, behaviour driven training, messaging and cross department collaboration. Leadership understands human risk and assigns a dedicated awareness lead.	Strong Executive sponsorship, dedicated team of professionals, annual formal program reviews, security integrated into onboarding and workflows, active champion/advocate networks.	Integrated with business strategy; continuous measurement and optimisation, alignment with standards and frameworks and/or and benchmarking against peers, tailored executive reporting.
People Indicators	Employees are unaware of expectations and rarely demonstrate secure behaviours. Security decisions based on personal judgement. Secure behaviours rarely demonstrated.	Low engagement, employees view training as a requirement. Policies seen as disconnected from daily work, risky shortcuts common	Employees recognise security responsibilities; active reporting of suspicious activity, adoption of secure behaviours at work and home. Increased phishing and incident reporting. Staff actively engage in discussions.	Peer to peer reinforcement of secure behaviours, teams proactively seek security advice, open reporting culture, Staff suggest process improvements, sense of shared responsibility, proactive engagement with security teams, open communication about mistakes.	Shared accountability for risk; leaders use insights for strategic input and resource allocation, high Staff confidence and resilience, Staff confidently recognise/respond to threats.
Behavioural Analysis	Tracking completion of foundational tasks, such as initial training or policy acknowledgment. Policy acknowledgements. Number of basic awareness communications. Program ownership assigned.	Percentage of employees completing annual training, number of awareness materials distributed, number of training sessions. Training completion rates, policy acknowledgement rates.	Phishing click and report rates, MFA/password manager adoption, frequency of policy violations, malware incident rates, Secure data handling incidents, lost/stolen device statistics.	Security culture survey results, requests for security engagement/support, number of Staff improvement suggestions, participation in optional security events, feedback regarding security support and policies. Surveys measuring security beliefs and perceptions; number of requests for briefings.	Number of security incidents over time, organisation trust/reputation, time to detect/recover, correlation between behaviour and incidents, security incident trends over time, compliance violation trends, industry benchmark comparisons.
Steps to Next Level	Lay groundwork by identifying regulations, assigning responsibility for a program, and creating initial training materials. Identify compliance obligations and standards. Define awareness requirements. Assign program ownership Create or source foundational training. Communicate baseline expectations. Track completion and acknowledgement activities.	Shift focus to risk, engage leadership for executive support and a strategic role, assign a dedicated owner; and identify top human risks. Create a formal program charter, define desired secure behaviours, build communication and reinforcement plans.	Shift from individual behaviour to shaping collective attitudes; increase leadership visibility and expand to Champion networks. Simplify policies, integrate awareness into operational activities and improve collaboration across business areas.	Strongly align culture with business objectives and strategic functions; deepen leadership engagement with cultural insights. Develop unified behavioural/cultural dashboards, align metrics with frameworks, standardise culture expectations across business units. Increase business-security engagement. Continue refining communications and reinforcement.	Maintain through continuous refinement, adjusting messaging and measurement as threats and business needs evolve. Maintain unified dashboards, use insights in Executive decision making to ensure effective resourcing, continuously refine training and communications, monitor emerging risks, sustain cross functional collaboration.



Implementation

Cyber Culture Goals

Key Performance Indicator s (KPI's)

Metric Measurement

Metric Measurement

Metric Measurement

Metric Measurement

Delta

Gap Treatment Plans

Improvement

Figure 4 - Measurement of cyber culture will invariably create iterative gap (risk) treatment plans

Summary

- Cultural resilience sustains behaviour
- Behaviour and culture can be measured against goals for improvement – there is no one size fits
- Applying a consistent process and re-measuring parodically is best practice

Reference

UK National Cyber Security Centre
The SANS Security Awareness & Culture Maturity Model
Cyber Health Check Tool | Cyber.gov.au
Cyber Security Culture in organisations | ENISA
DVMS Institute Culture Assessment Tool
Culture Assessment | SANS Institute
Praxis Navigator
Institute of Community Directors Australia | Cyber security...
Security Culture Tool | Security Culture | NPSA
Determining Cyber Security Culture Maturity and Deriving Verifiable Improvement Measures
Towards a cybersecurity culture-behaviour framework: A rapid evidence review – ScienceDirect
Security Culture | KnowBe4

Q& A