Human risk as a compliance driver

Data breaches are among the most expensive in North America, averaging over CA$6M in Canada and $10.22M in the US. With the human element involved in 68% of breaches, security is increasingly judged on verifiable behaviour, policy acknowledgement, and your ability to evidence a security culture to auditors and insurers.

What’s driving requirements

North American regulators, insurers, and enterprise clients increasingly expect continuous evidence, not annual check-box activity:

- **CMMC + SOC 2 assurance**: increasing pressure for documented, repeatable evidence of training and security responsibilities to support contract and customer requirements

- **HIPAA + Canadian privacy obligations (PIPEDA and provincial laws)**: appropriate workforce awareness and verifiable policy acknowledgement

- **Cyber insurance**: insurers often request training logs, phishing results, and policy acceptance evidence during renewal

Where organisations struggle

- Limited IT time to manage ongoing training, policy sign-off, and reporting alongside day-to-day operations
- Outdated annual training that doesn’t stand up to audits or customer reviews
- Policy acceptance scattered across inboxes and folders, making proof hard to produce on demand
- Evidence spread across tools, creating manual work and slowing audits and assurance requests

How We Support Your Compliance Evidence

☑ **Ongoing training + phishing**

Automated programmes with measurable participation and improvement

☑ **Centralised policy management**

Distribute policies and capture eSign acknowledgement in one place

☑ **Human Risk Score + reporting**

Exportable, board-ready outputs for auditors and evidence logs for auditors and stakeholders

☑ **Quick cloud deployment**

Microsoft 365 or Google Workspace sync, no installs

Begin your human-risk review
A short assessment to benchmark your evidence posture and define next steps.

Schedule Your Risk Review