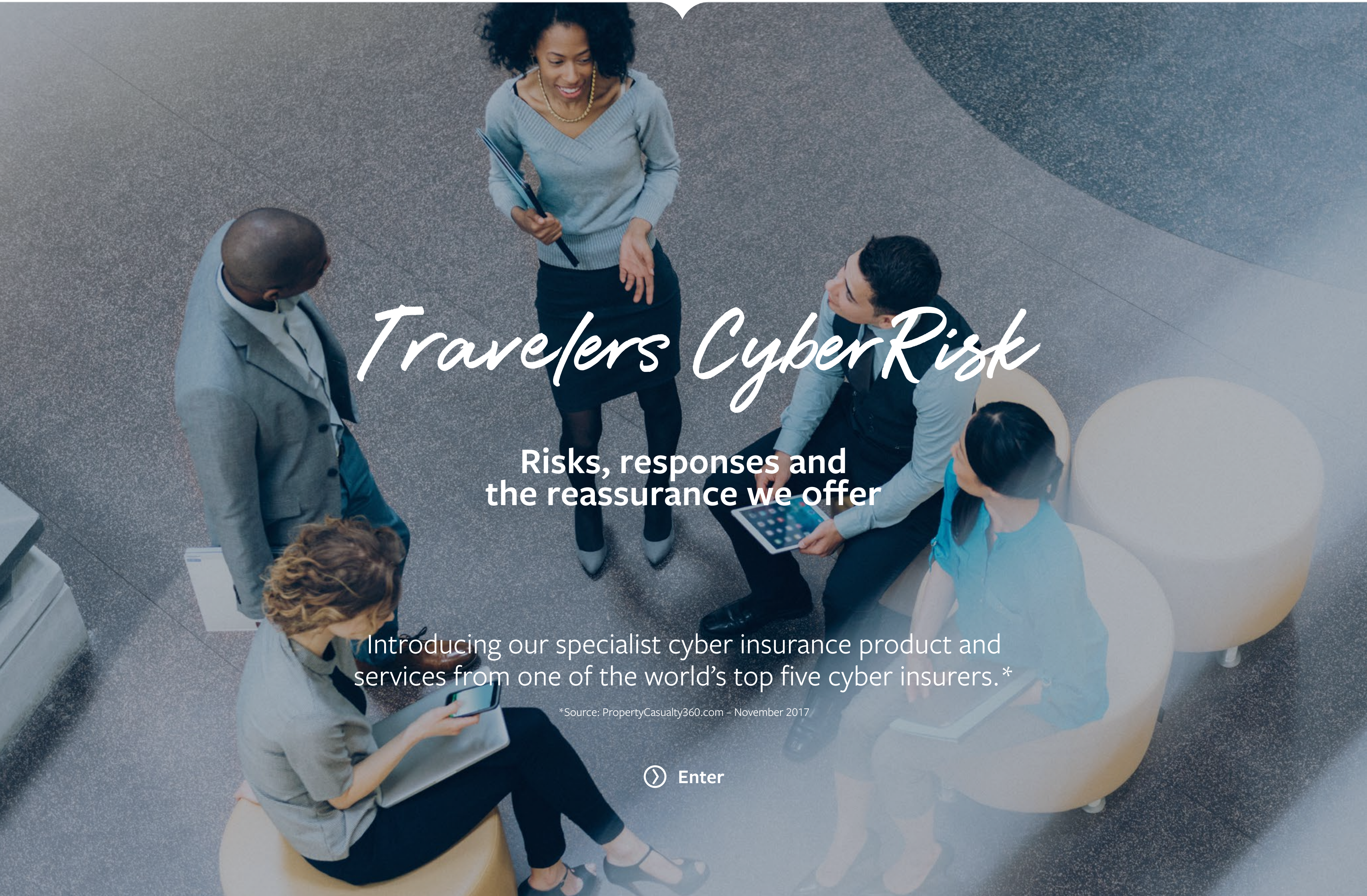
TRAVELERS



Travelers CyberRisk

Risks, responses and the reassurance we offer

Introducing our specialist cyber insurance product and services from one of the world's top five cyber insurers.*

