cybercon IQ

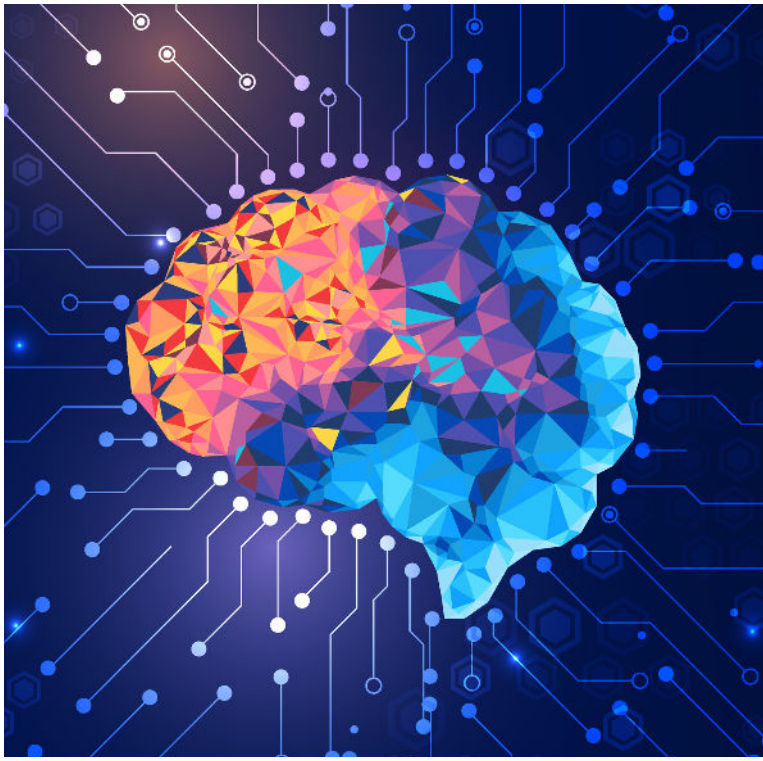
Why We Can Guarantee a Change in Risky On-the-Job Behavior

By Dr. James Norrie, Founder & CEO

How We Reduce Any Organization's Cybersecurity Risk:

Why are we so confident that we can guarantee a dramatic decrease in any organization's cybersecurity risk? And what measurable proof do we have that our solution is statistically superior to any other alternative? It all begins with a simple fact: **we are all different, with our own personalities and tendencies and preferences around risk**.

Each enterprise's cybersecurity program needs to adapt to this obvious fact to succeed. Programs need more sophisticated ways to embed security awareness deeply into daily corporate life, novel methods that **educate employees** about the impact of their own security behaviors, ways to **provoke mindfulness** to **combat situational distractibility**, and consequences that allow management to praise employees when doing things right instead of focusing on their failures. cyberconIQ delivers a proprietary solution that encompasses all that and more.



The Underlying Theory:

New research involving a large-scale study of 1500 people conducted by the University of Basel suggests an individual's propensity to take risks remains stable over time, akin to differences in our personalities and other individual characteristics such as one's Intelligence Quotient (IQ). The findings have been published in leading journals like *Science Advances* and *Nature & Human Behaviour*. Investigators wanted to determine how our risk preferences drive risk-related decisions to determine if risk preference depends on the context or is largely consistent in different situations.

"Our findings indicate that risk-taking propensity has a psychometric structure similar to that of psychological personality characteristics...there is a general factor of risk preference," said Dr. Renato Frey from the University of Basel and the Max Planck Institute for Human Development. "In other words, your willingness to take risks may vary across different areas of your life, but it will always be affected by the underlying general factor of risk preference."

This finding is completely consistent with cyberconIQ's own proprietary research that drew a similar conclusion. Research using the scientific method ultimately led to the development of the patented myQ instrument that we use to assess anyone's online risk style today. We can predict risk appetite, link individual behavior to specific vulnerabilities, and then educate employees about voluntarily changing their security habits to **lower risk**. These relevant personality insights gained from the myQ instrument make this possible.

Isn't This Hard to Do?

Yes, and no. Of course, we expect new prospects and clients to be skeptical of our claims. And they should be. They continually hear claims of distinction and difference from vendors. The market offers hundreds of choices regarding whom they choose to trust to make a difference in their employees' security behavior. And, let's face it, changing vendors is both a hassle and has a cost, right? Nobody will make that decision unless they are very sure they will gain a measurable ROI and superior result.

