cyberconIQ®

White Paper

Innovative Insider Risk Solutions

CYBERology™ - Using Education to Improve Security

Dr. James Norrie

May 2022

The Intersection of Cybersecurity & Behavioral Science

cyberconIQ.com

INNOVATIVE INSIDER RISK SOLUTIONS

CYBERology™: Using Education to Improve Security

Why Education Is Different From Training

So often we see security training focused on delivering pre-determined knowledge about a specific domain or topic specific to IT systems, policies, and internal security requirements. Gripping right? Not so much – its pedantic and boring mostly. Worse still, other security training vendors often suggest that simply delivering this kind of detailed information and then testing for content knowledge will be sufficient to instill employee success at staying safer online – that this repetitive exercise will change behavior. But it will not, and any educator can tell you why this assumption is so dangerous - knowing something and doing something are two entirely different things. Learning something new does not mean you will then apply that learning consistently. That is a flawed assumption.

Instead, we need to focus on security education intended to impart lifelong knowledge and deeper self-awareness. The goal of a recurring educational process is to inspire a voluntary behavior change. The goal of assessment is not testing for content knowledge but application in context. By instilling new security awareness, online employee behavior changes, which measurably improves organizational security – **one employee, one style and one lesson at a time**.

97.8% of our users feel more confident in being able to successfully deal with cyberthreats.

CYBERology™: What Does That Mean for the Educational Experience?

CYBERology™ embeds behavioral science into a technology platform focused on human factor risks. This patented method detects your employees' risk and rules-based preferences and helps them self-manage their online vulnerabilities. In less than 10 minutes, we can help any employee discover their innate style and begin an educational experience that **immediately focuses on changing behaviors**.

At cyberconIQ, we create laddered content personalized to an individual's risk-style. We continue the educational experience through nudges and connections to existing knowledge with each new lesson and situation. Our learning platform improves both learner satisfaction and reinforces the value of the new knowledge acquired by using gamification, multi-dimensional learning assessment, and measuring behavioral modification to ensure we can guarantee a change in on-the-job behavior. We can provide actuarial proof of a reduction in the risk of phishing, social engineering, and business email compromise as well as an increase in compliance behavior that reduces the risk of data loss and leaks.

We can remediate any employees' propensity to fail phishing tests between 45%-95% within 90 days.

The Changing World of Insider Risk

Insider risk is a growing threat to businesses globally which has been exacerbated by the COVID-19 pandemic and the emerging hybrid workforce (remote and on-site) leaving many management teams without a clear path for ensuring on-going data security. When you combine this with trends in outsourced systems, cloud computing, and a reliance on third-party vendors, one can imagine how complex the task of protecting an organization from insider threats is today. Every organization needs to increase the maturity of its data loss protection and insider threat programs to keep pace. A recent Ponemon research report indicated that the typical cost of an insider attack had increased from $11.45M USD per incident in 2020 to $15.38M in 2021. That is a staggering 34% increase in one year while the number of successful insider attacks similarly skyrocketed by 44.3%.

Gartner's most recent Market Guide for Insider Solutions clearly states: "**There continues to be a lack of focused education and awareness around insider risk**" (Cares & Furtado, April 2022). cyberconIQ's educational approach is mentioned as a potential differentiated solution in that Cares & Furtado study. In fact, standard training methodology contained in most vendors' materials cannot provide actuarial proof that their current methodology produces an ROI by mitigating insider risk. But we can!

> **"Cost of an insider attack increased from $11.45M USD per incident in 2020 to $15.38M in 2021"**

Cybersecurity Safe Space: Elevating Compliance Not Consequences

cyberconIQ uses automated methods to encourage voluntary compliance with policy and practice by creating a cybersecurity safe space in which employees can experiment using their new awareness and skills without fear of failure. We focus on security resiliency by catching employees doing things right, not their mistakes. This encourages further exploration and instilling an understanding of how to catch themselves before they put their organization at risk and become an accidental insider. **Mitigating human risk factors through education is cheaper**, **quicker, and more effective** than engaging in premature consequence management that leaves employees feeling vulnerable and afraid.

While our methods refrain from advancing to consequences too quickly, we do recognize there is a point at which more education will not change behavior. The identification of that small pool of resistant employees is vital to managing deliberate and accidental insider threats. Our platform aids in more quickly identifying these vulnerable groups and using our knowledge of your employees' styles, we can recommend more appropriate selective controls and other methods that might yield the required change in behaviors quickest – another benefit of embedding behavioral science theory into practice.

cyberconIQ is a new solution to an old problem; a dramatically different educational experience using the Power of One to reduce your insider risk - permanently and effectively.

If you are ready to learn more about why and how we guarantee a measurable reduction in employees' risky online behaviors, contact us today at info@cyberconIQ.com to schedule your CYBERology™ briefing.

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