Decode the human threat.

Driving a cyber-savvy culture to combat cyber threats

By Patrick Kulesa

The constant drumbeat of headlines about data breaches, stolen assets and network outages signals the real and ongoing threat of cyber risk for today's organizations. Whether in response to the WannaCry ransomware attack or news about breaches at competitors, companies in all sectors and geographies are focused on cyber threats as a matter of necessity and survival.

Technological defense is often the main tactic applied in efforts to combat cyber risk. Although critical to an organization's cyber strategy, technology on its own is not enough to meet the challenges that today's hackers present. What is required in addition, is a focus on a major source of vulnerability that can allow hackers into the front doors of any business regardless of technological defenses — the human element, namely, the employees working daily in corporate systems. One misstep, even if accidental, by an employee working in a critical network can potentially facilitate a disastrous data breach.

Focus on the human element and company culture

The human element should be a major source of concern. As highlighted in our Winter 2016 brief, data related to cyberinsurance claims show that employee negligence or malicious acts accounted for two-thirds of cyber breaches; by contrast, only 18% of breaches were directly driven by an external threat. The data further showed that approximately 90% of all cyber claims are the result of some type of human error or behavior. The range of human action that can result in cyber breaches includes seemingly innocuous behaviors such as removing paper files from the office to use to work from home, logging into a public Wi-Fi to quickly download a key document and even discussing work-related topics in public. The simple truth is that a data breach is more likely to result from an employee leaving a laptop on a train than from a malicious criminal hack.

The data further showed that approximately 90% of all cyber claims are the result of some type of human error or behavior.

How can an organization target the human element effectively in efforts to drive the right employee behaviors? While at work, people's actions are driven by many influences, including what the company emphasizes in its communications, the policies and practices in place to direct work, what behaviors get rewarded, and the visible actions of important role models. Collectively, these influences describe "how work gets done here," or what is called the culture of the organization. No two cultures are alike, as all face differing business conditions, and cultures are somewhat fluid, able to adapt to changing environmental needs or be shaped in ways that optimize work activity. An understanding of what cultural factors increase cyber risk from employee behavior would offer a blueprint for organizations seeking to mitigate threats from this human element.

Willis Towers Watson research has identified the organizational culture factors associated with cyber breaches. For the research, results from all-staff opinion surveys were studied in a database that includes information from over 400 companies and over 4 million employees annually. Within that database, 12 organizations with employee survey findings corresponding to the period of a significant data breach were identified, with opinion information available from over 450,000 employee insiders in those firms. The 12 organizations represent major business sectors --including technology, telecommunications, consumer products, manufacturing and utilities — with headquarter locations in North America, Europe and Asia Pacific.

Comparisons were made between the views of employees across this set of 12 "breached companies" and opinions from employees in organizations with strong financial results, a cross-sector high-performance group of 28 organizations and over 400,000 employees. In addition, given the critical role in cyber risk of employees in information technology (IT) roles, results from IT staff were also compared with a benchmark from IT staff globally, which was drawn from over 400 companies and 150,000 workers.

Research findings point to three elements of culture associated with cyber risk. Specifically, organizations that have experienced data breaches are judged by their employees as falling short in efforts to promote a customer-centric environment, provide effective training for employees (especially newcomers in IT), and conduct business with high integrity, especially in interactions with third parties. From a cultural perspective, these findings suggest that cyber threat is exacerbated when organizations do not:

- Emphasize strongly enough that the customer is the center of the business, and that understanding and reacting to customer needs is essential to success; because behaviors related to handling customer information happen constantly in an organization, a customer-centric attitude can be a line of defense in mitigating cyber risk
- Deliver a learning environment in which new entrants are trained well in the basics of doing business, and new information is shared continually, especially among IT staffers; because the nature of cyber risk is ever-evolving, an organization that enables its people to constantly update their knowledge base is better equipped to react to threats in cyberspace
- Stress the importance of always conducting business the right way, avoiding shortcuts and acting responsibly, especially when working with third parties; because much business today involves passing information (even customer data) across multiple providers, the expectations set by corporate leadership to conduct business carefully and with high standards of integrity have to be part of the blueprint for defending against cyber threats

