# Decode the human threat .

## The importance of boosting your organization's "Cyber IQ"

**By Tracey Malcolm and Brian Warszona**

Albert Einstein once said "I never think about the future – it comes soon enough." In many ways, that is exactly where we are today with the Industrial Internet (machines connected to the internet) and the Internet of Things (devices connected to the internet and to each other). This pace has set in motion new insights, expectations and behaviors in our personal lives and at work.

Most organizations in this tech-oriented age have responded with security protocols, authorized computers, firewalls, incident response through dedicated information security teams and broad-based training for employees. Further, encrypting data and having people in place to oversee cybersecurity is now expected.

But is this enough? What can we learn from companies that have experienced data breaches?

### The backdrop: corporate confidence

According to a survey by Willis Towers Watson, 73% of U.S. businesses believe that their organization is highly protected from attempts by outsiders to gain access to their systems and data. Further, 79% maintain that they have the right processes in place to adequately react to privacy and security threats.

**Several cybersecurity studies have concluded that approximately 60% of security incidents are attributable to employee errors such as losing laptops or not updating software.**

Example threats include:

- Phishing emails
- Malicious attachments
- Password and other suspicious requests (cybercriminals posing as employees or contractors to bait employees into divulging information)
- Unauthorized devices on network
- Firewall vulnerability
- Software updates

However, several cybersecurity studies have concluded that approximately 60% of security incidents are attributable to employee errors such as losing laptops or not updating software. The remaining 40% of incidents are hacking related and the result of inadequate network security practices.

What should a cyber risk management and mitigation strategy take into account when focusing on the human factor?

### Workforce culture

Willis Towers Watson recently analyzed employee survey results across its database, with opinions from 450,000 employees, corresponding to a period during which significant data breaches were identified within the firms. We wanted to understand if there were vulnerable aspects of culture risks in data breached companies, and compared these opinion scores with global high–performance organizations with the highest levels of favorable opinion in the database.

Willis Towers Watson

**84%** of cyber functions are anticipating **headcount growth** but are not clear on where they will source the talent.

**86%** of cyber functions plan to change their structure. The need for IS and IT to work together more effectively is driving structural changes. Structure is only part of the solution, as the new requirements for work and culture also need to be defined.

Cybersecurity teams continue to **shift their workforce model rapidly,** frequently **without a plan** for building capacity and capability for cyber work.

**Cyber:employee ratio**
**1:900 with permanent employees**
**1:600 with contractors**

Cybersecurity is shifting to be **"co-led"** with the business as the most predominant partner model. This requires **new skills and hybrid roles** to effectively partner with the business.

Pivotal **roles in cyber** tend to **take longer to recruit and develop,** are more "expensive" to buy, and difficult to retain due to high in demand skills and experiences.

Willis Towers Watson Research

In comparison with high-performance companies, opinions from employees in the data  breached companies are consistently unfavorable when it comes to training. These organizations may not be placing the same emphasis on training for the work employees do. When we consider the increased use of technology at work, coupled with a lack of training, there is a risk of not having the necessary "Cyber IQ" to safeguard information and handle data appropriately.

To create a cyber-savvy organization, there is a need for a learning culture where emphasis is placed on applying acquired skills to business challenges. For data breached companies, this inability to create an ongoing learning environment may reflect a lack of emphasis on staying current with emerging business needs and trends, which could include knowledge of how to circumvent attempts to acquire protected and sensitive data by determined hackers. Some organizations are recognizing how central data security is to their brand, and have taken steps to update employment policies so that repeat offenders of phishing emails are terminated. When we examine the security gaps in breached organizations more closely, IT workers converge on a common theme related to training: inadequate onboarding. For IT staff, onboarding needs to cover the processes and procedures to manage cyber risk given the business environment.

Risk managers must review training and onboarding practices to complete a better assessment of the risk and claims profile of their organization. Meeting with HR, business line leaders and even select employees will help gauge the perception and adequacy of training and whether it is merely viewed as a requirement or something for which these individuals feel a sense of personal accountability.

## Getting "real" about one's cyber workforce

Willis Towers Watson benchmark research has highlighted the real challenges faced by companies as they build, expand and sustain their information security capabilities. There are many required emerging skills in cybersecurity, such as threat intelligence research, architecture and engineering (systems/network/platform), and business acumen. Increasingly, there is a need for hybrid roles that can address the changes in the business with the existing technology and information security requirements.

A risk manager should become familiar with its information security workforce plan, and if one is in place, whether there are role gaps. Where there are gaps, the estimated time to productivity should be determined. For many companies, it often takes 12 – 18 months to effectively onboard employees and for them to be fully productive. Understanding these identified gaps and their prioritization will inform the risk and claims profile.

Through these lenses, what would be the mark on an organization's risk scorecard?

- A strong, risk-averse culture
- Favorable views of training
- Identified talent strategies in information security

The key question underwriters and others who assess risk are now asking is whether there is proper on-boarding and on-going privacy training for employees – including company executives all the way up to the CEO. Targeted phishing attacks (known as "spear phishing") on specific, often high-level individuals in a company are real and employees need to be trained on how to respond. Moreover, many higher executives are routinely granted unnecessary administrative privileges and/or controls making the organization more vulnerable to these security threats.

## The impact of employee training on cyber liability insurance

How are underwriters reviewing this type of training? How can this type of protocol assist the risk management team to get better terms and pricing for their cyberinsurance? While information such as an organization's revenue and industry is commonly used by underwriters in evaluating cyber risk, whether the organization invests in training is often overlooked. One can hypothesize that the investment in specific, detailed training could have a larger impact on underwriting considerations in the future.

Investments in research to assess cyber risks and training of employees is expected to increase relative to the investment in technology measures currently in place to defend against attacks or vulnerabilities. Just a few years ago, organizations were simply asked whether they encrypted their sensitive data. Today, applications ask whether this encryption is at rest, in transit, end-to-end, or point-to-point. Similarly, whereas training of employees has historically been absent from the risk assessment process, underwriters are beginning to ask questions such as:

- How often are your employees trained?
- Are any phishing exercises conducted and how often?
- Are your C-suite employees part of these same trainings?
- How are you managing access to confidential data and critical infrastructure networks?
- Is additional training provided to those with such sensitive access?

It is imperative that organizations start to treat employee cyber risk training with as much importance as software and hardware security tools. This could pay dividends in the long run, by not only avoiding potential cyber incidents, but also by broadening cyber coverage and reducing policy premiums. In some cases, we are already seeing carriers offer a 10% return premium for the use of mitigation services up to a specific dollar amount. We expect this trend to continue in the context of employee training as it evolves and the insurance industry increasingly recognizes its value.

## Contact

Tracey Malcolm
416.960.4490
Tracey.Malcolm@willistowerswatson.com

Brian Warszona
312.288.7850
Brian.Warszona@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-8053a1g

willistowerswatson.com

Willis Towers Watson