Willis Towers Watson's
Input to NIST on Enhancing National Cybersecurity

Workforce culture is as much a driver of cyber risk as is the failure of or inadequate investment in IT systems and poor corporate governance. To more effectively manage cyber risk, organizations must better understand how the various elements of their workforce culture shape their employees' behavior and, ultimately, either reduce or drive their exposure to cyber risk. Seeking to better understand the relationship between workforce culture and cyber risk, in May 2016, Willis Towers Watson analyzed employee opinion results from over 450,000 employees corresponding to a period during which significant data breaches were experienced within their organizations. The results were then benchmarked against high performance companies (financially superior companies that had not experienced data breaches) and global information technology (IT) staff.

The study indicated that there were significant gaps in favorable opinion scores between employees in data breach groups and each benchmark group. Compared to the high-performance group, employees at data breach companies report significantly lower scores in three areas of workforce culture:

- Training
- Company image
- Customer focus

Compared to the IT employee group, IT workers in data breach companies have less favorable views of training and score especially low on perceived training of new employees. The analysis points to new staff as a blind spot and potential serious source of cyber-risk if not effectively trained in processes and procedures. Compared to the IT employee group, pay for performance emerges as a challenge. The findings indicate that frontline IT staff in data breach companies perceived a misalignment between their efforts and associated rewards, potentially undermining efforts to identify and manage cyber-risk.

Compared against both benchmarks, employees in data breach companies indicated a widespread lack of customer focus. This finding is significant from a risk management perspective, as it could set the stage for poor decision making and undermine the vigilance needed to counteract attempts to steal online customer information. The above results are significant because they offer an inside view of workforce culture and reveal the vulnerabilities within companies experiencing cyber breaches based on the ultimate insiders — their employees. This snapshot of employee opinions within firms that have experienced data -breaches suggests that workplace culture may be the first line of defense against cyber risk. And perhaps more importantly, the data suggests a significant part of the answer in helping organizations assess and minimize cyber risk lies in understanding the workforce culture that shapes everyday employee behavior.

How Assessment and Quantification of Workforce Culture Can Improve Cyber Insurance

Today, most cyber insurers have processes in place to select risks, set deductibles or attachment points, and establish the price for each policy. These underwriting processes and pricing models vary widely in approach but generally rely on factors such the insured's industry type, revenue and employee count, number of records, and value of assets, as well as underwriters' qualitative assessments of the insured's network security policies, practices and procedures.

While insurers inquire generally about employee awareness training during the underwriting process, those inquiries do not go far enough in understanding the susceptibility of a particular organization to cyber risk as a result of employees' behavior. Given the human element involved in cyber risk, insurers and insureds would be well-served to place more or equal emphasis on an organization's overall workforce culture and, in particular, how employee behavior may negatively (or positively) impact the organization's cyber risk management strategy. By analyzing and embedding workforce culture data within the underwriting process and tools, underwriters would be better able to predict overall risk to their portfolio. More importantly, we believe that cyber insurers would be better positioned to offer more tailored cyber insurance coverages, additional capacity and competitive premiums to insureds.