AXELOS
GLOBAL BEST PRACTICE

CYBER RESILIENCE: THERE'S NO TIME TO WASTE

AXELOS.com

Balancing opportunity and risk

The opportunities

$4.2 trillion

estimated value of the internet economy in G20 economies by 2016

13.5% to 23%

projected rise in consumer purchases via the internet from 2010-2016

94%

of businesses with 10+ employees are online

4.1%

of GDP contributed by internet

936 exabytes

growth in global internet traffic from 2005-2015

The risks

$445 billion

cost of cyber-crime to the global economy per year

44%

increase in cyber incidents - 1.4 per organization per week

95%

of cyber attacks succeed because of the unwitting actions of a member of staff

$145

average cost paid for each lost or stolen file containing sensitive or confidential information

The risks are real

…why is Cyber Resilience important?

Material impacts

Risk and responsibility

Situational awareness

We all have a role to play

Common statements

AXELOS GLOBAL BEST PRACTICE

“Why would anyone want to attack our organization?”

“We do not know what our most critical information assets are in our organization.”

“We have our networks well protected by good technology”

“Our current information security training is ineffective in driving new behaviour across organization.”

“We know we have already been attacked but do not know how best to respond and recover effectively.”

“We do not know what good cyber resilience looks like for our organization”

What are the strategic challenges?

Our people are our strongest asset but…

No-one is safe

Mind the language gap

Threats are constantly adapting and more targeted

Compliance does not = security

CONSEQUENCES: reputation, cost and competitive advantage

Known needs

We need to develop a coherent cyber resilience strategy

We need to know what our critical information assets are

We need a cyber smart workforce and partner network

We need to embed good practices across our organization

We need to communicate and understand more effectively across the organization

We need to understand how we will respond and recover from attack more effectively

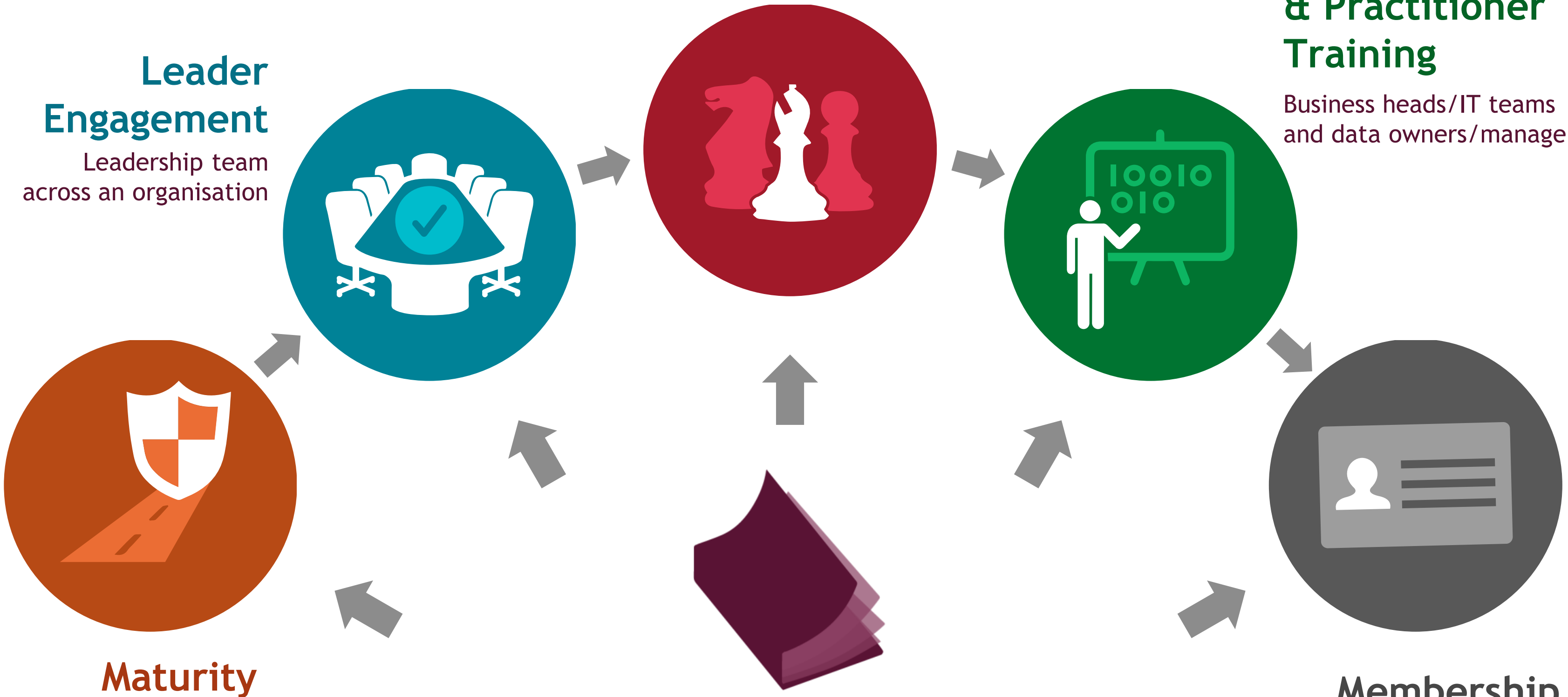
What is Cyber Resilience?

