Empowered employees: The frontline against cyber threats  

by Suzanne McAndrew

While companies understandably make significant infrastructure investments to defend against external cyber threats, they are increasingly recognizing that their biggest security vulnerability is internal and hiding in plain sight, namely, their employees. Willis Towers Watson claims data shows that two-thirds of cyber breaches are caused by employee negligence or malfeasance including losing laptops, the accidental disclosure of information or actions of rogue employees. In fact, only 18% of breaches are driven directly by external threats.

As a result of this growing recognition of the human element in cyber risk, a large majority of employers (roughly 75%) expect to make progress addressing factors tied to human error or actions in next three years according to the Willis Towers 2017 Watson Cyber Risk Surveys.

But what will it take for employers to meet this challenge? First, they need to more fully appreciate the scope of the threat. Next, it's critical for them to understand the strategies and tools that can turn their biggest security vulnerability—employees-- into their first line of defense.

Assessing the insider threat

Most employers say they have established and communicated effective policies and processes to manage the gamut of cybersecurity threats. And most employees indicate that they understand their company’s policies regarding data privacy and information security in their jobs. But, in practice, employees often lack of the awareness, responsibility and accountability required to thwart cyber threats, thus increasing the likelihood of their engaging in risky behaviors. For their part, many employers appear to lack visibility into employees’ poor cyber habits, a clear sign that their cyber risk management strategies are falling short.

Our research reveals opportunities to learn about and improve employees’ cybersecurity behaviors in key risk areas:

**Data privacy and security**

Employees often lack awareness of cybersecurity risks at a basic level. For example, a common and perilous belief among employees is that their organizations' central IT systems are their ultimate protection. This thinking leaves employers exposed to cyber risks, and may explain why roughly 45% of employees say that it’s safe to open any email on their work computer.

Other behaviors that threaten data privacy and security include: using a work computer or cellular device to access confidential company information (approximately 40%); logging into a work device on an unsecured public network or using a work computer in public settings (about 30%); taking confidential paper files home and using unapproved devices to do work at home (roughly 25%).

In addition, employees have a low awareness of data privacy threats by [other] employees or contractors. Only 40% think that a disgruntled employee or contractor could deliberately compromise their organizations’ systems or steal customer/client data.

**Social engineering**

Employees’ risky behaviors can also leave their organizations vulnerable to social engineering attacks where cyber criminals can learn about employees’ activities and profiles which then allows the criminals to convincingly manipulate...
employees into giving up confidential information or data. To this end, our Survey revealed that approximately 69% of employees change the password on their work computer only when prompted. This type of passive behavior can expose organizations to social engineering threats because of the likelihood that employees use the same password across all their personal computing devices and sharing personal information (e.g., date of birth, employer name, job title) on social media sites.

Additionally, not all employees feel empowered to report data privacy and security incidents. Among those who received a suspicious email at work meant to trick them into opening a harmful link or attachment, a fifth did not report the suspicious email to their IT department, thus making it more unlikely for IT to prevent or mitigate potential security issues.

Overall our research findings indicate that many employees lack the “cyber IQ” necessary to protect company and client information. So, how can employers improve employees’ awareness, responsibility and accountability in matters related to cybersecurity? And how can they ensure that the right behaviors are sustained even as cyber threats evolve?

**Building a cyber-savvy culture**

Workforce culture drives employee behavior. Culture generally refers to the shared set of values, principles, assumptions and beliefs that influence how work gets done. Many employers indicate that they are looking to build a culture of cyber risk awareness in their organizations in order to promote employee behaviors that will lessen their vulnerability to cyber threats. Moreover, employers appear to recognize the urgency of this situation. While fewer than half have a formally articulated cyber strategy currently in place, employees’ understanding, awareness and responsibility with respect to this objective by conducting field test of its workers. This practice is done to engage employees and assure customers of the company’s commitment to quality food and service. The same logic applies to cyber risk: as employees adopt more customer-centric behaviors, they will take action to safeguard customer information and lessen the threat of cyber breaches.

Employee feedback mechanisms such as the Willis Towers Watson Cyber Risk Culture Survey can enable employers to gain a deeper understanding of the cultural factors influencing employees’ cyber awareness, responsibility and accountability across their organization. This type of survey can help companies measure the risk inherent in their employees’ behaviors and determine how to lessen this risk.

Willis Towers Watson’s Cyber Risk Culture Survey, grounded in the latest research on employee engagement as well as cyber risk trends, serves as an analytic tool that can identify employee groups within an organization that do not score well on measures of cyber awareness and personal sense of responsibility for cybersecurity. Also assessed is how well an organization and its leaders support a cyber risk culture. For example, survey results measure perceived organizational support for raising security issues and effectiveness of cyber risk training (Figure 1).
This survey also allows companies to compare their results to those of other organizations in their industry and those that have experienced major cyber breaches.

Using the survey insights, organizations can develop an action plan to bridge gaps in cyber risk education as well as overall organizational support for cybersecurity.

### An ongoing learning environment

As companies begin to tackle people risks and build a cyber-savvy culture, they are prioritizing training for their employees and contractors. Over half of employers plan to complete comprehensive training programs on cyber risks for employees in the next two years while over 40% plan to do so for non-employees such as contract workers.