*Source: PropertyCasualty360.com – November 2017

Enter

Overview

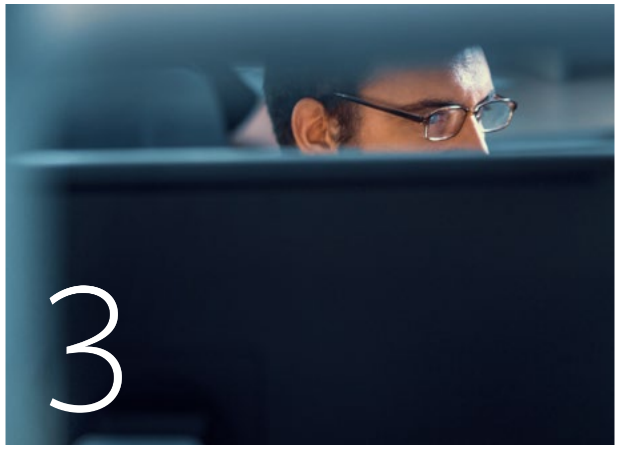
How Travelers CyberRisk can help your clients to stay safe amidst the ever-evolving challenges of cyber security.

→

Our CyberRisk product

A comprehensive range of first and third party insuring clauses covering Breach Response, Cybercrime, Business Loss and Cyber Liability.

→



Who we work with

Our expert partners specialise in Breach Response and assist during the claims process, from initial response through to final payment.

→

Quote & bind

CyberRisk is available either as a standalone policy or as part of a management liability package and can be purchased through our e-trading platform MyTravelers.

→

Claim scenarios

To help bring cyber exposures to life, we look at some examples of risk scenarios and Travelers' policy response.

→

Risk Management

By partnering with Travelers to help understand and manage their risks, customers can manage their cyber exposure

→

About Travelers

Market-leading expertise and speciality insurance across multiple sectors, from one of the world's top five cyber insurers.

→

Travelers CyberRisk – protecting the future of your client's business

In today's data-driven world, keeping information, data and finances safe and secure online is essential for almost any organisation.

As the CEO of the National Cyber Security Centre has stated:"UK businesses must treat cyber security as a top priority if they want to take advantage of the opportunities offered by the UK's vibrant digital economy.[1]"

In addition, a UK government report found that 78% of UK businesses say that cyber security is a high priority for their organisation[2]. So, the government and most businesses are agreed: cyber security is very important to them.

The good news is that Travelers, one of the world's top five global insurers for cyber insurance, can help. Travelers CyberRisk provides a range of specialist covers, services and other benefits, designed to protect businesses or other organisations from current and emerging cyber threats.

CyberRisk is a standalone product but can be bought additionally when purchasing a product from our Management Liability Package, which includes Crime, Directors and Officers, Employees Practices Liability and Pension Trustee Liability.

For more information see the **Quote & bind** section.

Cyber security – a growing and evolving concern

The top three causes of data breach are malicious or criminal attacks, human error and system glitches[3], so it's not surprising that, while typical scenarios may differ, all industry sectors are vulnerable.

The UK's National Crime Unit has reported that cybercrime has overtaken all other forms of crime for the first time ever, with over two million incidents recorded annually. 40% of small businesses and 60% of medium businesses identified a cyber breach within the last 12 months.[2]

Cyber attacks are also continually evolving and becoming more sophisticated – recent high-profile ransomware cases are just one example of this.

In addition, despite advances in technology (or in some cases because of it) and more widespread awareness of cyber vulnerabilities, human and system error are ever-present threats. Everything from a lost laptop to a disgruntled employee can now pose a major risk.

Data protection laws focusing attention on an individual's privacy rights, the growth of cloud computing, the increasing use of social media as well as corporate 'bring your own device' policies are all factors in raising the risk stakes.

Why Travelers CyberRisk is the answer

Proper protection is therefore essential. But without dedicated cyber insurance, a business is not likely to have complete insurance coverage. Travelers' research has found that only 20% of companies currently have a cyber insurance policy, although over 70% overall say they expect to buy it.

CyberRisk protects against a wide range of first and third party losses. This includes cover for data breach, fines and penalties (if insurable by law), losses from business interruption, plus cyber extortion, social engineering and other financial cybercrimes, in addition to third party cyber liability claims. CyberRisk also gives the insured access to specialist professional advice and teams, including from our expert breach response partners, Pinsent Masons.

There's also the reassurance that comes from being with a global top five cyber insurer and a company that has been safeguarding UK businesses since 1990.

In this guide, we'll look at our CyberRisk product, our breach response service, the quote & bind process and the various cyber security threats across different scenarios, together with the flexible and innovative ways Travelers CyberRisk can mitigate the harm such threats can cause – and even help to prevent them.

[1] Quoted in National Cyber Security Centre press release, April 2017 [2] Cyber Security Breaches survey 2019 [3] Ponemon Institute Cost of Data Breach Study 2017

CyberRisk Policyholder Benefits

Travelers eRisk Hub®:

Access to a private web-based portal containing information and technical resources that can assist you in the prevention of network, cyber and privacy events and support you in a timely response if an incident occurs.

Travelers eRisk Hub portal powered by NetDiligence® features news, content and services from leading practitioners in risk management, computer forensics, forensic accounting, crisis communications, legal counsel, and other highly-specialised segments of cyber risk.

Please note the following:

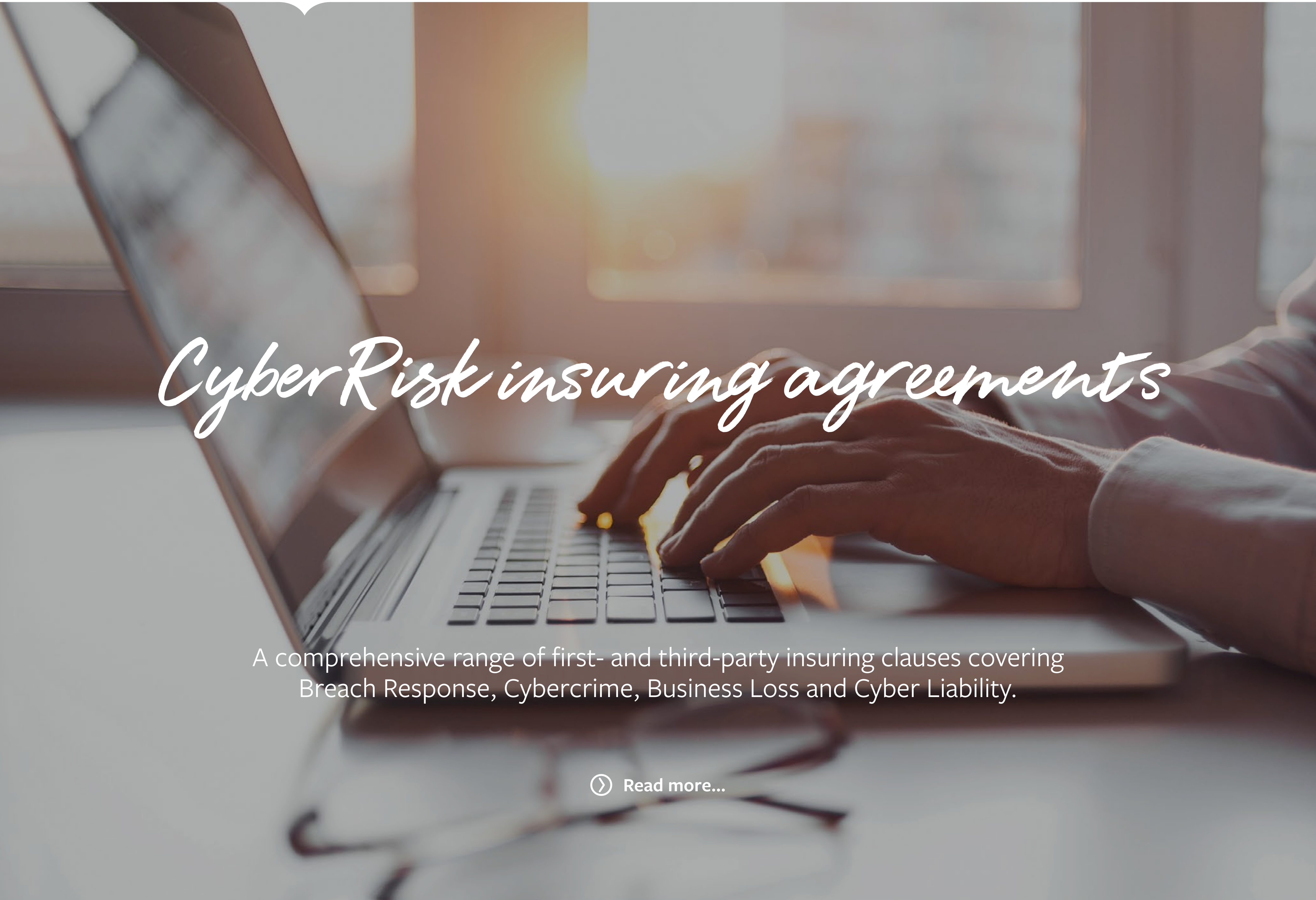
- Travelers eRisk Hub is a private site provided to certain cyber insureds of Travelers. Please do not share portal access instructions with anyone outside your organisation. You are responsible for maintaining the confidentiality of the Access Code provided.
- Travelers eRisk Hub contains a directory of experienced providers of cyber risk management and breach recovery services. Travelers does not endorse these companies or their respective services. Before you engage any of these companies, we urge you to conduct your own due diligence to ensure the companies and their services meet your needs. Unless otherwise indicated or approved, payment for services provided by these companies is your responsibility.