However, measuring risk propensity is easy. Our tool takes any employee only 8–10 minutes to complete and provides them with personal insights that immediately begin to **change their perspective on their own security behavior**. Employees report this as fun, and providing a level of developmental insight into themselves that makes them safer online at both home and work. When paired with our differentiated education platform, sophisticated assessment methods, and personalized training plan, we can remediate any employees' propensity to fail phishing tests between **45% - 95% within 90 days**. Further, by helping employees get it right, we reduce your need to remediate what they are doing wrong. This positive cycle of empowerment creates a voluntary and sustainable behavior change.

But don't just accept our marketing claims. Accept scientific proof of our difference instead. Here are a few summaries of independent, client-led studies where deploying our platform created an immediate, **measurable reduction in risky behavior that directly reduced cybersecurity costs and risks**.

Continued

Our solution remediates an employees' propensity to fail phishing tests between

45%-95%

within 90 days.

Industry Case Study - Insurance

The insurance industry is driven by actuarial measurement of risk. To offer insurance products, risk needs to be quantified and occur predictably enough that pooling risk to share it makes sense. An insurer's loss ratio determines profitability ultimately, and so tools that are proven to reduce risk are both attractive and offer an immediate return on investment.

Think about your car insurance. While there are many competing companies with different go-to-market brands and strategies, their willingness to offer you lower insurance rates will ultimately depend on the type of risk you represent. To assess this, if you are a new driver, they might offer a discount if you complete a recognized driver education course. This education is proven to mitigate risk. When applying for coverage, the insurer will consider your past driving record and claims experience as a proxy to assess your likely future risk. Or, you might agree to have a device installed in your car that monitors your driving habits in real-time to secure a lower rate due to **proving you are a lower risk to them**.

We apply all of these same concepts to employees' online behavior. Client studies from the insurance industry prove that we **reduced internal phishing failures** from a benchmark national average rate of 15% - 18% after 90 days of training to consistently **less than 2% after only 30 days**. Further, we were able to remediate those who serially fail phishing tests **more than 90%** of the time, with one client experiencing a **100% remediation** of that risky population with just one pass of phishFixIQ, our one-time, low-cost phishing remediation platform. By doing this, we improved their profitability by reducing claims – the **real business ROI** of our solution for them. To be clear, these phishing tests were done using independent tools not managed by cyberconIQ but by our clients. And all benchmark data was collected and assessed independently. Can your current security training vendor claim a similar result?

"Our view is training that does not impact risky behaviors is a waste of time and money for our clients. For us, the goal is to find proven ways to detect and prevent harm which then **lowers the risk of both a security event for our clients and also a future claim**. Our partnership with cyberconIQ accomplishes that."

Kirsten Bay, CEO of Cysurance

Industry Case Study - Global Financial Services

Some of the most sophisticated enterprises in the world are large global banks. These institutions are highly targeted and as a result, have very mature cybersecurity programs.

In 2021, we began a proof of concept with a large Canadian chartered bank, among the top 20 banks in the world as measured by asset base, with approximately 77,000 employees. With divisions in both the US and Canada, they were very confident they had seen it all before and had heard every pitch ever made.

At cyberconIQ, we don't try and pitch ourselves as a replacement to your current program and vendors but as a complement. We have tools to improve your results and reduce your risk, no matter your approach. We often tell prospects: "just give us your 'serial clickers' first, and we will hand you back successes!"

After launching a POC in late 2021, only months later, we are a significant vendor of record with thousands of seats deployed and growing rapidly. Why? Because we reduced failure rates on independent phishing tests by **95% within 3 months**. Those we trained clicked at a rate of **0.5%**, the **lowest sustainable benchmark the bank had ever experienced**. They were very impressed.

Further, valuable employees who were situationally distracted and continually clicking were facing an escalating cycle of consequence management, becoming a time-consuming and costly business problem. In that particular population, we **remediated 100% of their "serial clickers"**, all of whom had been initially trained on a competing platform and who haven't clicked since. This is absolute proof of actual results that demonstrate a clear connection between **how we teach** and **how employees behave**.

0.5%

Is **your** benchmark phishing failure rate this low?

Why Engage With Us?

We promise that the information you will receive will be valuable and independent of your decision to explore a business relationship with us. As experts in behavioral science, often called upon to advise clients on improving their security program maturity, we know how to **reduce cybersecurity risk, everywhere and every time**. While our platform makes all of this easy, our goal is always to deliver critical insights that help everyone stay safer online. We are here to help.

Learn more at **cyberconIQ.com**.

Data Breach Statistics for 2021

Ransomware Still on the Rise

Appearing in **10%** of breaches - more than **double** from 2020.

The Human Element

85% of breaches involve the human element. Breaches caused by **phishing** were also up **25%**.

Business Email Compromise

The **second-most common** form of social engineering leading to a cyber breach.

*Source: Verizon DBIR, 2021 Data Breach Investigations Report - https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf