
Willis Towers Watson
Decode cyber risk

Willis Towers Watson

Decode cyber risk

A tailored approach to deliver integrated cyber risk management solutions that align cyber risk management with business objectives, support risk transfer and deliver cost effective Cyber Risk Resilience.

People

Through our market leading, global team of cyber risk consultants we provide customized solutions based on each client's unique business operations and priorities.

+

Capital

Our risk transfer solutions, especially in insurance advisory and placement, are tailored to an organization's risk appetite and provide balance sheet protection to address residual financial risk following the implementation of risk management controls and strategies.

+

Technology

Our cyber risk consultants identify, assess and quantify key technology risks, taking a multidisciplinary approach and ensuring that cyber risk strategy and technological solutions are tailored to an organization's business goals and minimize, mitigate, and manage cyber risk across the enterprise to achieve cost effective cyber risk resilience.

=

Cyber resiliency

Needed: A comprehensive organizational strategy for building cyber resiliency

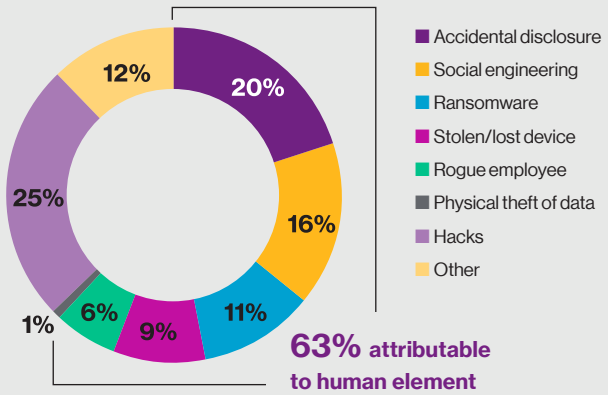
The evolving nature of cyber risk requires a cross functional plan that addresses the full spectrum of client's cybersecurity issues that can include operational, technological, privacy, physical and financial impacts.

More than half of all cyber incidents begin with employees so it's a people and cultural problem too. As a global leader in cyber risk advisory and broking, we aim to simplify cyber risk management strategy into achievable, business wide goals that can address an organization's specific needs across people, capital and technology.

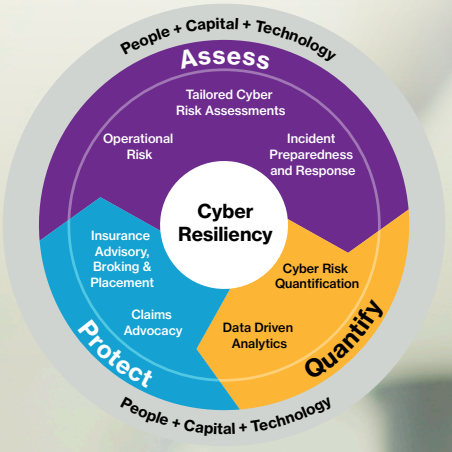
We provide a range of tailored consulting services that can address operational risk, incident preparedness and overarching cyber risk management governance and strategy, alongside quantifying risk through the analytical and assessment tools that enable protection of core assets through innovative coverage solutions and risk transfer strategies.

This fully integrated, holistic approach for managing cyber risk across the enterprise ensures a cross organizational approach to managing this critical risk to ensure comprehensive solutions to cyber risk challenges.

Percentage of claims by breach type



Cyber risk is everywhere. We start by helping our clients decode it.



Assess

We implement a range of tailored services to identify and analyze an organization's core risks across the entire enterprise, focusing on cyber risks affecting people, capital and technology. We identify the gaps and provide practical solutions to reduce risk, achieve business goals and ensure a cyber-resilient organization.

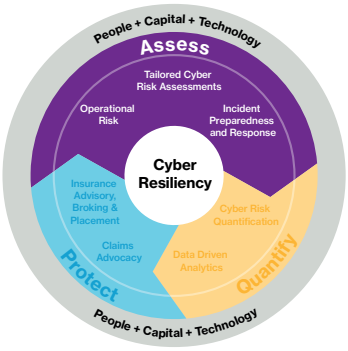
Quantify

We leverage our global experience, incident data and customized assessment tools to provide a strategic suite of best-in-class solutions designed to quantify, inform and mitigate cyber risk exposures.

Protect

Utilizing our leading team of global risk advisors, consultants and insurance specialists, we create tailored risk transfer solutions, ensuring balance sheet protection alongside a range of services to protect our clients after a cyber incident occurs including post incident support, claims advocacy and post incident review and analysis.

