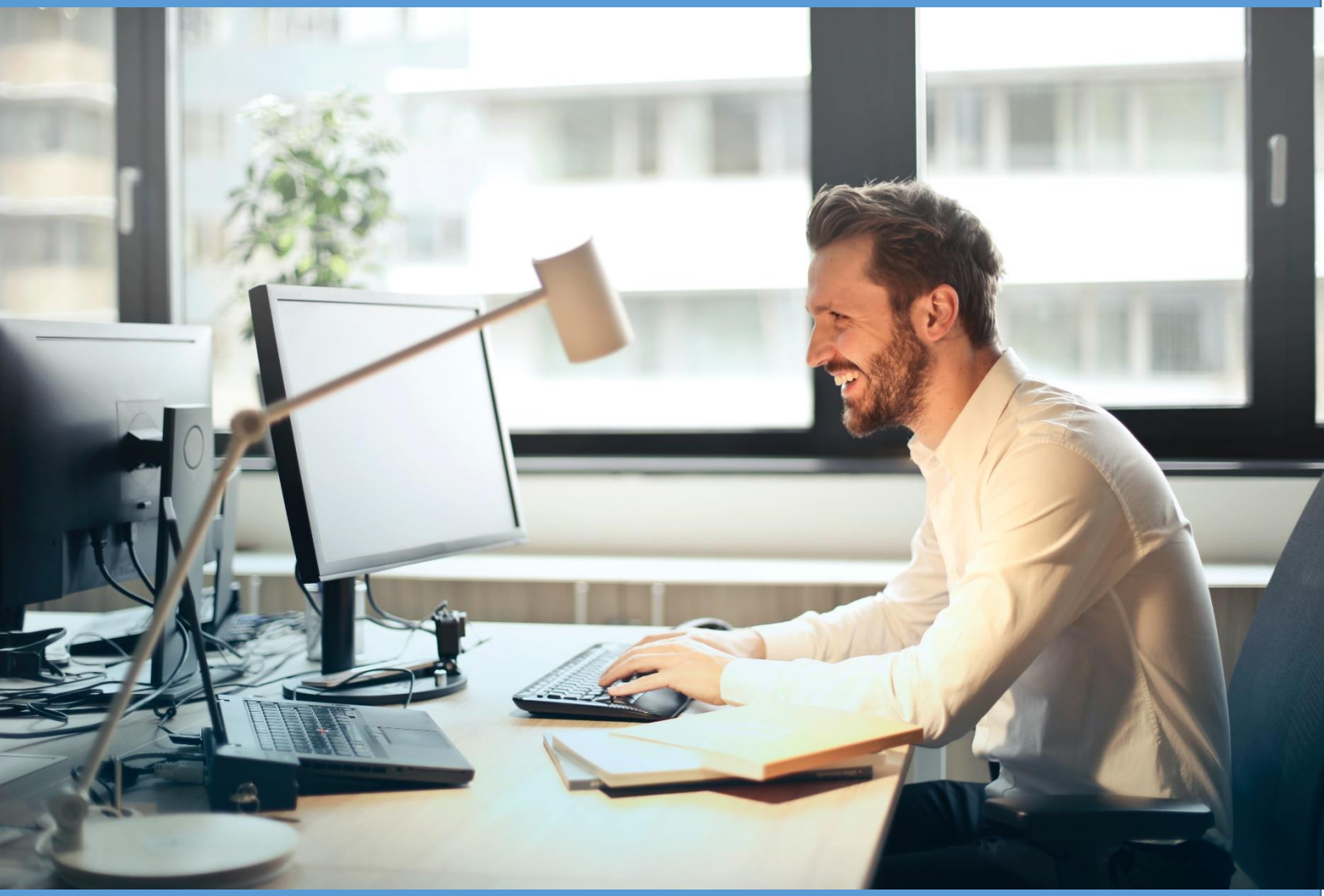

The Case for Cybersecurity Training Awareness as a Process

WHITE PAPER

cyberconIQ

The Case for Cybersecurity Training Awareness as a Process

By Dr. James Norrie, Founder & CEO

How often do we hear from our clients about the pushback on the quantity, quality, and effectiveness of their current cybersecurity awareness training approach? Every day. Most of the leading vendors in this space with whom we compete tout the volume of their offering ("over 500+ modules") often missing a critical component of effective training: it must not be a monthly, quarterly or annual event but rather a deeply considered process designed to create and maintain a cyber aware culture within the company. So, what are the distinctions between the two?