Cyber risk culture survey drives awareness and action

These three pillars provide both insight into the aspects of culture that may mitigate cyber risk and the core of a measurement system that any organization can use to track cyber vulnerability. Cultural conditions matter in the cyber defense equation and the quality of culture can be assessed through employee feedback mechanisms. A cyber risk culture survey serves as an analytic tool to help companies evaluate their internal risk culture, with a particular focus on where it might be most vulnerable to employee-driven cyber incidents. The content of such a survey tool needs to have two main emphases:

Awareness. The research findings on cultural shortfalls in breached organizations point to a fundamental lack of awareness of the value of customer centricity, domain-relevant knowledge and the importance of business integrity. Other aspects of basic employee understanding can be studied in a cyber risk culture tool from multiple perspectives — specifically:

- Clarity of roles and responsibilities for data security in the structure of the organization
- Individuals' roles in data security processes
- Personal sense of responsibility for data security
- Perceived organizational support for raising data security issues
- Knowledge of how to raise concerns about threats
- Effectiveness of training received about data and information security

Action. Ultimately, cyber defense is about driving the right behaviors across the workforce. A cyber risk culture survey taps into behavior at the individual and organizational levels by assessing:

- Personal cyber IQ – frequency of cyber-smart behaviors
- Adequate time in role to address data security
- Pressure to cut corners on data security when delivering for customers
- Experience of leaders taking information security concerns seriously
- Open communication from leaders about data security best practices
- Ability to locate information about data security plus the relevance of that material to job requirements
- Speed of organizational response to data security events

Willis Towers Watson research on awareness of cyber threats and effective employee behavior suggests significant room for improvement. For example, survey findings from a national sample of over 2,000 U.S. respondents reveal challenges creating awareness and driving action. Among the findings from those surveyed:

- 46% believe that opening any email on a work computer is safe
- 43% have received a suspicious email at work (with 80% indicating they informed IT)
- 34% have witnessed a co-worker violating company information security policies
- 32% have logged into their work computer using an unsecured public network
- Only 32% report discussing information security risks with their immediate managers
- 22% used personal computing devices not approved by IT to do work at home
- 18% have downloaded software not approved by IT onto their work computers
- 15% have shared network passwords with work colleagues

Cyber risk is a horizontal, enterprise-wide challenge that demands a collaborative response including input from IT, human resources, legal, operations, finance and risk management.

The value of a tool to monitor awareness and action is multi-fold. With the results from a cyber risk culture survey, organizations can benchmark results versus other similar companies and those organizations that have experienced major cyber breaches. They can also learn what aspects of awareness and experience drive cyber-savvy behaviors across their workforce. Most importantly, they can profile segments of the organization most in need of education and resources by isolating poor-scoring groups within the enterprise.

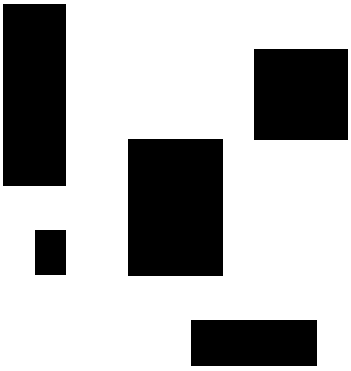
In addition, survey findings can support a dialogue about cyber strategy. Cyber risk is a horizontal, enterprise-wide challenge that demands a collaborative response including input from IT, human resources, legal, operations, finance and risk management. The survey solution touches all corners of a workforce and consequently brings to light challenges that involve many organizational constituencies. Taking action based on the findings likewise requires input and commitment across an organization.

It takes a holistic strategy

Employee feedback is ultimately one part of a comprehensive cybersecurity strategy involving technological defenses, effective management of information security talent across an organization, and even risk transfer to cyberinsurance. In a recent survey of nearly 100 U.S. firms by Willis Towers Watson, 85% of employers report cybersecurity as a top priority, even though 53% say they lack a formally articulated cyber strategy and 85% aspire to embed cyber risk management into their company culture over the next three years. A survey-driven approach to identifying challenges and gaps related to that goal would enable any organization to shape a cyber-savvy workforce and ultimately reduce exposure to cyber risk.

Contact

Patrick Kulesa
212.309.3746
Patrick.Kulesa@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 40,000 employees serving more than 140 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/social-media

WTW-GL-17-PUB-8053a1f

willistowerswatson.com

Willis Towers Watson