Assess



Our holistic approach to assessing cyber risk evaluates all threats - people, capital, technology - to ensure that our client is best prepared to protect and grow its business. We appreciate that no two organizations are the same: The development and execution of a comprehensive cyber risk management strategy must be tailored to an organization's specific needs which alter over time. Our approach is to listen to a client's needs, then determine a tailored solution to achieve there business goals. Drawing from a cross disciplinary, global team of consultants, we can develop customized consulting services focused on client needs, including:

a. Risk Assessment and Quantification

b. Incident Response Preparedness and Planning

c. Insurance and cybersecurity alignment

d. Operational Risk Analysis

e. Business Continuity Planning

f. Employee Training and Awareness

While no two engagements are the same, we first listen to our client's need and then develop tailored solutions that can include:

a. Cyber Risk Diagnostic Workshops, aligned with NIST or ISO cybersecurity framework

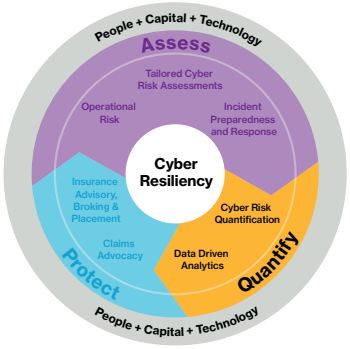
b. Executive Workshops

c. Incident Response and Business Continuity Plan testing and Improvement

d. Risk Quantification and Peer Benchmarking projects

e. Cybersecurity policy review and analysis

f. Insurance Feasibility and Quantification



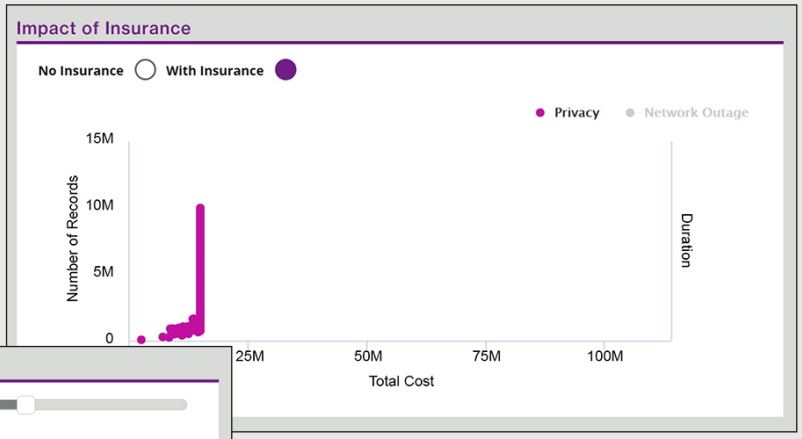
Quantify

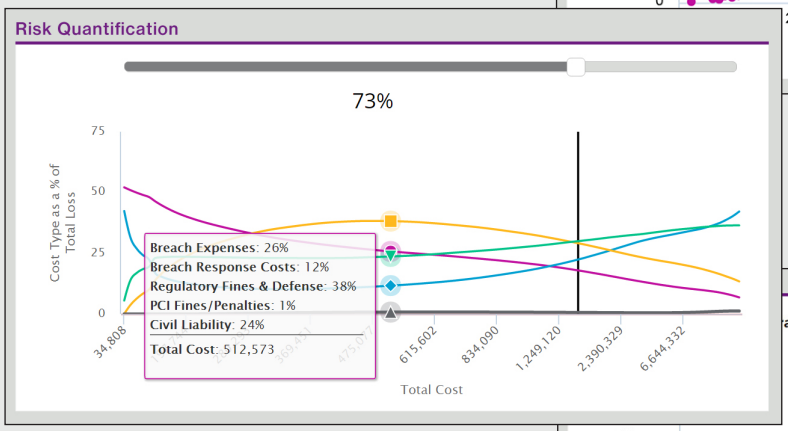
Protection requires understanding the consequences

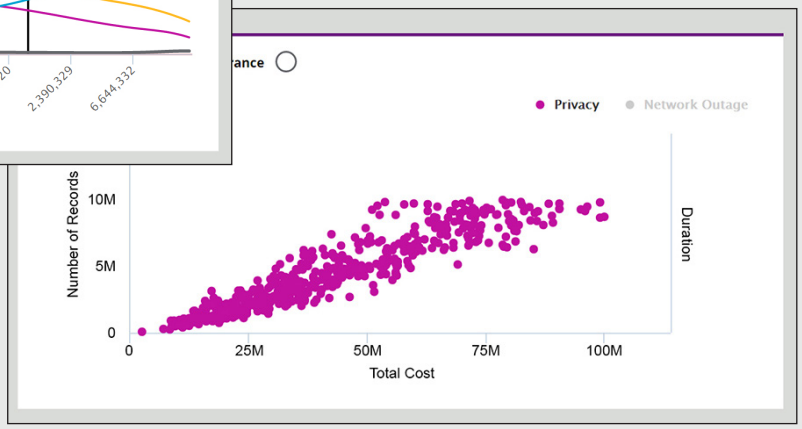
We leverage our global cyber insurance claims data, organizations' cybersecurity maturity data and other customized data to help organizations quantify and benchmark the financial impact of cyber risk. This process enables organizations to make informed and sound decisions regarding their capital allocation and mitigation strategies.