Not Periodic but Constant

At cyberconIQ, we establish a trusting relationship between your employees and our system. It begins with my**Q**, our personalized cybersecurity assessment that provides deep and meaningful insight for each employee into their online instincts and impulses. Think of it like Myers-Briggs for the web! Once that is established, we invite the employee into a core learning journey that is curated specifically for their style and is adaptive to their level of knowledge about cybersecurity. As their journey progresses, they experience not only higher engagement because of this personalized, style-aligned content but also a sense of relief that their dread of the assigned training was not so bad after all!

Yet, completion of this first journey only improves their recall and application of critical cybersecurity practices that reduce their vulnerability to known attack vectors. While effective, it is also ephemeral. The basic psychology of education suggests that most of us will forget more over time than we learn. This is not only normal but should be expected. Therefore, we must engage employees in a constant and steady diet of fun, interesting and new learning experiences to keep what they have learned "top of mind" and firmly in place to establish a cyber aware culture across the organization. So rather than only reporting on completion of their first tranche of style-aligned training, we invite learners back periodically and unexpectedly to receive more curated, personalized content that keeps them educated, engaged, and excited about their role in keeping themselves and their safer company online.

Positive Reinforcement and Engagement not Fatigue-Based Complacency

One of the things that many cybersecurity professionals have had to rely on was fear to motivate compliance. Given the potential financial, regulator, legal, and brand impacts of a successful hack or attack, it was perfectly normal for us to try and alert employees to the dangers of that. However, as I note in my most recent book, the dangers of this approach is the unleashing of hyper-vigilance among your employees.

This biological state is undeniable and is triggered by a constant stasis of low-level fear being present in an environment around someone – like the workplace. Once triggered, this state begins to induce fatigue, feelings of helplessness or event inevitability, and resignation to imminent failure. Does that sound familiar to anyone? As we stress the dangers of a successful online cyberattack arising from human error, our employees conclude its inevitable anyway, is bound to happen and so there's not much point in trying to reduce the risk because we can't. That is a very dangerous development for your company, and you as an IT professional trying to keep it safe.

So, whatever your approach to cybersecurity awareness training and compliance, it should engage your employees as part of an active solution over which they have control and can voluntarily comply. Help them create pathways to improving their knowledge, skills, and ability to catch them doing something right instead of catching them doing something wrong. Fake phishing email campaigns anyone? While they are a tool and may have a place, there is a danger that their use reinforces danger and reduces rather than improves your security posture. Maybe measuring before and after security events, for example, or tying training accomplishments to an improving risk profile and posture will work better. Consider approaches that enable your employees to engage with each other, offering mutual support and encouragement to master important skills and again, to keep a deeply embedded cyber aware culture firmly in place. Do not default to fear but rather pivot to hope and turn cybersecurity into a collective team sport where everyone wins, instead of an individual effort where some will lose.

Educate Don't Train

A fatal flaw we noted in our work with early adopting clients was the fact that many cybersecurity awareness training vendors try and focus on the content of hacks and attacks. They build a set of rules for employees to dutifully follow and then bombard them with reminders of the latest example of that threat in real-time. We do not think this can ever work because the sheer escalating volume of new threats will eclipse our collective ability to warn employees about them before they are hit with them.

Instead, our approach is to educate employees on the context of various threat vectors and how they are individually vulnerable – or not – too specific attack architectures. In addition to that, we use cognitively complex assessments built right into our system that adapt the quantity, level, and sophistication of the training to your employees' existing knowledge base. Built on years of deep research with real organizations, we have learned to align known threat vectors to different types of personalities that are so different, it has been patented! We consider cybersecurity education with an obvious assumption: if we can reduce an employee's personal vulnerability to a successful attack, we can reduce the aggregate probability of a successful attack for the company. And it works – pre/post studies of reduced attack activity suggest that a targeted approach to training reduces both the volume and success rates of both real and false attacks more effectively than generic training of all employees against all attack vectors. Why? Because with higher engagement you get

better learning. It also does not hurt that this approach is inherently more efficient right – who does not want to spend less time in training for a better result? And more learning creates better application of knowledge and creates more changes in on-the-job behavior which is ultimately the goal of any corporate training process. Call us today to learn more about our process and to experience our educational difference.

For more information or to learn more about the cyberconIQ solution, please contact us at info@cyberconiq.com