Cyber Resilience is the ability for an organization to resist, respond and recover from threats that will impact the information they require to do business.

...many are struggling to answer...

...what does good look like?

Cyber Resilience Portfolio



Maturity Pathway Tool

Leaders of the organisation

Leader Engagement

Leadership team across an organisation

Individual Awareness Learning & Know-how

All staff across an organisation

Foundation & Practitioner Training

Business heads/IT teams and data owners/managers

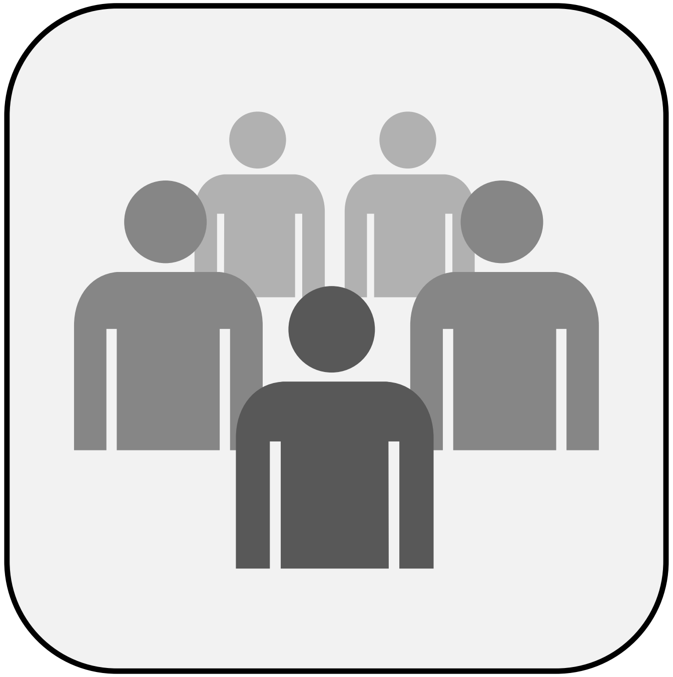
Membership & CPD

IT teams and data owners/managers

Best Practice Guide

Core practical guidance for strategy, implementation and management: “what good looks like”

Target markets and audiences



Key target sectors:

- Critical infrastructure: Energy, Financial services, Health, Utilities, IT/Telecoms, Federal government
- Other: Retail, NGOs, Manufacturing/Hi-Tech, Construction, Education, Professional Services

Target buyers/influencers:

- VP/Head of ITSM
- VP/Head of HR or Learning & Development
- VP/Head of IT, Security or CISO
- VP/Head of Risk and/or Compliance

We want to target:

- Large and medium sized organizations – commercial and federal

Cyber Resilience Best Practice Guide

“Practical information for IT and business staff to better understand the risks and benefits of Cyber Resilience - with practical guidance on assessing, deploying and efficiently managing good Cyber Resilience within business operations.”

The principles

Applicable to all organizations across commercial and public/federal sectors

Alignment with common approaches and standards

Focus on improving organization resilience

Background of complex multi-party and multi-system transactions define the cyber landscape