Cyber Quantified

This innovative and proprietary analytical tool is part of the broader suite of Willis Towers Watson's Core Analytics "Quantified" models. Cyber Quantified is designed to quantify the financial impact of cyber incidents. It estimates frequency and severity of cyber incidents to determine a company's risks and financial exposures arising from both privacy breach and network outage events. Cyber Quantified provides decision support to clarify insurance purchases and guides a company to its optimal risk transfer strategy.







How boards can lead the cyber-resilient organisation

A study conducted by The Economist Intelligence Unit (EIU) and sponsored by Willis Towers Watson, aims to explore organisations' efforts to become cyber resilient – and, in particular, how board oversight can enable this strategy.

The stark reality

Serious cyber incidents

1/3 of companies surveyed reported one

Most place high odds it will happen again in 12 months

Vulnerabilities exist

Workforce resiliency needs much improvement.

Executives who rate their cyber-resilience competencies well above average

13% Applying lessons learned (worst self-assessment)	**21%** Integrating technology and governance post-acquisition
15% Ability to develop a cyber-savvy workforce	**14%** Ability to identify and fill talent gaps

There's room for improvement

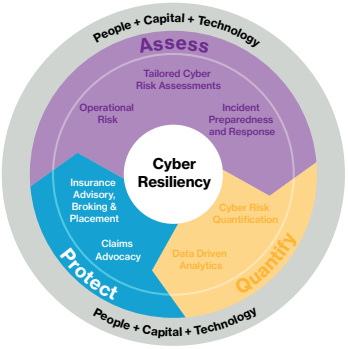
Executives don't believe their companies are spending enough on cyber-resilience.

What investments should look like:

15%	50%	23%	6%	6%
No change	Up by 10% or less	Up by 11+%	Down by 10% or less	Down by 11%+

How executives think that investments should be deployed:

Technology	20%
IT talent acquisition, skills training/development	19%
Business continuity and disaster recovery	16%
Rewards and incentives	16%
Training	15%
Insurance	14%

