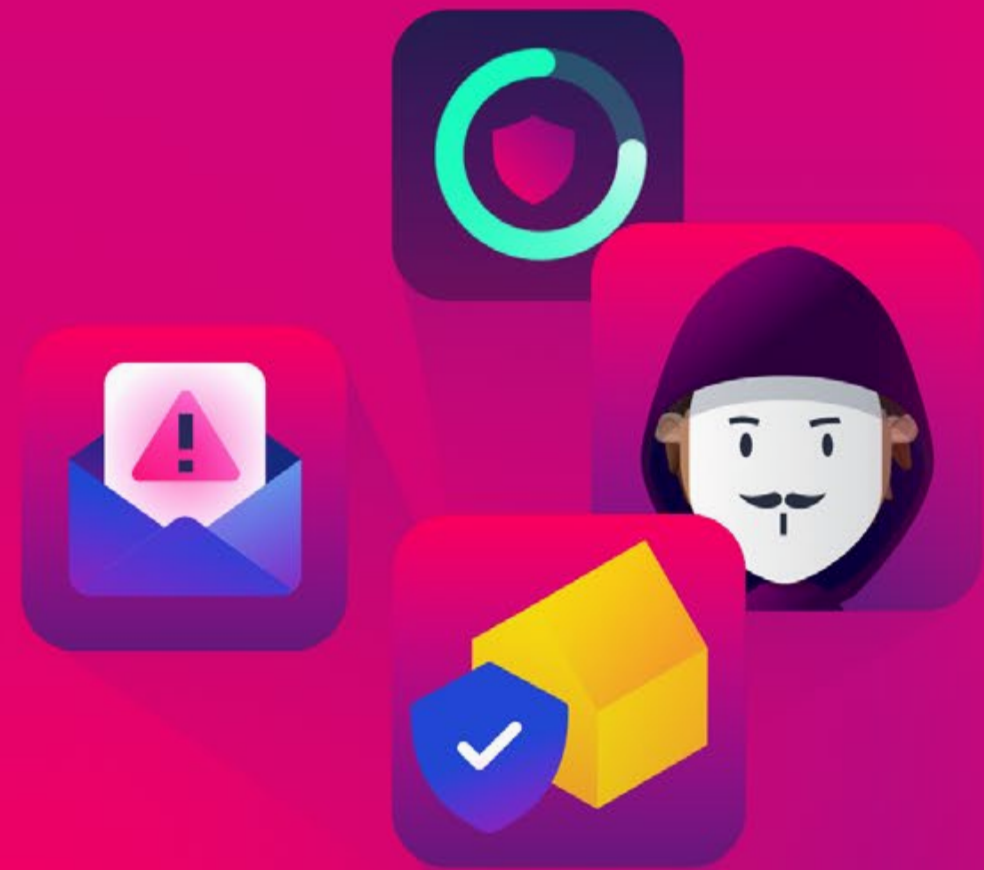




Checklist Cyber Resilience Learning

How security and L&D teams can build cyber learning
that is risk-relevant, engaging, and measurable

Cyber resilience is a shared challenge.

Security teams understand the risks employees face. L&D teams understand how people learn, retain information, and change behaviour. But strong cyber awareness programmes will need both.

Use this checklist to align CISOs, security awareness managers, and L&D leaders around a more effective approach to cyber resilience learning.



Cyber resilience learning: What good looks like

A resilient workforce is not built solely off the back of awareness content. Employees need realistic practice, clear reporting expectations, continuous reinforcement, and learning experiences that help them act well when something feels suspicious.

Together, they build resilience

Strong programmes connect cyber risk with learning design. They help employees recognise threats and then respond appropriately and quickly.

This checklist helps you assess whether your current cyber learning approach is:

- Relevant to the modern-day threats your organisation faces
- Engaging enough to hold people's attention
- Designed to support behaviour change
- Reinforced beyond one-off training
- Measurable in ways that matter to security and L&D
- Clear about reporting expectations
- Credible for senior stakeholders

The shared model

Security defines the risk

CISOs and security teams should clarify:

- Which human-risk behaviours matter most
- Which employee groups are most exposed
- Which threat scenarios are becoming more common
- Which reporting behaviours need to improve
- What evidence is needed for leadership, audit, or compliance conversations

L&D shapes the learning

L&D teams should clarify:

- How to make cyber learning engaging and accessible
- How employees will practise decision-making, not just absorb information
- How learning will be reinforced over time
- How content will fit into the flow of work
- How learning transfer and behaviour change will be supported

The cyber resilience learning checklist

How many statements can you confidently check off?

1. Risk relevance

- ☐ Have we identified the human-risk behaviours that matter most to the organisation?
- ☐ Do our scenarios reflect current phishing, impersonation, and social engineering tactics?
- ☐ Are high-risk roles or departments given relevant examples?
- ☐ Does our training reflect realistic pressure, urgency, and ambiguity?
- ☐ Are AI-enabled threats included where they are genuinely relevant, without turning the programme into hype?

Why it matters:

Cyber learning is more effective when employees recognise situations they may actually face in their day-to-day roles. Generic advice is less likely to change behaviour.

2. Learning engagement

- ☐ Is the learning experience engaging enough for busy employees?
- ☐ Does it use realistic stories, scenarios, or decisions rather than passive instruction alone?
- ☐ Does it avoid fear, blame, and technical overload?
- ☐ Is the content accessible to non-specialists?
- ☐ Does it help employees understand why their actions matter?

Why it matters:

Employees are more likely to remember and apply cyber guidance when the learning feels relevant, relatable, and practical.