The structure

Lifecycle structure for cyber follows ITIL

Scope covers entire organization

Guidance covering people, process and technology

Concepts and guidance

The detail

Aimed at those responsible for IT, security, risk and resilience

Extensive practical management guidance

Framework for assessing the right

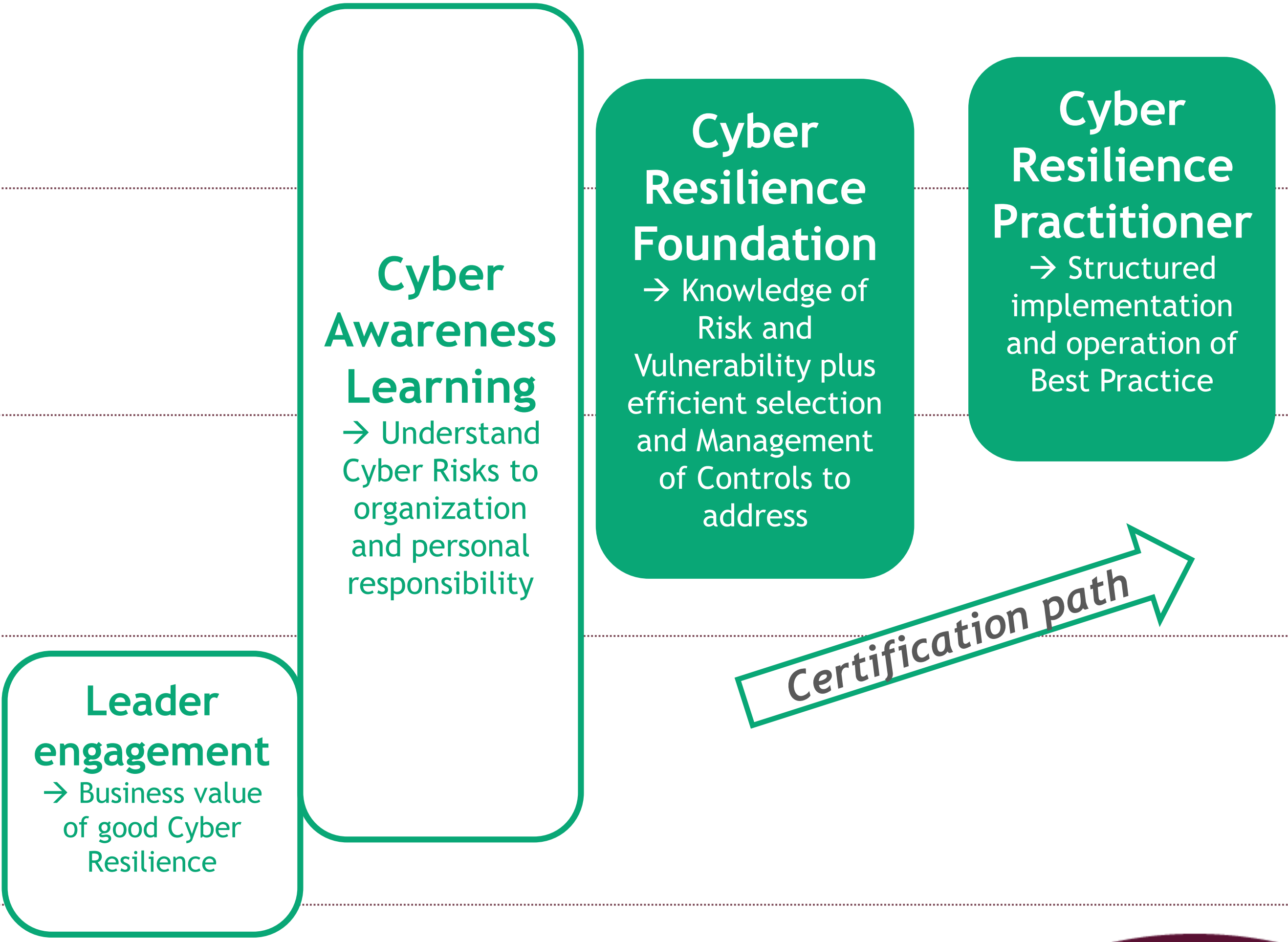
Targeted learning across organization

InfoSec & Risk
Security Ops
Info Assurance
Risk Management

IT & SM
Service Operations
IT Dev (& DevOps)
Architects
Bus analysis
Project Management

Business
Finance & HR
Sales &
Marketing
Customer service
Operations

Exec
CxO
Business strategy
Department
Heads



Leader engagement
→ Business value of good Cyber Resilience

Cyber Awareness Learning
→ Understand Cyber Risks to organization and personal responsibility

Cyber Resilience Foundation
→ Knowledge of Risk and Vulnerability plus efficient selection and Management of Controls to address

Cyber Resilience Practitioner
→ Structured implementation and operation of Best Practice

Cyber Resilience Certification Training

	Course structure	Target audience	Learning outcomes
Cyber Resilience Foundation	**3** day classroom course or **20** hours of distance learning, optional simulation to start course, Foundation certification multiple choice exam	Complete IT team Basic understanding of general cyber security Good understanding of IT and business goals	How decisions impact good/bad Cyber Resilience Comprehensive approach across all areas How to make good Cyber Resilience an efficient part of business and operational management
Cyber Resilience Practitioner	**2** day classroom course or **15** hours of distance learning, optional simulation to start course, Practitioner certification multiple choice exam, bundled with Foundation as a 5 day course	Similar to Foundation but skewed to more experienced roles Complete IT team Good understanding of cyber security Good understanding of IT	What effective Cyber Resilience looks like Pitfalls, risk and issues that can easily hit Cyber Resilience Getting the best balance of risk, cost, benefits and flexibility within an organization

Why do security awareness programmes typically fail?

