Global FINEX: Cyber Risk Solutions (CRS)

Workforce Cyber Culture Assessment (WCCA)

An enterprise-wide assessment of your people-centric cyber risk profile giving you the information and tools to reduce the likelihood, frequency and impacts of people-related security incidents.

Your employees play a key role in organisational cyber security. Our research (WTW 2017 Cyber Risk Survey Report) shows that over two thirds of reported cyber incidents continue to be directly attributed to the actions of people or, in other words, your workforce.

Akin with many businesses, your focus and investment is likely to be directed at protecting your technical security environment. But given that your current expenditure can be undermined if the actions and attitudes of your workforce are contributing towards heightened cyber risk, maybe it is time to revisit your priorities.

The inclusion of an assessment of your workforce and business culture, performed alongside and in conjunction with other traditional cyber risk management activities (Figure1. overleaf), is key to comprehensively understanding your cyber risk profile – knowledge of your strengths, weaknesses and areas in need of attention.

What is the Workforce Cyber Culture Assessment (WCCA)?

The WCCA leverages traditional employee engagement methodologies to probe an employees' awareness and understanding of cyber risk, their own attitudes and behaviours as well as the emphasis that their organisation places (or not) on addressing cyber risk. By assessing which aspects of a company's workforce are working to increase or decrease the likelihood and frequency of a cyber incident, the WCCA will give your organisation a firm understanding of your people risk profile. It also provides focused recommendations to assist in mitigating and managing the associated risk(s) as well as supporting positive behavioural change across all levels of the business.

How does the Assessment work?

Every level of your organisation is assessed within FOUR key respondent groups (Figure 2. overleaf). How the assessment is structured and delivered is entirely flexible depending on your precise business requirement; this could be as a web-based survey via our proprietary survey distribution platform or through in-person, consultant-led interviews/workshops. The WCCA is designed to provide an assessment of your people + cyber threat in line with our custom framework. This framework allows us to focus on the analysis of individual's responses to questioning within six key categories. These outputs form the basis of our targeted recommendations and support the creation of a 'fit-for-purpose' and people-centric cyber culture management strategy.

In designing the delivery methodology, we have been conscious to limit any operational impacts to your business and your teams whilst maximising the value and efficacy of the assessment outputs.

Willis Towers Watson

The Benefits?

The WCCA delivers key actionable and measurable benefits.

Each of the benefits below will provide your organisation with a greater understanding of your people + cyber risk culture. Used together, they provide a powerful engine for positively identifying and managing human cyber risk across your enterprise.

- **Identify areas of people cyber risk.** Key groups or functions representing your greatest cyber risk are identified, allowing for the objective allocation and prioritization of security budget and delivery of high impact fixes
- **Highlights high risk cyber-security attitudes and behaviours across your organisation.** The traits of your risk culture are mapped and assessed against our custom framework
- **Prioritises cyber risk improvement recommendations** By benchmarking your people risk profile against companies that are consistently strong cyber-security performers, breached companies, as well as industry peers
- **Allows stakeholders to quantify cyber risk in financial and monetary terms**, aiding the selection of effective risk transfer options
- **Develops a people-centric cyber strategy to support positive behavioural change.**

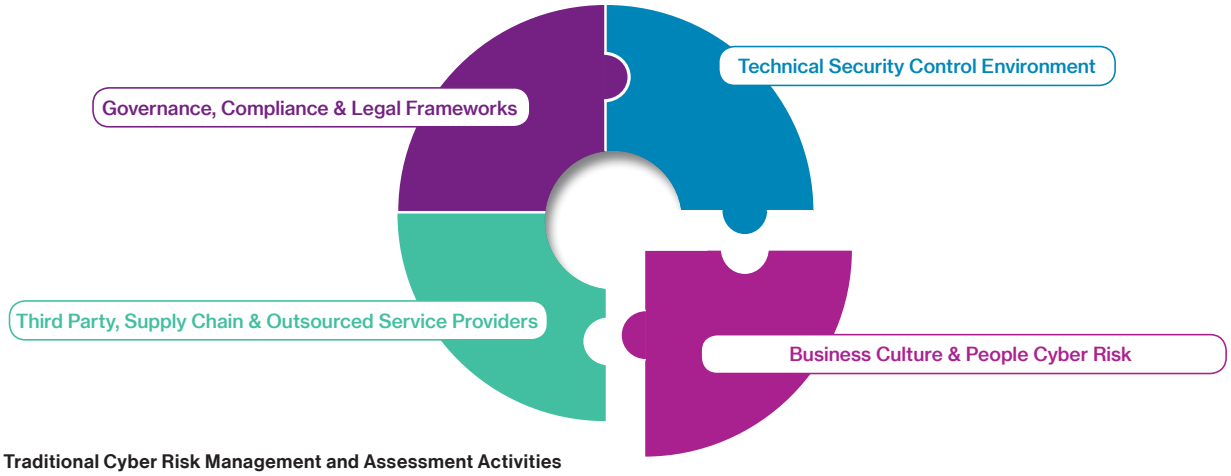

Figure 1. Traditional Cyber Risk Management and Assessment Activities

FOUR key respondent groups

Figure 2. Survey Respondents Groups

1. Senior Leadership / C-Suite
2. Function – Middle Management
3. Information Security / Technology
4. General Workforce

For further information please contact: Dean.Chapman@WillisTowersWatson.com / +44(0)7920 211 779

willistowerswatson.com/social-media

willistowerswatson.com

Willis Towers Watson