FROM FEAR AND ANXIETY TO HOPE AND EMPOWERMENT: CREATING A ROBUST RESPONSE TO CYBERSECURITY THREATS

Cyberspace may be the new frontier, but massive data losses, theft of intellectual property, credit card breaches, and identity theft make it seem like the wild west of two centuries ago. And the cost of breaches is high. To the company, consider fines to UK British Airways of $230M, Marriott of $124M, Equifax of $575M, and Uber of $150M. To individual leaders, consider the firings of CEOs and CIOs directly tied to cyber attacks and losses. If those were not enough, consider the incalculable reputation cost to these organizations trusted with customer data.

If these shocking facts make you feel anxious - as an organizational leader, an employee at work or an individual on your home computer or mobile phone – you are not alone. But instead consider a different approach, one where we are empowered to stand tall in the face of the many attack vectors in this new cyber frontier, to knowledgably operate with the support of our peers and organizations. We need a more robust response to cybersecurity threats.

The Ponemon Institute[1] recently reported that world-wide we are spending nearly 11% of our IT budgets on securing our IT environments. Yet even with this ever-increasing spend, successful cyber attacks are on the rise. Clearly reinforcing the technical thresholds is not enough; we need to consider the human factor as well.

Addressing the human factor has already been highlighted by the Center for Internet Security, Inc. (CIS)[2] as a necessary component of cybersecurity. CIS is a 5019(c)(3) non-profit

---

[1] Find the Ponemon Institute report at https://www.ibm.com/security/data-breach

[2] CIS Controls are a "prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks." Read more at https://www.cisecurity.org

organization whose mission is to identify, develop, validate, promote, and sustain best practices in cyber security. Specifically, CIS promotes the implementation of an enterprise wide training program that "can be focused on concepts and skills that cannot be managed technically". Such training should be "specific, tailored and focused based on the specific behaviors and skills needed by the workforce". We have all seen training programs provided by various cybersecurity vendors. Of concern are approaches that focus on delivering information about cybersecurity rather than changing actual behaviour when confronted by cybersecurity threats. It is one thing to know the terms phishing and smishing and quite another to truly learn how to change personal behaviour in response to these threats. We know that a change in behaviour reflects that learning has occurred.

We each bring a unique set of talents, skills and abilities to our workplaces, and indeed our lives, every day. No employee arrives at work wanting to be the cause of a major security breach. But we have often de-sensitized our employees and created a false sense of security with the messages "don't click on that link" or "don't open an email from someone you don't know". Not only does information delivery not equate to learning, but by providing information in just one way we will not reach every individual in order to create those needed behaviour changes. Rule-based learning ("don't click on that link") does not work for everyone. Real learning is about changing behaviour, creating the ability to respond in an empowered way to critical cybersecurity threats.

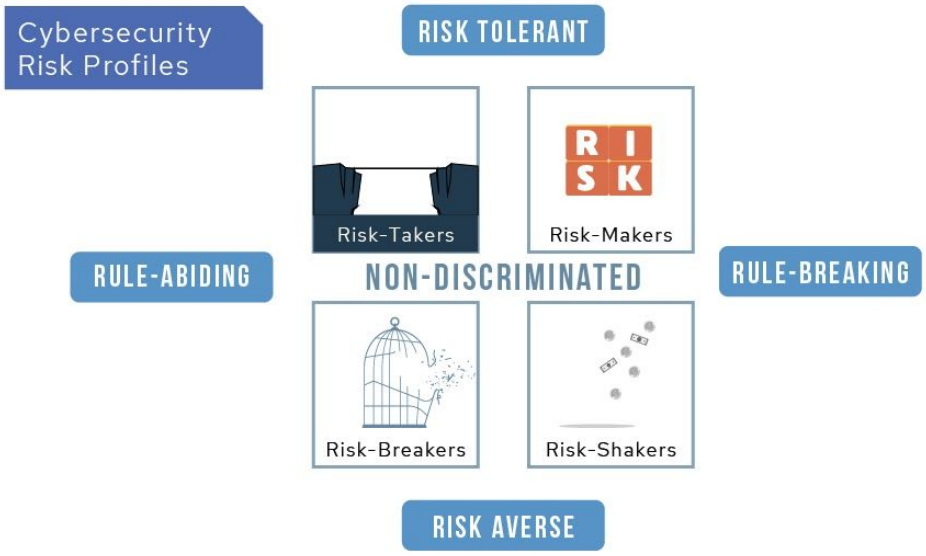
As researched by Parsons et al (2010), personalizing cybersecurity learning for individual learners can "result in more positive behaviours and lead to more secure information environments"[3]. Cognitive style, risk posture, and organizational culture were just some of the human complexities that the research team identified as contributing to an individual's response to a cyber threat. What if we could create a new and different approach that helped