Prevention benefits:

- Access to experts who can help your organisation build or improve its cyber programmes
- News centre with the latest cyber-related headlines
- Tools to build privacy controls as well as information and IT security programs
- Learning centre featuring white papers, articles and upcoming webinars on a variety of topics including business interruption, forensics, compliance and security awareness
- Resources for statutory, regulatory and case law updates regarding privacy liability and notifcation obligations.

HCL Technologies pre-breach services

- **Cyber Resilience Readiness Assessment and Cyber Security Professional Consultation** An online assessment designed for an organisation to quickly understand their current cybersecurity posture while receiving an official report and up to 1 hour consultation with a HCL Technologies security professional to help in improving areas of weakness or vulnerability.
- **Cyber Security Awareness** Training Gain access to security awareness training as a method of defence against cybersecurity threats by promoting proactive employee behaviour. These courses can be accessed on a cloud-based learning management system hosted by HCL Technologies or on your existing SCORMcompliant LMS platform.
- **Risk Management Expertise** Topical insights and expertise on current cyber related trends, risks and threats that face organisations in today's business environment. These resources will help with your organisation's preparedness when it comes to cyber related events
- **Service Discounts** Obtain meaningful discounts on HCL Technologies services and solutions including HCL Technologies Endpoint Potection (SBE), DeepSight™ threat intelligence, HCL Technologies Managed Security Services, HCL Technologies Incident Response Tabletop Assessments, and more.



CyberRisk insuring agreements

A comprehensive range of first- and third-party insuring clauses covering Breach Response, Cybercrime, Business Loss and Cyber Liability.

Read more...

CyberRisk coverage

As a global top five cyber insurer, Travelers understands the potential cyber exposures businesses face, and how to properly assess these; ensuring your clients are fully protected, with additional breach response support and expert claim assistance. It's also why there are a comprehensive range of first- and third-party insuring clauses in our CyberRisk policy spread across: Breach Response, Cybercrime, Business Loss and Cyber Liability.

Liability Insuring Clauses:

Privacy and security

Coverage for claims arising from unauthorised access to data, failure to provide notification of a data breach where required by law, failure to destroy confidential information, failure to comply with a privacy policy, wrongful collection of private or confidential information, failure to prevent a security breach that results in the inability of authorised users to gain system access, the participation in a DDoS attack, or the transmission of a computer virus.

Media

Coverage for claims arising from copyright infringement, plagiarism, defamation, libel, slander, and violation of an individual's right of privacy or publicity in electronic and printed content.

Regulatory

Coverage for administrative and regulatory proceedings, civil and investigative demands brought by domestic or foreign governmental entities or claims made as a result of privacy and security acts or media acts.

