cyberconIQ

PATENTED
PROVEN
PROTECTION

WHITE PAPER

Educating Employees Differently for Improved Compliance Outcomes

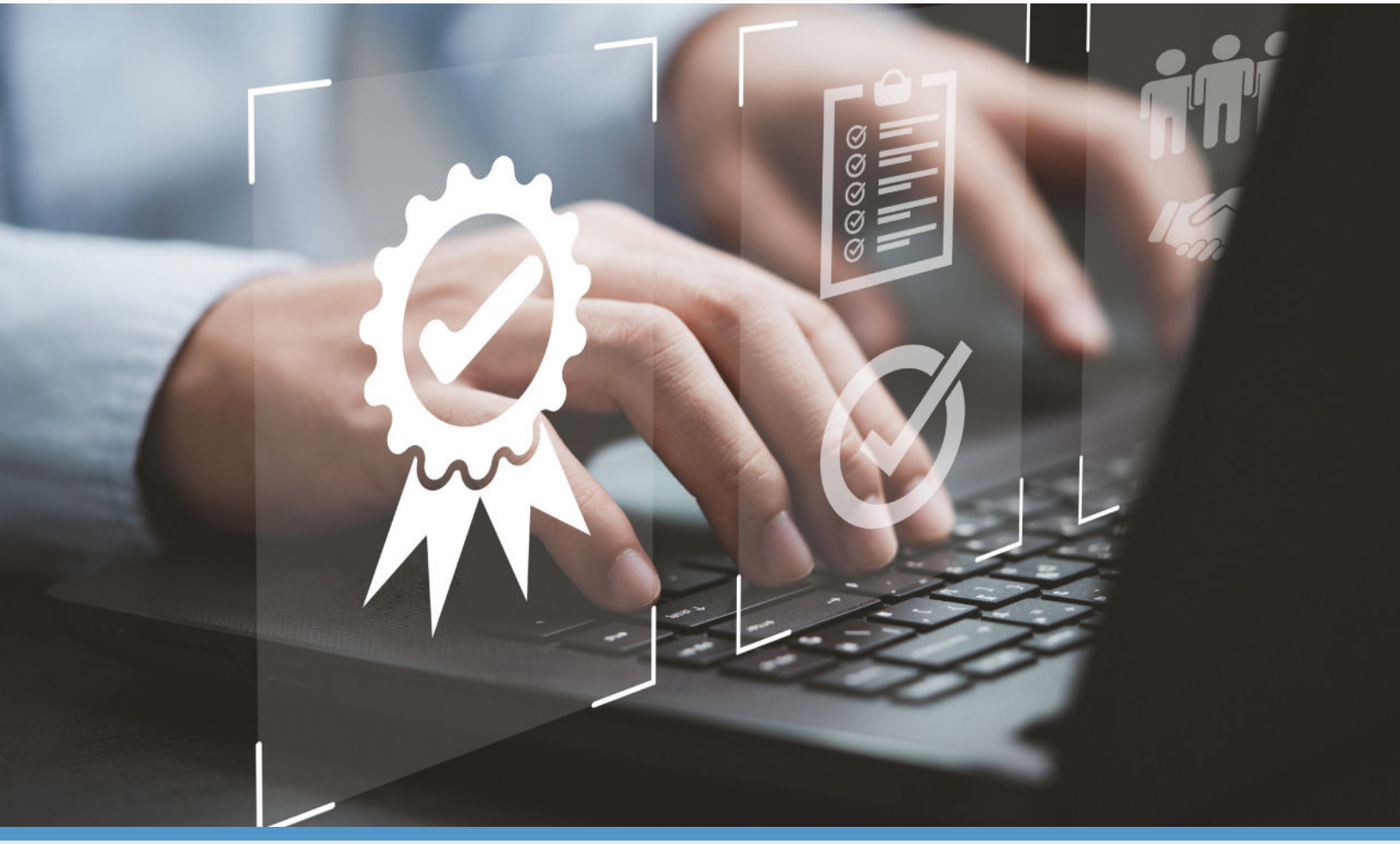
By Dr. James Norrie, Founder & CEO

cyberconIQ

Improving Employee Compliance Outcomes to Benchmark Levels

For years, our team at cyberconIQ have researched the most common dilemma executives face when managing enterprise cybersecurity risk: **how can we enhance employee compliance outcomes?** We know that successful cybersecurity breaches today – studies report more than 80% – rely on a human-factor or accidental insider to succeed. Obviously conventional, often costly, generic Security Awareness Training has failed to offer an effective solution to this problem as it has continued to grow in risk, scope and cost for enterprises of all sizes globally. Our research discovered three main reasons why:

1. Most employees begin with a negative mindset, completing yet another mandatory generic training module, that often casts them as the problem instead of the solution;
2. Content that only trains a person to know versus actually getting them to do it in the moment renders most training of no value unless it prompts a corresponding voluntary change in on-the-job behavior;
3. This "training fatigue" creates lack of engagement that impairs retention and internalization of the content prompting employees to complete assigned training quickly so as to get on with their "real work" instead of a tiresome "compliance task".

