Financial & Executive Risks (FINEX) North America

Cyber Risk Alert
May 2016

The inside threat: Why employee behavior and opinions impact cyber risk

The human element as a risk factor in data security breaches is as enduring as it is troubling. Compromised laptops and phishing email scams continue to appeal to hackers as avenues to damage corporate servers and the confidential, sensitive information they maintain. Effective risk management strategy must therefore acknowledge and respond to this source of widespread vulnerability.

Several cybersecurity studies have cited statistics noting that:

- Approximately 60% of incidents are non-hacking related and attributable to employee errors that fall within several categories, including lost laptops, rogue employees and software errors.
- The remaining 40% of incidents are hacking related and the result of social engineering or inadequate network security practices.

Until now, none of those studies have answered this question: how can organizations track the extent of risk inherent in their people's behaviors and determine how to mitigate this factor?

The answer(s) to this critical question is not only relevant to human resources professionals charged with addressing employee behavioral issues but is also pertinent to corporate leaders, network security professionals, corporate risk managers and insurance underwriters — all of whom are links in the chain of cyber risk management and mitigation.

Workforce culture shapes everyday behavior

A significant part of the answer to the above question lies in understanding the workforce culture that shapes everyday behavior. An organization, and in particular its leaders, create and reinforce a culture that influences every employee. This culture holds the shared values, norms, beliefs and assumptions that ultimately drive employees' actions. The emphases within the culture can support or inhibit behaviors that mitigate risk. For example, a culture with a strong customer focus will create norms for prioritizing customer needs above other demands, encouraging extra effort when interacting with customers and handling their information internally. Over time, through thousands of individual employee decisions, behaviors that help prevent data breaches will occur with more frequency than behaviors that create significant vulnerabilities.

A new analysis of employee survey results sourced from organizations that have experienced significant data breaches — including the loss of business-critical, employee

and consumer data — further reinforces this position. The survey results tap into the factors most often emphasized inside a company, gathering views of culture as experienced by the ultimate insiders — the employees themselves. By examining the cultural landscape in organizations experiencing data breaches, the critical human element comes into sharp focus.

Employee opinions in organizations that have experienced cyber breaches

Willis Towers Watson analyzed employee survey results across its rich database, capturing employee opinions from over 450,000 employees corresponding to a period during which significant data breaches were identified within their firms. The organizations represent major business sectors, including technology, telecommunications, consumer products, manufacturing and utilities, with headquarters in North America, Europe and Asia Pacific.

In order to benchmark employee opinions from the organizations and uncover critical understandings, Willis Towers Watson applied information from its world-leading database of employee surveys, drawing on responses from over four million employees and 400 organizations annually across all business sectors and regions. More specifically, to identify vulnerable aspects of culture in companies experiencing data breaches, opinion scores in the breached organizations were compared with two sets of benchmarks from this database:

- **Global high-performance organizations.** These 28 organizations are financial leaders in their industries, with above-average top- and bottom-line performance versus sector-specific scores over a 36-month period. This benchmark includes organizations with the highest levels of favorable opinion in the database.
- **Global information technology (IT) staff.** This benchmark is pulled from IT staff across organizations globally, representing over 400 companies and more than 150,000 IT workers. Opinion scores from IT functions in the breached organizations are contrasted with this benchmark.

Survey content across organizations covers a wide range of issues from local work experiences (opinions of training, immediate supervision and individual involvement) to views of oganizational systems and programs (perceptions of senior leadership, pay and rewards, customer focus and company image). Results from these two comparisons are displayed in the following figures, which show gaps in favorable opinion scores between employees in data breach organizations versus each benchmark group.

Compared against the high performance group

In the comparison with high-performance companies, opinions from employees in the data breach organizations are consistently below the favorable scoring levels of employees in the high performance group, as expected. Scores are lowest for three aspects of culture:

Gaps: Breach Companies Below Global High Performance

Training: Questions in this topic include employees' opinions about whether they have received adequate training for the work they do and have access to training to improve their skills and learn new skills to advance in their roles.

