Decode resilience.

Cyber risk check up: Willis Towers Watson's top 9 steps for greater cyber resilience

Baseline your organization's cybersecurity maturity against either the NIST Cybersecurity Framework or ISO 27001. Both NIST and ISO authorities have emerged as globally accepted baselines that provide roadmaps for building comprehensive cyber risk management programs. By using either or both of these industry best practices to assess where their cybersecurity is strong or needs improvement, organizations can make more informed decisions about where to allocate limited resources to ensure maximum security impact.

Develop a Cyber Risk Register and Action Plan that identifies your organization's greatest cyber risks to inform your risk prevention, mitigation, and transfer strategies, to prioritize your cybersecurity spending. Every organization should create its own register of cyber incident scenarios and cyber risks relevant to them and determine how existing and planned cyber risk controls work to reduce their occurrence. Organizations need to take into account their industry sector, the data they hold, the cyber incidents that they and their peers have experienced, and their own cybersecurity maturity in order to model cyber risk scenarios relevant to their operations. In so doing, organizations can strike a fully aligned and cost-effective balance among their risk prevention, risk mitigation, and risk transfer strategies that help boost true cyber resilience. Comparing and contrasting the likelihood and consequence information in a centralized Cyber Risk Register helps guide the development of a highly effective Action Plan and a defensible cybersecurity budget.

Ensure your organization's cyber risk management activities are aligned to support your core business goals. Effective cybersecurity can't happen in a technical vacuum that isn't aligned with overall business objectives. Organizations instead should identify their priority cyber risks by listening not only to CISOs and CIOs but also to other key leaders who know their businesses best – the CFO, the CRO, the General Counsel, the HR lead, and additional influencers in authority positions. By taking a cross-functional approach, organizations put their cybersecurity work into a more relatable "impact on operations" context, garner essential support across the enterprise, and increase an organization's chances for lasting cybersecurity success.

Understand whether your organization's executive leadership is setting the right cybersecurity "tone from the top". Human-caused cyber incidents proliferate in environments where leaders "talk the talk" about cybersecurity but don't "walk the walk" themselves, fail to hold employees accountable for poor cyber hygiene, and neglect to set clear expectations for cybersecurity behavior. Organizations therefore should ask managers – at all levels – how they're promoting cybersecurity across their teams and then check separately with those teams on the answers. Organizations should direct competency development, performance management, and other appropriate leadership investments to wherever disconnects between these two populations are consistently found.

Willis Towers Watson

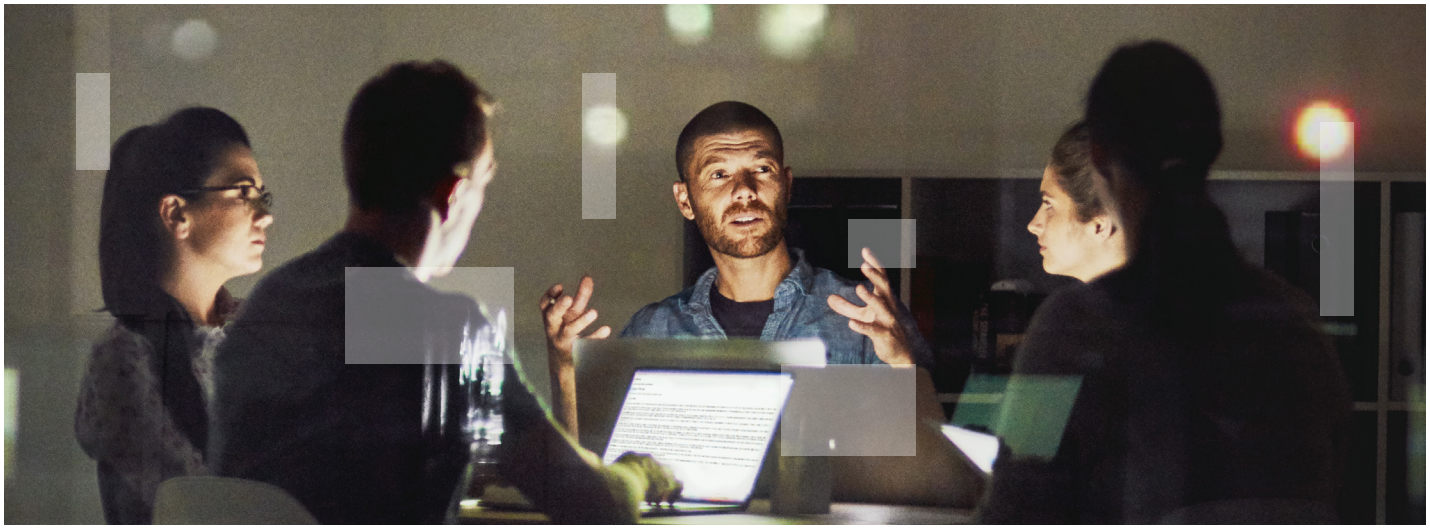
Determine whether your cybersecurity training is effective, and assess if your cybersecurity communication strategy resonates with your workforce. As a first step, organizations should identify the subset of the workforce for whom the training is not working so customized content can be directed to that population specifically. Organizations should also work to understand what environmental factors – social, psychological, and otherwise – are preventing employees from gaining the cybersecurity knowledge they need. As such, many organizations run cybersecurity awareness campaigns that fail to make cyber risk management relevant to the day-to-day work of their employees. Organizations should ask themselves if the messages they're sending are communicated in ways that ensure that different workers with different roles and responsibilities understand not only the dangers of cyber risks but also what they personally can do to prevent and/or mitigate them. Tailoring cybersecurity communications this way promotes both cybersecurity accountability among individuals and good cybersecurity behavior across the board.