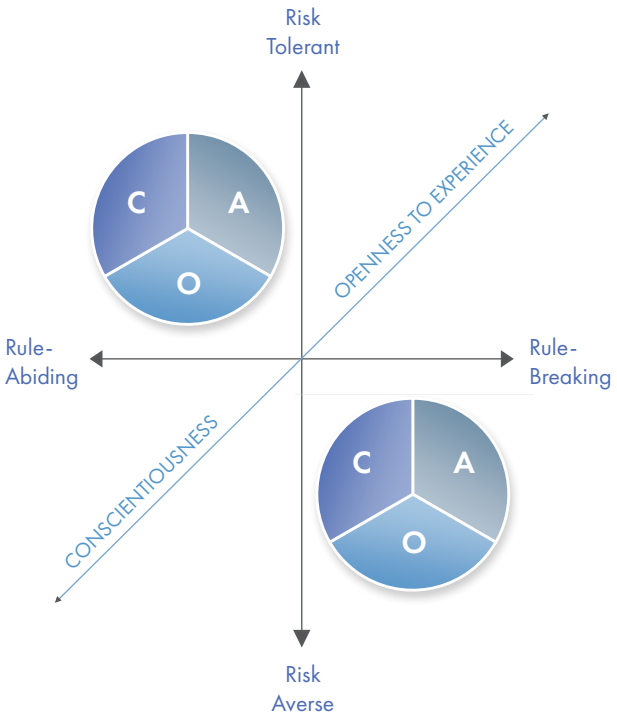


As executives tasked with enterprise risk management, we all know that compliance is every employee's real work regardless of which function, level or in which specific role they operate. We strive to make compliance everyone's business, or else we risk the business. This means cybersecurity is no longer a simple technical problem, but a more complicated employee behavioral challenge.

cyberconIQ has addressed these gaps by understanding how to apply trait-based personality theory through our Human Defense Platform so as to impact how people behave online. We personalize the training experience by tailoring it to individual risk vulnerability, making it more engaging for every employee. This patented method shows a **quantifiable shift** in employees from simply knowing to actually doing. And a growing body of independent client studies offer measurable proof of this outcome, dramatically improving employee security habits and reducing overall cybersecurity risk for our clients. By embedding proven elements of behavioral science across all aspects of our platform, we create unique pathways to **voluntary on-the-job employee behavior change to inspire a more resilient and security-aware culture**.

The original journey to this significant outcome began with a simple research question: could we predict which particular online vulnerabilities were more or less triggering based on particular personality traits?

To our delight, we found we could. In fact, we obtained statistically significant correlations between different personality traits and particular online vulnerabilities. This led to our **US patent** (#11,411,978) on the standardized myQ tool and associated use of its proprietary business processes.



Our patent defines the original idea that risk and reward, and the intention to follow rules or not, are endemic to one's personality, not random occurrences in any particular moment. This makes behavior both predictable and controllable. By creating a pattern of predictability surrounding personal vulnerability to specific attack vectors – what we call ***pathways to compromise*** – we prepare individual employees to avoid being manipulated by outsiders trying to turn them into ***accidental insiders*** whose behavior is then compromising and damaging. While this risk can never be reduced to zero, our platform dramatically reduces the potency of this threat to **benchmark low levels**. This dramatically improved result made us wonder: can this method be applied to other compliance use cases beyond cybersecurity?

Creating Pathways to Compliance

Your Compliance Training Library

From Knowing to Doing

Our behavioral science approach provides a higher rate of compliance than your existing training programs.

The emerging answer is yes. Every organization has a raft of governance, regulatory and compliance (GRC) goals linked to business outcomes it needs to assure for itself and report to stakeholders and regulators. This often means organizations invest significant employee time completing mandatory compliance training. This can include not only Security Awareness Training, but also industry specific training such as Anti-Money Laundering or know your client training in banking, or HIPAA Training for employees working in the healthcare or the health insurance sectors for example. Or perhaps compliance with health and safety protocols, especially in industries such as energy, utilities and manufacturing, where the critical link between compliant employee behavior and both safety and operational availability are crucial goals of your enterprise compliance program?

Regardless of the specific use case, what is apparent and clear is that we need employees to move from knowing to doing, if the important business goals of our compliance programs are to be met. We know that the traditional approach to training has marginal, if any, effect on actual employee behavior. For us, this suggests new methods to instead create meaningful ***pathways to compliance*** that are internally motivated enabling employees to voluntarily comply with policy and procedure. This gradually improves your overall **culture of compliance**, one employee and one style at a time.

How do we know this differentiated approach works better? Recently, a healthcare related client already using our platform to address their cybersecurity needs asked us about using myQ as the front and back end of their existing HIPAA training curriculum. Would it positively impact employee compliance in this application too? The client performed an experiment that divided their employee population into existing employees (trained previously using traditional generic HIPAA training) and newly hired employees, exposing them to a new Style-Aligned® version of HIPAA training. Remarkably, not only did the new employee group report **higher satisfaction** with their training itself – already an important link to voluntary compliance – but over time, this population showed a **lower rate of reportable HIPAA events**. This is a measurable ROI demonstrating higher employee compliance with required procedures and protocols that improved their HIPAA compliance.

This impact mirrors our clients' repeated findings from security and DLP compliance where the myQ tool already broadly supports more consistent employee security compliance resulting in an **improved risk posture while driving down costs**. By aligning training to style, cyberconIQ transforms training into education that produces higher levels of recall, more voluntary changes in employee behavior, and generates a **higher ROI** on your training investment compared to any generic alternative method.

If you want to explore how our Human Defense Platform can help you achieve new levels of certainty around employee compliance behavior, contact us to learn more. Or, if you have an in-house custom compliance training program, consider adding personalization to help you achieve **higher employee satisfaction** and **better results** than any other available method in the market today. Our product and business development teams stand ready to help you deploy both existing and develop custom training solutions to rapidly and measurably improve GRC outcomes across your organization.