Breach Reponse Insuring Clauses:

Privacy Breach Notification

Coverage for costs to notify and provide services to individuals or entities who have been affected by a data breach. Examples include call centre services, notification, credit monitoring and the cost to purchase identity fraud insurance.

Computer And Legal Experts

Coverage for costs associated with analysing, containing, or stopping privacy or security breaches; determining whose confidential information was lost, stolen, accessed, or disclosed; and providing legal services to respond to such breaches.

Betterment

Coverage for costs to improve a computer system after a security breach, when the improvements are recommended to eliminate vulnerabilities that could lead to a similar breach.

Cyber Extortion

Coverage for ransom and related costs associated with responding to threats made to attack a system or to access or disclose confidential information.

Data Restoration

Coverage for costs to restore or recover electronic data, computer programmes, or software lost from system damage due to computer virus, denial-of-service attack or unauthorised access.

Public Relations

Coverage for public relations services to mitigate negative publicity resulting from an actual or suspected privacy breach, security breach, or media act.

Rewards

Coverage for rewards paid for information that directly leads to the conviction of any person for committing or attempting to commit an illegal act related to the cover provided under the policy.

Cyber Crime Insuring Clauses:

Funds Transfer Fraud

- Coverage for loss of money or securities due to fraudulent transfer instructions to the Insured's financial institution.
- Coverage for loss of money or securities due to a person impersonating another and fraudulently providing instructions to transfer funds.
- Coverage where due to a security breach the insured's client or vendor is duped into sending money or products to a fraudster rather than the rightful recipient.

Computer Fraud

Coverage for loss of money, securities, or other property due to unauthorised system access.

Telecom Fraud

Coverage for amounts charged by a telephone service provider resulting from an unauthorised person accessing or using an insured's telephone system.

Business Loss Insuring Clauses:

Business Interruption

Coverage for loss of income and expenses to restore operations as a result of a computer system disruption caused by a virus, computer attack or system failure, including the voluntary shutdown of systems to minimise the business impact of the event.

Dependent Business Interruption

Multiple coverage options for loss of income and expenses to restore operations as a result of an interruption to the computer system of a third party that the insured relies on to run their business.

System Failure

Coverage for loss of income and expenses to restore operations as a result of an accidental, unintentional, and unplanned interruption of an insured's computer system.

Reputation Harm

Coverage for lost business income that occurs as a result of damage to a business' reputation when an actual or potential cyber event becomes public.

The CyberRisk journey

From breach to business as usual

Introducing our breach response service
and how a typical claim process unfolds.

Read more...

Introducing the role of the Breach Coach

As data breaches become increasingly complex, a new role has emerge to help businesses navigate their response and recovery – the Breach Coach. They can help to identify the scale and nature of the cyber event, isolate any affected data, notify customers where necessary, retain forensic professionals and manage public communications.

At Travelers, we partner with Pinsent Masons for Breach Coach services:

- They have unique knowledge and experience of over 10 years across hundreds of breaches, plus the breadth of expertise to be able to respond to an insured's needs. That includes understanding of the credit monitoring environment, the regulatory requirements and experience in insurance.
- Their cyber risk experts combine a deep understanding of technology and data protection law plus practical experience of successfully managing data breaches and security incidents. Their cyber team are part of a Technology Media and Telecoms (TMT) practice rated Tier 1 by the Legal 500.
- Their knowledge of the underlying technology means they can discuss technical matters with any expert and ensure the scope of any investigation is sufficiently wide-ranging, but not excessive, thereby controlling cost and speed of resolution.
- As solicitors, communications with third party experts can gain extra privilege and protections. This can be particularly important with litigation claims and/or regulatory investigations led by a data protection authority or a financial regulator. Non-legal advisors cannot offer the same potential protection.
- Cyber breaches often affect multiple jurisdictions, so it's an advantage that Pinsent Masons is an international company. They have offices throughout the UK, in 28 European countries, and in Asia, Africa and the Middle East. They are thus capable of providing the quick international response that will often be needed.
- Their team works to a proprietary breach methodology based on internationally recognised standards, including the European Union Agency for Network and Information Security (ENISA) Good Practice Guide for Incident Management.