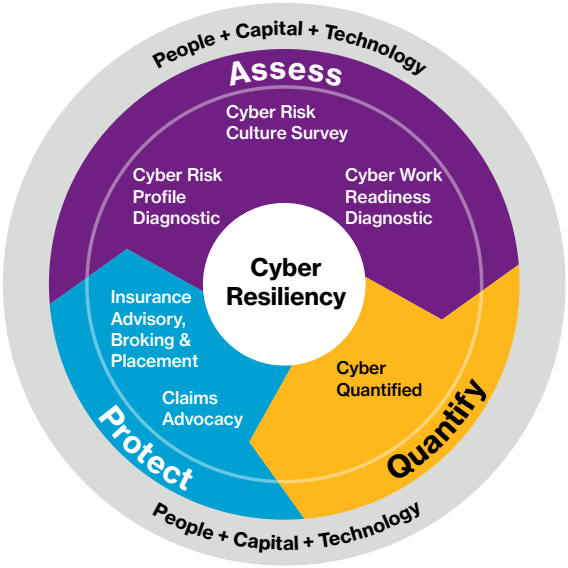
Identify which of your employees represent your greatest source of cyber vulnerability and why. 61% of all cyber incidents are caused directly by an organization's employees – either through negligence or intentional malicious activity. Boards of directors have become increasingly aware of this statistic and are adjusting their cybersecurity budgets in response to address this human element of the risk. To do so effectively, organizations need to pinpoint which of their workers are struggling most to do the "right cyber thing". Once they've identified those populations, HR leaders can pursue targeted solutions that bring them into the fold while improving the overall cyber risk culture for everyone.

Remove organizational obstacles that prevent your employees from being good cyber citizens. If an organization's cybersecurity policies, procedures, and technologies aren't easy to apply and/or use, employees invariably will find work-arounds so they can get their jobs done. Those work-arounds, however, often open up entirely new and unforeseen cyber vulnerabilities. Organizations must strive to strike the right balance between protecting their sensitive data, systems, and other assets while enabling their employees to successfully complete their daily duties.

Win the war for cybersecurity talent. In today's job market, there simply aren't enough talented cybersecurity professionals available to meet demand. Without them, organizations face cyber losses that are likely to be exponentially worse than if they had the right people with the right skills on staff. Organizations should develop a clear sense of what job functions and skill sets are most critical to address their particular cyber risk circumstances – now and into the future – so they can develop the targeted recruitment and retention strategies they need for their protection.

Make an informed purchase of cybersecurity insurance. Cybersecurity insurance is an essential part of any comprehensive cyber risk management program. Organizations should be smart consumers of such policies by first determining their cybersecurity gaps and then taking responsive prevention and mitigation steps that make economic sense. For the residual cyber risk that remains, customized insurance policies serve as powerful transfer mechanisms that help impacted organizations not only survive serious incidents but also thrive in their aftermath.





About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

For more information

Thomas Finan
+1 571 639 1010
thomas.finan@willistowerswatson.com

Timothy Rees
+44 203 124 8026
timothy.rees@willistowerswatson.com

Corrado Zana
+39 024 778 4301
corrado.zana@willistowerswatson.com

willistowerswatson.com/social-media

WTW-NA-2019-WTW236970

willistowerswatson.com

Willis Towers Watson