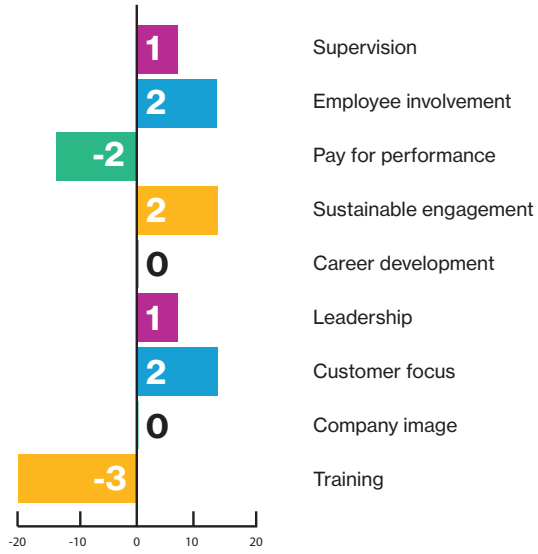
- **Company Image:** Questions in this area focus on corporate social responsibility, environmental responsibility, regard from customers, and integrity when dealing with external stakeholders.
- **Customer Focus:** These questions tap into employees' overall sense of emphasis on the customer, responsiveness to customer needs, and proactive efforts to gather and act on customer feedback.

In short, these results versus the high-performance group indicate that organizations experiencing data breaches in the study period are judged by their employees as lacking a learning culture that flourishes with high integrity and puts the customer at the center of business activity.

Compared against the IT employee group

IT workers in organizations with data breaches are aligned with relatively similar functions globally. That said, workers in the data breach organizations report less favorable views of training and perceived pay-for-performance in their role. In the training area, IT staffers in data breach companies score especially low on perceived training of new employees, suggesting a vulnerability among workers as they are recruited and onboarded. Related to pay, scores in data breach companies are especially low on matching pay to performance, indicating that incentives should be better aligned with employee efforts to more clearly show the connection between behaviors and consequent rewards.

Gaps: IT employees in breach companies below global IT functions on training



Common themes emerge

Results across comparisons with both high-performance organizations and IT staff converge on a common theme related to training. Among IT staff, the analysis points to the induction of new staff as a blind spot — potentially a serious source of risk if new IT staff is not effectively trained in processes and procedures to manage cyber risk. Across the full enterprise, this inability to create an ongoing learning environment may reflect a lack of emphasis on staying current with emerging business needs and trends, potentially including knowledge of how to circumvent attempts to acquire confidential and sensitive data by determined hackers.

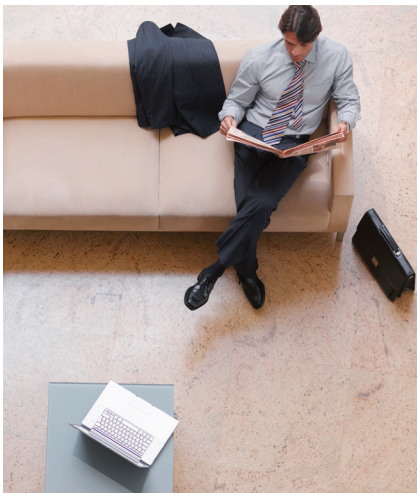
Also among IT staff, a pay-for-performance challenge emerges from the analysis. This finding indicates that front-line IT staff in data breach companies may perceive a misalignment between their efforts and associated rewards, potentially undermining their motivation to give the extra effort in roles needed to effectively identify cyber risk concerns and take corrective action.

More generally, the finding that perceived customer focus is lacking in data breach organizations is significant from a risk mitigation perspective. Customer service is a foundational company value for many organizations and is essential to business success in service industries. A lack of emphasis on the customer as central to organizational performance likely sets the stage for poor decision making related to business risks and may undermine the vigilance needed to successfully counteract attempts to steal online customer information.

Mitigating cyber risk

Addressing fundamental emphasis in workplace culture is a first step to creating an environment that supports a holistic, integrated risk mitigation strategy. In addition to emphasizing a customer-centric workplace culture, and developing and implementing employee incentive and training programs designed to foster cybersecurity, organizations should consider the following cyber risk mitigation approach:

- Ensure enterprise-wide governance is in place
- Assume hackers are already inside
- Consider technology one of several lines of defense
- Insure for cyber threats that cannot be mitigated
- Allocate enough capital to the right cyber defenses — protect the organization's crown jewels!



Willis Towers Watson

Contact

Patrick Kulesa, PH.D
Global Research Director
Research & Innovation Center
Human Capital & Benefits
+1 212 309 3746
patrick.kulesa@willistowerswatson.com

Adeola I. Adele
Employment Practices Liability Product Leader
and Cyber Thought Leader
Corporate Risk & Broking
+1 212 915 8889
adeola.adele@willistowerswatson.com

Anthony Dagostino, EVP
Cyber/Errors & Omissions Practice Leader
Corporate Risk & Broking
+1 212 915 8785
anthony.dagostino@willistowerswatson.com

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 39,000 employees in more than 120 countries. 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.

willistowerswatson.com

Willis Towers Watson