Insider Threats Awareness

Best For

This program is ideal for:
Early to mid-career professionals
Employees with access to systems, data, or sensitive information
Team leads and managers overseeing people, data, or processes
Organizations strengthening internal risk awareness and trust

Delivery Style

The learning experience is awareness-driven, behavior-focused, and designed to help professionals understand insider risks without blame, fear, or technical complexity.

Outcome Level

Participants develop stronger awareness of insider-related risks, improved judgment around access and behavior, and the ability to prevent security incidents caused by internal actions — intentional or unintentional.

Program Positioning

Not all security threats come from outside the organization. Many incidents originate **inside** — through human error, negligence, misuse of access, or, in rare cases, malicious intent.

Insider threats are especially damaging because they often involve **trusted access**, familiarity with systems, and knowledge of processes. This program is designed to help professionals understand how insider threats occur, recognize early warning signs, and act responsibly without creating fear or suspicion.

The program emphasizes **awareness, accountability, and prevention**, supporting organizations across the USA, Canada, Australia, and global markets where internal risk management is a growing priority.

✅ Ideal for professionals with 0–20 years of experience
✅ Ideal for organizations strengthening internal security culture

LEARNING STRUCTURE (8 HOURS)

Block 1 — Understanding Insider Threats in the Workplace

This session builds a strong foundation by explaining what insider threats are and why they present unique risks compared to external attacks.

It covers:

- What insider threats mean in workplace contexts
- Why trusted access increases risk
- Types of insider-related incidents
- Difference between malicious and unintentional threats

✅ **Outcome:** Clear understanding of insider threat fundamentals.

Block 2 — Types of Insider Threats

This session helps participants understand the different forms insider threats can take.

It covers:

- Unintentional insider threats caused by mistakes
- Negligent behavior and poor security habits
- Misuse of access or privilege
- Intentional insider actions

✅ **Outcome:** Improved ability to categorize insider risk types.

Block 3 — Common Insider Risk Scenarios

This session focuses on real-world situations where insider threats often arise.

It covers:

- Oversharing information internally
- Inappropriate data access
- Bypassing controls for convenience
- Poor handling of sensitive data

✅ **Outcome:** Better recognition of insider risk situations.

Block 4 — Behavioral Warning Signs & Red Flags

This session strengthens awareness of behavioral indicators that may signal increased risk.

It covers:

- Changes in behavior or attitude
- Repeated policy violations
- Unusual access patterns
- Stress, frustration, or disengagement indicators

✅ **Outcome:** Increased awareness of early warning signs.

Block 5 — Access Responsibility & Privilege Awareness

This session emphasizes responsible use of granted access.

It covers:

- Why access should match job roles
- Risks of excessive privileges
- Sharing credentials and access misuse
- Respecting boundaries of authorized access

✅ **Outcome:** Stronger access-discipline awareness.

Block 6 — Protecting Data From Internal Exposure

This session focuses on preventing internal data exposure.

It covers:

- Secure handling of confidential information
- Avoiding internal data leakage
- Proper data storage and sharing
- Reducing accidental exposure

✅ **Outcome:** Improved data protection behavior.

Block 7 — Reporting Concerns & Supporting Prevention

This session emphasizes the importance of speaking up responsibly.

It covers:

- When and how to report concerns
- Avoiding assumptions or accusations
- Supporting a trust-based reporting culture
- Preventing incidents before escalation

✅ **Outcome:** Increased confidence in reporting insider-risk concerns.

Block 8 — Insider Threat Awareness Action Plan

This final session helps participants apply awareness consistently in daily work.

It covers:

- Identifying personal insider-risk areas
- Strengthening responsible access habits
- Supporting peers and teams
- Creating a personal insider-threat prevention action plan

✅ **Outcome:** Clear, practical plan for preventing insider threats.

✅ What You Will Walk Away With

Participants complete the program with:
Stronger awareness of insider-related risks
Improved judgment around access and behavior
Reduced likelihood of internal security incidents
Greater confidence identifying and addressing risk
A structured approach to insider-threat prevention
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 internal risk scenarios
Skill-focused learning with immediate application
Programs designed specifically for modern professionals

Copyright