Building a Culture of Cybersecurity

Best For

This program is ideal for:
Professionals across all departments
Team leads, managers, and supervisors
Employees involved in day-to-day digital operations
Organizations aiming to strengthen cybersecurity beyond technology

Delivery Style

The learning experience is awareness-driven, behavior-focused, and designed to help professionals understand how everyday actions, attitudes, and decisions collectively shape an organization's cybersecurity posture.

Outcome Level

Participants develop a shared sense of responsibility for cybersecurity, improved security-aware behavior, and the ability to contribute positively to a strong, sustainable security culture.

Program Positioning

Cybersecurity is not just a technical issue — it is a **people and culture challenge**. Even the most advanced security systems can be undermined by poor awareness, unsafe habits, or lack of accountability.

This program is designed to help professionals understand **how culture influences cybersecurity outcomes**. It focuses on mindset, communication, accountability, and everyday behavior rather than technical controls.

The program supports organizations across the USA, Canada, Australia, and global markets where regulators, customers, and leadership increasingly expect a visible, organization-wide commitment to cybersecurity.

✅ Ideal for professionals with 0–20 years of experience
✅ Ideal for organizations strengthening long-term cybersecurity resilience

LEARNING STRUCTURE (8 HOURS)

Block 1 — Understanding Cybersecurity as a Shared Responsibility

This session builds a strong foundation by explaining why cybersecurity is everyone's responsibility, not just the IT or security team's role.

It covers:

- Why technology alone cannot prevent breaches
- How human behavior impacts security outcomes
- Shared accountability across roles and levels
- The cost of weak security culture

✅ **Outcome:** Clear understanding of collective cybersecurity responsibility.

Block 2 — The Role of Behavior, Attitudes & Habits

This session focuses on how daily habits shape cybersecurity outcomes over time.

It covers:

- Secure vs insecure workplace behaviors
- How shortcuts create long-term risk
- Importance of consistency and discipline
- Reinforcing positive security habits

✅ **Outcome:** Increased awareness of behavior-driven security risk.

Block 3 — Leadership Influence & Cybersecurity Culture

This session explores how leadership behavior sets the tone for cybersecurity across teams.

It covers:

- Role modeling secure behavior
- Encouraging open communication about risks
- Avoiding blame culture
- Supporting accountability without fear

✅ **Outcome:** Stronger leadership contribution to cybersecurity culture.

Block 4 — Communication, Awareness & Engagement

This session highlights how communication strengthens security awareness across organizations.

It covers:

- Clear messaging around security expectations
- Encouraging questions and reporting
- Making security relevant and understandable
- Sustaining awareness over time

✅ **Outcome:** Improved engagement and security communication.

Block 5 — Learning From Incidents & Near Misses

This session emphasizes learning rather than blame when incidents occur.

It covers:

- Treating incidents as learning opportunities
- Sharing lessons responsibly
- Preventing repeat mistakes
- Improving processes and behavior

✅ **Outcome:** Healthier, learning-oriented security mindset.

Block 6 — Empowering Employees to Speak Up

This session focuses on building confidence to report concerns without fear.

It covers:

- Removing fear and hesitation
- Encouraging early reporting
- Supporting employees who raise concerns
- Building trust in response processes

✅ **Outcome:** Stronger reporting culture and trust.

Block 7 — Aligning Security With Business Goals

This session helps participants understand how cybersecurity supports business continuity and reputation.

It covers:

- Linking security to trust and credibility
- Protecting customers and stakeholders
- Supporting long-term business success
- Understanding reputational impact

✅ **Outcome:** Better alignment between security and business objectives.

Block 8 — Cybersecurity Culture Action Plan

This final session helps participants apply cultural principles in daily work.

It covers:

- Identifying cultural strengths and gaps
- Reinforcing positive security behaviors
- Supporting peers and teams
- Creating a personal cybersecurity culture action plan

✅ **Outcome:** Clear, practical plan to support a strong cybersecurity culture.

✅ What You Will Walk Away With

Participants complete the program with:
Stronger understanding of cybersecurity culture
Improved security-aware behavior
Greater confidence reporting concerns
Reduced risk from human-factor vulnerabilities
A structured approach to building security culture
A Knowledge Que Course Completion Certificate (8 PDUs)

✅ Certification (Delivery-Neutral & Legally Safe)

On successful completion of the program, learners receive:
Knowledge Que – Course Completion Certificate
Recognition of 8 Professional Development Units (PDUs)
A digital certificate suitable for:
LinkedIn
Resume & Portfolio
Professional Profiles
Issued by Knowledge Que – Powered by Experts

✅ Why Knowledge Que

Expert-led, practical professional skills training
Real-world workplace cybersecurity scenarios
Skill-focused learning with immediate application
Programs designed specifically for modern professionals

Copyright