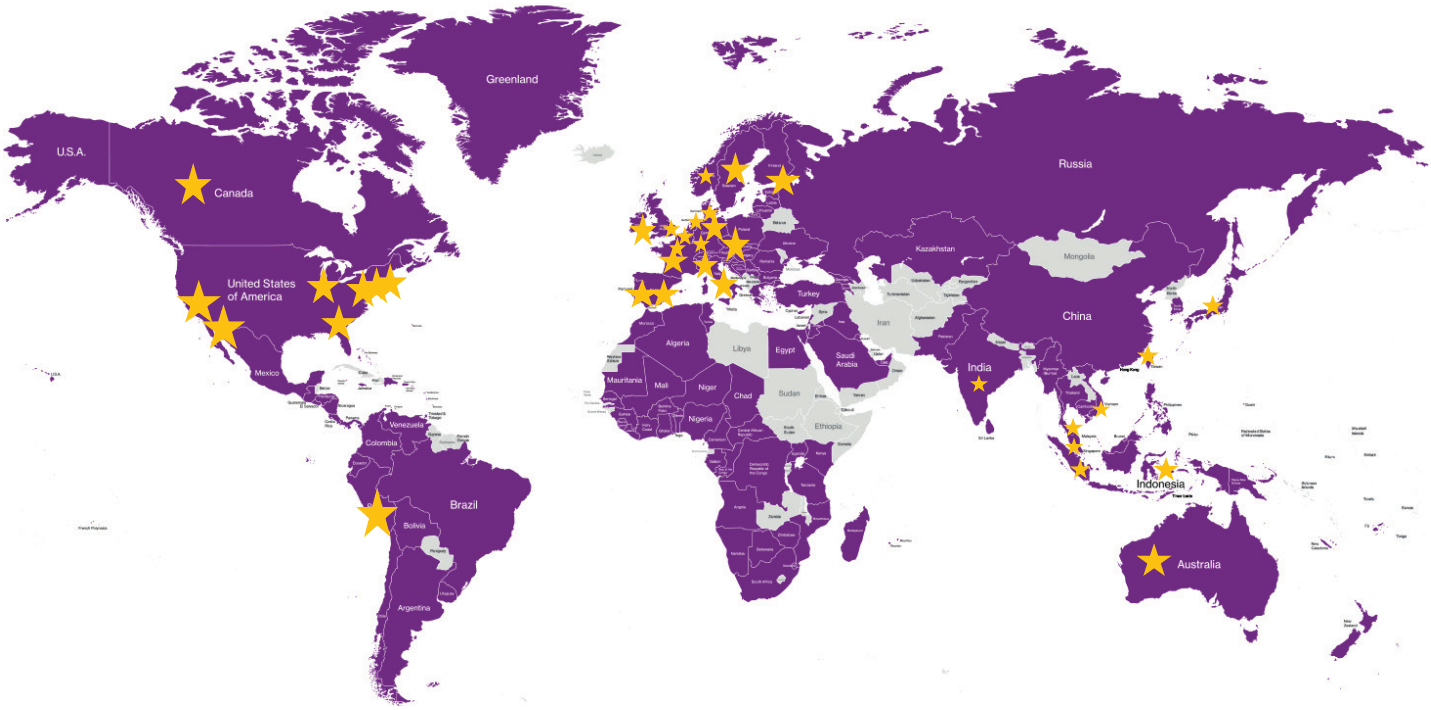


Protect

To achieve financial resilience an organization must understand the impact of unforeseen events on it's bottom line. This is why we also protect organizations through the negotiation and placement of best-in-class cyber insurance policies. And when an incident occurs, we move with speed and flexibility to provide incident response support and claim notification to insurers. We help recover losses under relevant insurance policies and provide deep analysis to learn causes and quickly develop new strategies to maximize insurance recovery.

Why Willis Towers Watson?

We are a trusted advisor partnering with a wide range of cybersecurity companies across the globe for clients of all sizes to complement their specific needs.



20+
Global locations with cyber resources

100+
Cyber insurance specialists

400+
Large global clients

Cyber Insurance Advisory and Broking

As technology has become a driver of business models, cyber risk has grown into a systemic threat to successful operations. Now more than ever, businesses need to protect themselves from threats that could jeopardize their financial growth and sustainability. Willis Towers Watson's insurance advisory broking expertise is unrivaled in the marketplace. With over 50 brokers globally, we strive to help organizations make informed and meaningful risk transfer decisions, relying on the results from our various assessment and risk quantification tools.

Claims Advocacy

In the event of an incident, our experienced claims advocates work closely with the client's response teams – both internal and external – to coordinate the client's notice to insurers, where applicable. Our claims advocates – all attorneys – provide organizations with guidance regarding claim notification and work to ensure that the costs and losses incurred as a result of the incident are covered to the extent specified under the policy terms and conditions.

Cyber risk is evolving. Organizations' resiliency plans should too.

Cyber threats are dynamic and more complex than ever, and millions of dollars (if not tens of millions) in loss of customer loyalty and reputational damage are at stake with every incident. Now, more than ever, a fully integrated, comprehensive solution that manages people, capital and technology risks to create a cyber-savvy workforce and resilient organization is a priority.

Why Willis Towers Watson

More than half of all cyber incidents begin with employees, so it's a people problem. And the average breach costs $4 million, so it's a capital problem, too. No one decodes this complexity better than Willis Towers Watson. As a global leader in human capital solutions, risk advisory and broking, we are well prepared to assess your cyber vulnerabilities, protect you through best-in-class cybersecurity solutions and radically improve your ability to successfully recover from future attacks.

Explore comprehensive cybersecurity solutions at willistowerswatson.com/cyber.

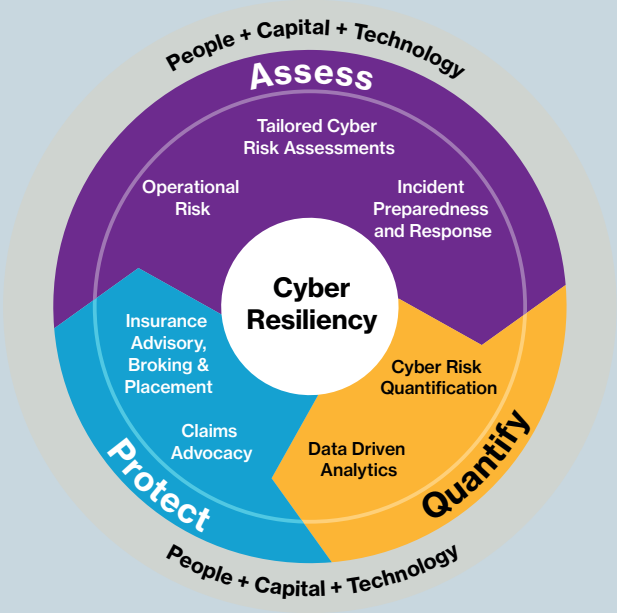
The mean number of breached records per claim is over 693,000.

Nearly one in ten breaches involved more than 20,000 records.

The direct event cost per breached record is $7.95.

For 10% of settled claims, the total cost (including defence costs/other expenses) exceeded $2.5 million.

Source: "Cyber Claims Data Analysis Report", Willis Towers Watson, June 2020.



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 45,000 employees serving more than 140 countries and markets. 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

willistowerswatson.com

Willis Towers Watson