Reliance on checking the box

Failure to acknowledge that awareness is a unique discipline

Lack of engaging and appropriate materials

Metrics are not collected

Unreasonable expectations

Reliance on a single training exercise

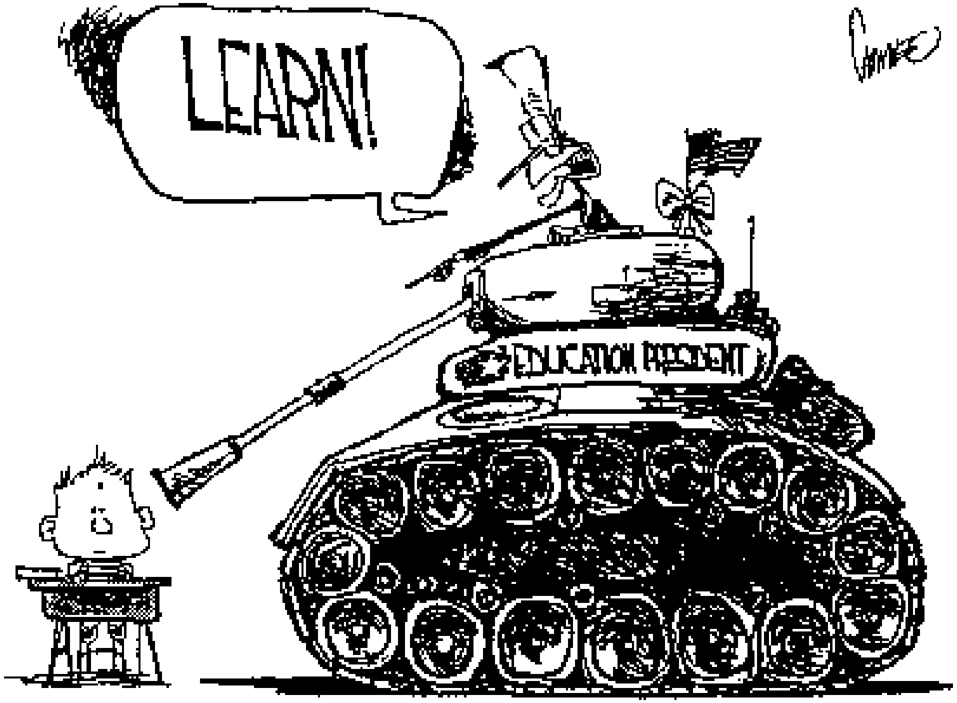
When does awareness learning 'stick'?

"Tell me and I forget,
Teach me and I remember,
Involve me and I learn."

Benjamin Franklin

"Everybody can learn, just not on the same day or in the same way"

George Evans



© 1991 CAMUSO – SYRACUSE-HERALD JOURNAL

Our Awareness learning principles

Principle	Summary and benefits
On-going, regular learning	• Regular learning • Short and concise • Supporting updates and refreshers
Adaptive & personalised	• Suit individual learning preferences • Content tailored to different skill levels • Focus on the priority security issues
Engaging, competitive and fun	• Different learning styles and formats • Ability to learn inside and outside work • Play to the competitive element of games
Measurable benefit	• Tracking changing behaviours over time • Qualitative and quantitative metrics • Demonstrate value of investment

Our Awareness learning

Learning areas

- Phishing
- Social engineering
- BYOD
- Password safety
- Personal information
- Information handling
- Remote and mobile working
- Online safety
- Social media
- Removable media

…role based and sector specific learning

Learning formats

- Gamification
- Animations
- Video
- eLearning
- Posters
- Refreshers/Reminders

…part of an ongoing campaign to influence and measure the impact of new behaviours

Evangelists and early adopters!

Test

Learn

Adapt

June launch

Live events

Panel discussions

Game playing

Interaction

Innovation and creativity

Networking

Questions and observations?

Nick Wilding
Head of Cyber Resilience, AXELOS
E: nick.wilding@axelos.com T: 07860 950108