FREQUENTLY ASKED QUESTIONS:

Current Corporate Clients

cyberconIQ

Frequently Asked Questions: Current Corporate Clients

1. **What if employees continue to believe the assessment is really a 'test' that will be used against them for selection or promotion purposes?**

A: When we use language like 'test', we trigger all manner of fear in people. Bad school 'grading' memories arise. You surely do not want an 'F'; an 'A' would be much better. Right? There must be a way to 'trick' the system. For all these reasons and more, we at cybercon**IQ** go to great lengths to collaborate with management *before* our full system is rolled out. This includes having the senior leadership team complete the assessment and attendant learning modules first. Ideally, those insights would be transparently shared with the organization to encourage team member confidence and commitment. See also **Question #5**.

2. **What is it in for us to know our Cyber Risk Style personally and/or in team situations?**

A: Knowing your unique combination of Risk Tolerance/Aversion and Rule Following/Breaking is invaluable whether at work, at home or even in consumer contexts like eldercare. We encompass the range at cybercon**IQ**. In the corporate arena, we can confirm that experiencing the assessment *plus* curated training results for many employees in feeling like a team of "Cyber Warriors". So much so that one of our catch phrases has become "cyber as a team sport". One of our aims is to empower people to "talk amongst themselves" about collective cybersecurity in whole new ways. We consider one of our primary roles to be "purveyors of hope" in supporting you to defend yourself and your organization from harm.

3. **Why do we need to take the training which accompanies the assessment? Can't we just stop once we know our personal score?**

A: Indeed, you could… However, that would be to miss pretty much the whole *power* of the exercise. It is one thing to gain illuminating insights into your own Cyber Risk Style. It is quite another to deeply comprehend that, *no matter where you land within the four quadrants*, you can be hacked according to the threat vectors attackers have identified as your vulnerability. This critical point reflects much of what standardized training misses. Namely, such offerings focus on knowledge acquisition rather than addressing differentiated personality instincts. We find the latter must be dealt with *before* knowledge can be consistently applied.

4. **Surely, one Cyber Risk Style must be 'better' over all others. Isn't that what the assessment is secretly trying to uncover?**

A: We truly cannot reinforce the following often enough. NO one Style is 'superior' to another. Period. All four Cyber Risk Styles are necessary to a successfully functioning organization (and society as a whole). That is why, after considerable debate, we landed upon the term, Style, to describe the results which derive from a given respondent's combination of Risk and Rule axes. Especially in today's highly charged social climate, we can all undoubtedly understand why a term like Profile would be easily viewed as a politically incorrect descriptor. We anticipate that you appreciate our sensitivity in the language we use.

5. **How can I be sure that management is not looking for the 'right' answers from me when I respond to your questionnaire?**

A: May we take an educated guess as to why you feel that way? If you have ever been in a workplace (and not necessarily your current one) where participation in company-sponsored training about 'styles' or 'profiles' resulted in negative consequences, then your reluctance is perfectly founded. By contrast, one of our foundational beliefs is that *each* leader or business owner *must* be completely cyber-aware today – and ready to lead others in learning how to collectively keep the organization safer online. Rather than the over-used phrase "tone from the top" employed by other vendors and consultants, we prefer "pathways to leadership" to denote the style awareness plus consistent communication and engaged coaching that equals knowledge in action.

6. **What personal information do you collect and save once you have my email?**

A: In both demonstration and production versions of our systems, all access is triggered only by your first name, last name, and corporate e-mail address (non-private directory information). Neither the Test Management System (TMS) nor the Learning Management System (LMS) collect any other identifying personal information, demographics, or even individual assessment answers – only an encrypted final style. For enterprise users, the Product End User License Agreement (EULA) may be agreed globally in advance and suppressed for individual users.

7. How can I be sure *my* results will not be (publicly or privately) shared?

A: To be clear, cyberconIQ does not share your individual/personal/private results. Mind you, we have been known on request, *with permission that is explicitly communicated*, to compile *anonymous* assessment results for senior leadership into a visual that captures the *overall* mix of the four Cyber Risk Styles across the organization. Why, you wonder? The outcome reveals where you are *collectively* the most vulnerable to attack. Such analysis is essential to risk mitigation. Toward that end, we further urge you to share your own assessment results with colleagues. Always, this is only if you so choose. Our coined acronym SAVE (SAVE Yourself from Yourself!) is founded on the strength of consulting with colleagues (especially those of a different Style) when you suspect you are at risk of being hacked. **Refer to Question #2**.

8. How can I check the progress of all those enrolled in the cyberconIQ assessment and/or style-aligned training program?

A: Our customers can designate someone within their organization to monitor progress via the Client Admin. Portal. This person will be able to monitor activity by first and last name, email address, assessment status, Risk-Style Quadrant (and level in terms of Moderate or Strong), training % completed plus the start and end date of training. With this information in hand, reminders or other types of follow-up can be determined to drive successful completion by the desired conclusion period.