3. Behavioural practice

- ☐ Do employees practise what to do when a threat is not obvious?
- ☐ Does the training include decision points, consequences, and feedback?
- ☐ Are employees asked to judge context, not just spot basic warning signs?
- ☐ Does the programme support confidence as well as knowledge?
- ☐ Are common workplace scenarios included, such as supplier requests, payment changes, executive impersonation, or data-sharing pressure?

Why it matters:

Knowing about cyber risk is not the same as responding well under pressure. Practice helps close the gap between awareness and action.

4. Reporting culture

- ☐ Do employees know exactly how to report suspicious activity?
- ☐ Is reporting encouraged even when employees are unsure?
- ☐ Does the organisation avoid blame-based messaging?
- ☐ Do employees receive feedback or reassurance after reporting?
- ☐ Are reporting behaviours measured and discussed as part of programme success?

Why it matters:

Reporting is one of the clearest signs of workforce cyber resilience. Employees need clarity and confidence in a reporting process, when one is in place.

5. Continuous reinforcement

- ☐ Is cyber learning reinforced throughout the year?
- ☐ Are key behaviours revisited in different formats?
- ☐ Does reinforcement connect to current threats or organisational priorities?
- ☐ Are managers or team leaders supported in keeping cybersecurity visible?
- ☐ Does reinforcement feel useful rather than repetitive?

Why it matters:

A single annual module is unlikely to change long-term behaviour. This is where reinforcing key principles helps employees retain and apply what they learn.

6. Measurement and evidence

- ☐ Do we measure more than completions and quiz scores?
- ☐ Do we track reporting behaviour, engagement, and improvement over time?
- ☐ Can we show whether employees are becoming more confident in recognising and reporting threats?
- ☐ Can security and L&D agree what success looks like?
- ☐ Can we explain progress clearly to senior stakeholders?

Why it matters:

CISOs need evidence of risk reduction. L&D leaders need evidence of learning impact. A shared measurement model helps both.

7. Governance and stakeholder alignment

- ☐ Is cyber resilience learning connected to wider cyber risk, compliance, or governance priorities?
- ☐ Are security, L&D, risk, and compliance teams aligned on objectives?
- ☐ Does senior leadership understand the behavioural goals of the programme?
- ☐ Can the programme support conversations around cyber hygiene, AI literacy, and operational resilience?
- ☐ Is there a clear owner for continuous improvement?

Why it matters:

Cyber resilience learning is more credible when it is linked to business risk, workforce behaviour, and leadership accountability.

Quick scoring guide

For each section, count how many statements you can confidently tick.

>25

Mostly ticked

Your programme is likely moving beyond awareness and towards workforce cyber resilience. Focus next on measurement, reinforcement, and continuous improvement.

>15

Some gaps

Your programme may have strong foundations, but it may still rely too heavily on training activity rather than broader behaviour change. Prioritise the areas where security and L&D are least aligned.

<10

Many gaps

Your organisation may need to rethink its approach. Start by defining the human-risk behaviours that matter most, then design learning that helps employees practise and reinforce those behaviours.

Discussion prompts for security and L&D teams

Use these questions as the basis of a joint planning session:

1. What are the top three human-risk behaviours we need to reduce?
2. Which employee groups face the most realistic exposure?
3. Where do employees hesitate, misunderstand, or fail to report?
4. What does good behaviour look like in a real incident?
5. How can learning make those behaviours easier to practise?
6. What should we measure beyond completion?
7. How will we keep cyber resilience visible throughout the year?



Practical next steps

For security leaders

- Define priority human-risk scenarios
- Clarify reporting behaviours and escalation routes
- Identify the evidence needed for leadership and governance
- Share threat context with L&D in practical, non-technical language



For L&D leaders

- Translate risk into realistic learning moments
- Use stories and scenarios to make cyber decisions memorable
- Build reinforcement into the learning calendar
- Measure engagement, confidence, and application of knowledge, not just completion



For both teams

- Agree shared success measures
- Review the programme quarterly
- Keep content current as threats and working practices change
- Treat cyber resilience as an ongoing capability, not a one-off campaign



Where Cyber Crime Time fits in

Cyber Crime Time supports organisations that want to move from one-off awareness training towards more immersive cyber resilience learning.

Through story-driven scenarios and continuous reinforcement, Cyber Crime Time helps employees practise how to recognise, respond to, and report modern cyber threats, including phishing, social engineering, deepfakes, and AI-enabled attacks.

It gives security teams a more practical way to address human risk and gives L&D teams a more engaging way to support behaviour change.

Want to see how immersive, story-led cyber learning can support your security and L&D goals?

[Explore Cyber Crime Time](#)[Book a demo](#)

more than technology

information multimedia communication AG

Scheer Tower
Uni-Campus Nord
66123 Saarbrücken

T. +49 681 9476-0
info@im-c.com

Scheer IMC worldwide

Germany (Saarbrücken,
Freiburg, München)
Australia (Melbourne)
UK (London)
Austria (Graz)
Romania (Sibiu)
Switzerland (Zürich)
Singapore
The Netherlands (Vianen)
USA (Dover)

About Scheer IMC

Scheer IMC is an elearning technologies leader with over 25 years of experience. As a full-service provider, it offers cutting-edge training platforms, learning content, and strategic L&D expertise for global brands to achieve complex learning goals. Founded in the late 1990s by IT visionary Professor August-Wilhelm Scheer, imc AG originated out of a pioneering university education project.

Headquartered in Saarbrücken, Germany, the company today boasts a team of 400+ employees at 12 locations worldwide. As a trusted enterprise learning pioneer, Scheer IMC has transformed learning for over 10 million learners at 1,300+ organisations. Driven by bold innovation, imc goes beyond technology to deliver human-centred, award-winning, and impactful learning experiences.

Find out more at

scheer-imc.com