[3] Parsons, K., McCormac, A., Butavicius, M., and Ferguson, L. (2010). *Human Factors and Information Security: Individual, Culture and Security Environment.* Retrieved from: https://apps.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf

us understand our personal vulnerabilities and targeted specific ways we can arm ourselves against these attacks?

There is a new way. Each of us, in our uniqueness, perceives cyberthreats differently and likewise responds differently. By identifying our individual risk profiles, training can be specifically targeted to that profile and ongoing reinforcement (per the CIS framework) can be targeted as well.

What is this new way? Based on extensive research, cyberconIQ has developed a patented tool that identifies your cybersecurity risk profile along two continuums – risk tolerant/risk averse and rule abider/rule breaker.



Reprinted with permission: Norrie, J. L. (2019).

CYBERCON : protecting ourselves from big tech & bigger lies. Mindstir Media.

The assessment measures your instincts on these dimensions to locate your base personality in one of the four quadrants, or as non-discriminated if you are too in-between. Each quadrant represents a particular cybersecurity risk profile. It is important to note that no one profile is better than the other – every profile is vulnerable to cyber attacks. But the nature of the attacks that will be successful with any given profile differs. Imagine the ability to specifically target the appropriate training and support tools to a particular cybersecurity risk profile. This training, targeted to the specific risk profile of individual employees, is a learning environment that promotes empowerment and creates behavioural change. It is an investment that, compared to generic information delivery models that do even not reach all employees, will maximize the return on your training dollar.

There is, of course, more than a direct monetary benefit to this approach. Research demonstrates that by shifting the culture of your organization from fear to optimism, your employees are more engaged in collectively protecting the organization. As employees want the organization to be successful, they can personally contribute to that success by keeping the brand safe. These actions can be celebrated in the open, rather than hidden behind a curtain of fear.

Can cybersecurity training be mandatory, i.e. a condition of ongoing employment? In a word, yes. While legislation varies state to state and province to province, as long as the employer provides paid time for completion of the training, it can require employees to take the training. To gain the benefit from this approach, employees begin by taking the cyberconIQ assessment which identifies their cybersecurity risk profile. Most employees willingly participate when this is presented as a way to personalize mitigation against cyber attacks.

Every risk profile is susceptible to some form of cyber attack. (Interestingly, those employees most likely to not want to take the assessment come from the Risk Breakers quadrant. They may see themselves as already “following all the rules” and “not taking risks”. However, this profile is most susceptible to attacks that mimic someone in authority who has asked them to suppress the rules.) This tool is neither designed nor meant to be used to target a particular risk

profile in a negative way, but rather to assist employees in improving their own and their organization's cybersecurity defenses.

Creating an understanding of why this targeted approach is helpful for employees does require supportive communication from the top. An environment known for respect of employees' time, individuality, contribution and privacy are key messages to deliver. No one risk profile is better than another, as each and every employee makes an important contribution to an organization's success. Also by generating aggregate profiles by job function and organizational grouping, this approach can provide enormous insight into the group profiles that may be useful beyond this specific training. And should it be the culture of the organization, individual profiles can be kept confidential to that employee. However, the benefits of sharing in an open environment are well evident. The internal dialogue among colleagues is permanently changed after taking this assessment and training and the organization as a whole experiences a positive sensitization effect about how individual behavior can lead to improved collective cybersecurity outcomes.

The benefits are real. Within days of employees completing the assessment and training organizations see lower rates of incidents of compromise or concern (IOCs) and reduced failure rates on individual follow-up social penetration testing and retesting. These assessments capture direct impact on company-wide risk levels indicating a higher ROI for these methods compared to traditional, generic approaches to cybersecurity training. And empowering employees to respond creates a more engaged and hopeful workforce.

For more information about the cyberconIQ approach visit http://cyberconIQ.com.

Cindy Seibel (former CIO & Human Resource Professional)
Principal, LINKS Technology Consulting