It is with good reason that employers view training as an immediate priority as they have a substantial gap to bridge in this area. About half of employees spent less than 30 minutes on training in the last year. Moreover, 62% of employees completed their training only because it was required by their companies. Therefore, not only do employees need to spend more time in training, they need to move from merely complying with training requirements to tailoring training based on employees’ roles and competencies as well as actively engaging in the training.

To build a cyber-savvy organization, it is essential to create an ongoing learning environment that emphasizes staying up-to-date with business trends and applying acquired skills to business challenges including cybersecurity. Moreover, given the increased use of technology in the workplace and ever-evolving cyber threats, there is a pressing need for ongoing training to keep up with cyber risks.

Companies cannot afford to overlook or underestimate the value of tailored and specific training. In fact, our research reveals that employees in companies that experienced data breaches gave their companies significantly lower scores in the area of training compared to the opinions from employees in high-performing companies².

It is important to avoid a one-size-fits-all approach to cyber risk training. Because employees will have different levels of cyber risk awareness and knowledge, it can be useful to tailor training initiatives to different employee segments. Based on employee responses to questions regarding how they use technology at home and at work, we defined four types of employees:

---

**Figure 1 Cyber Risk Culture Survey**

Sample Results - Training: Item-level scores across major functions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>40 I have adequate time at work to learn about data privacy and</td>
<td>87</td>
<td>-2</td>
<td>2</td>
<td>-4*</td>
<td>-1</td>
<td>2*</td>
</tr>
<tr>
<td>information security risks.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41 I receive regular training on how to protect customer/client</td>
<td>96</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42 I have been well trained in understanding the data privacy and</td>
<td>94</td>
<td>-1</td>
<td>2</td>
<td>-1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>information security risks relevant to my job.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43 Employees new to my department receive adequate training for</td>
<td>67</td>
<td>-2</td>
<td>0</td>
<td>-3</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>their jobs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44 The training I have received has adequately prepared me for the</td>
<td>67</td>
<td>-2</td>
<td>-1</td>
<td>-4</td>
<td>1</td>
<td>-3</td>
</tr>
<tr>
<td>work I do.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>45 There are sufficient opportunities for me to receive training to</td>
<td>82</td>
<td>1</td>
<td>2</td>
<td>-3</td>
<td>-4*</td>
<td>-1</td>
</tr>
<tr>
<td>increase my eligibility for a better job.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

---

*Empowered employees*
Empowered employees

- Aware – those who protect personal information in daily life and are aware of information security at work.
- Comply – those who follow data/information protection policies at work but are careless on a personal level.
- Ignore – those who pay attention to protecting personal information, but who don’t act with the same care at work.
- Unconcerned – those whose technology usage patterns at home and work may lead to potential cyber risks.

Our research shows that just over a third of employees fall into the aware category, yet another indication of the urgent need for cyber risk training.

In planning training, employers should consider that behavior around cybersecurity is strongly linked to training time, work and age. Over 70% of employees who spent at least half a day in cybersecurity training exhibited safe behaviors. The training needs of these employees will differ from those with less training. It is also important to take into account that employees in different functions -- for example, IT vs non-IT staff -- will have different levels of cyber risk knowledge and awareness, and thus require different training. Finally, training needs can also vary by age group. Younger employees report more risky behaviors than their older colleagues. Only roughly a quarter of Gen Y employees meet the “Aware” criteria and thus protect data/information both at home and on the job.

Organizations stand to gain considerable value from cyber risk training. Approximately three-quarters of employees who went through training indicate that the training has improved their understanding of the steps they need to take to protect confidential information and it has increased their sense of personal responsibility for data security at work. Furthermore, employees who spend more time on cybersecurity training are more inclined to report co-workers who breach data protection policies.

Cyber talent strategies

To build a cyber-savvy culture with a robust training component, employers also need to ensure that they have an adequate talent pipeline. IT skills shortages in many companies can contribute to gaps in information security skills and by extension, in a company’s ability to address the human element in cybersecurity. Therefore, it is essential to identify cyber skills gaps and to determine how those gaps will be bridged – i.e., either by hiring new talent or upgrading skills of existing employees. When hiring new information security talent, onboarding should cover cyber risk management processes and procedures, and should emphasize the role of employees in mitigating cyber threats.

In addition to attracting top talent in cybersecurity, employers need to give their existing staff reasons to stay with the organization. Our research shows that IT professionals are concerned about their ability to retain talented information security staff. An effective retention strategy for information security professionals should include ongoing training to keep skills up-to-date and enable staff to advance in their roles as well as rewards programs that motivate employees to give the extra effort needed to address ever-evolving threats effectively. Given the critical importance of attracting and retaining skilled information security talent, organizations may want to consider using tools such as Willis Towers Watson’s cyber work diagnostic tool to develop a comprehensive view of skills gaps and talent deficits, and an action plan to address talent priorities.

Empowered employees – your most effective defense

Robust cyber risk management requires not only state-of-the-art technology solutions but also effective human capital programs. It takes a culture of cyber awareness, responsibility and accountability, an ongoing learning environment and forward-looking talent strategies to build and sustain employees’ “cyber IQ.” These cyber-savvy, empowered employees will serve as your most effective defense against cyber threats.

Sources

1 Data in this paper comes from the Willis Towers Watson 2017 Cyber Risk Surveys of U.S. and U.K. employers and employees.
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.