

Solution Positioning Guide

What makes us different?



cyberconIQ Solutions:

cyberconIQ's myQ is a patent-pending assessment tool with a foundation based on trait-based personality theory that provides insight into user behavior and online "style". The assessment can identify specific types of cybersecurity attacks (known as threat vectors) that are more likely to succeed given any individual's particular Risk-Style behavior. These also create the opportunity to consider overall rates of risk for the entire organization by mapping its organizational make-up, or risk DNA, according to the range of people found in each quadrant.

cyberconIQ's uniQue Adaptive Learning Platform is our innovative style-aligned cyber awareness education platform that provides users who have taken the myQ Assessment a more effective, personally curated educational journey to improved cyber awareness.

cybermetrIQs improves cyber risk management by aggregating trusted global data sources into a single dashboard and assists in developing cyber hygiene best practices according to industry standard frameworks (CIS, ISO, NIST).

Key Differentiators for cyberconIQ:

cyberconIQ's Risk Management platform provides insight into an organization's **people, process** and **technical** cybersecurity risks:

- Making them more visible, measurable and manageable
- Addresses the human element of cybersecurity risk by focusing on an employee's individual risk-styles and how they are uniquely susceptible to online threat vectors (**myQ**)
- Reduce the probability of a successful cyber breach by educating more effectively and more efficiently than our competition through style-aligned, personally curated adaptive training (**uniQue**)
- Advancing the risk and compliance culture through empowering, not exhausting clients, by emphasizing cybersecurity as a team sport and cultivating a trust that leads to long-term relationships.
- Innovative risk management platform that integrates behavioural science with cybersecurity framework-based best practices
- Ability to make enterprise risk analysis more "executive-friendly" with single dashboard view (**cybermetrIQs**)
- Tying cybersecurity investments to advancing maturity under NIST, CIS or ISO2700x compliance standards
- Transforming opportunities into ROI and risk-driven business decisions
- Reduce the total cost of a cyber breach through our platform's ability to change on-the-job behavior, as well as the ability to prioritize incidents of concern for CISO's (**cybermetrIQs**)

Qualitative Feedback from Customers RE: **cyberconIQ** Cybersecurity Learning Solution vs Competitors:

- **cyberconIQ's**: "**Adaptive**" approach is a relative benefit.
- Competitors: Administration of cyber security training platforms can be complicated and requires a dedicated administrator often because training needs to be assigned by level, role, etc.
- **cyberconIQ's**: "**Style-aligned**" advantage is that we train **MORE efficient** and **MORE effectively** which **improves productivity**.
- Competitors: More training content does not always translate to quality of content. Training material can be repetitive and often the last tranche of training is simply re-assigned.
- **cyberconIQ**: Continues to receive positive reviews and ratings of **4.71/5 customer satisfaction** rating.
- Competitors: Clients have repetitively mentioned that their associates did not particularly enjoy their cyber security training experience or embrace it.

Our myQ Style Assessment and unIQue Learning Platform:

- Produced **56% more self-reported changes** in on-the-job behavior than generic alternatives,
- Demonstrated **1.6 times better recall** at 30-day retests.
- Generated approximately **40% fewer IOC's (Incidents of Concern)**.
- In select clients, **phishing test failures was reduced by 75%**

What Customers are Saying About **cyberconIQ** Cybersecurity Solutions:

Employees survey showed 90% of the employees agreed that:

- They have a **better understanding** of **what and how** cyberthreats can affect **them**.
- Felt **more confident** in being able to deal successfully with cyberthreats.
- Helped them be **more cyber aware** in their **personal life**.
- Participants **reduced phishing test failures by 75%**

Employees experienced the following after working with our platform:

- Helped understand their **personal vulnerabilities**
- Appreciated the **ease of use, pace** and felt **content was well executed**
- **Resonated** with employees differently than generic training

Employees experienced the following after taking the training:

- **Confidence Levels Increased**
- Reported **Self-Changes in Cyber Behaviour**
- **Increased Recall**