Why speed matters

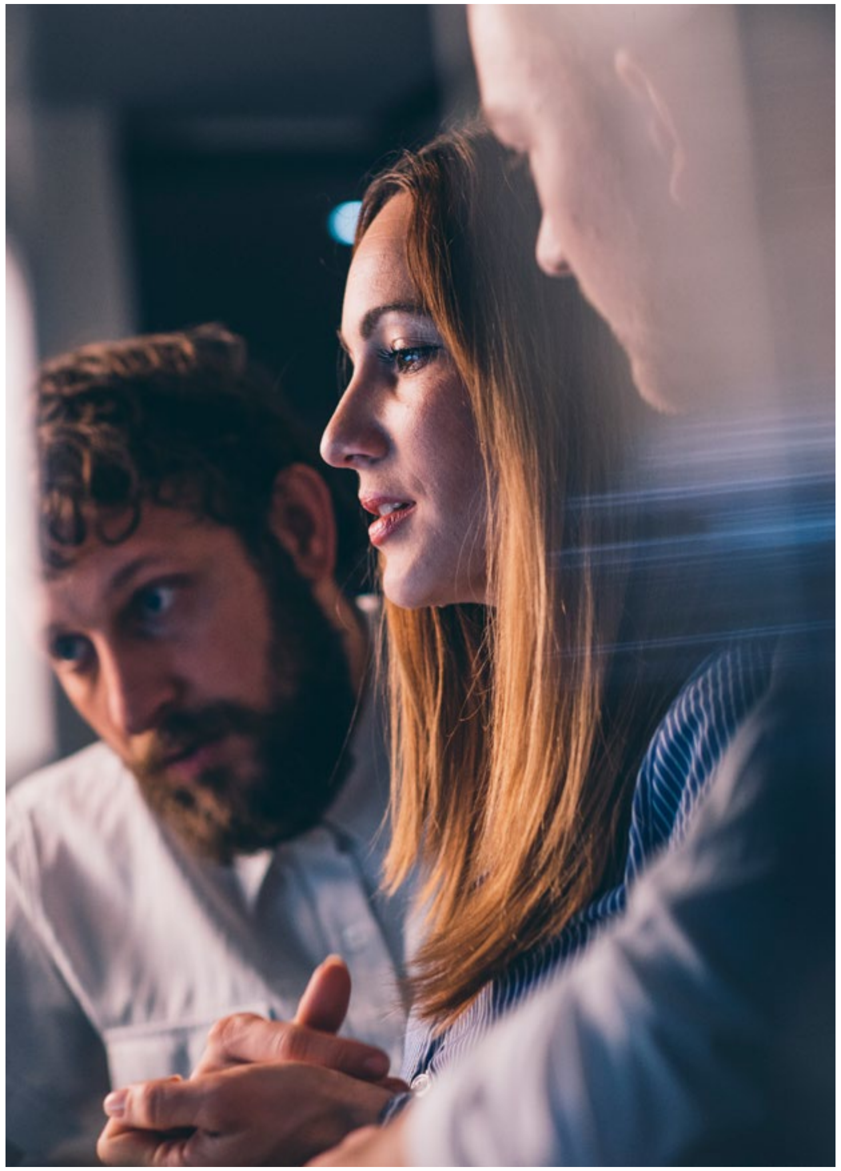
By providing a fast, decisive response immediately after a breach is discovered, Pinsent Masons works with Travelers to ensure the right course of action is taken – and helps to mitigate potential system damage plus data and financial losses.

The General Data Protection Regulation (GDPR) requires businesses to notify their customers of a possible breach of their data without delay; they must also notify the Data Protection Authority within 72 hours. Thus helping insureds comply with the law.

How it works

When an insured discovers that a breach has occurred, Pinsent Masons will act as their first port of call via the Breach Coach Helpline. This is open 24/7/365 and response is guaranteed within two hours between 8am and 8pm, and within four hours at other times.

For more information, see our six-step process



The CyberRisk breach response journey

The CyberRisk claims process follows a defined path. It's designed to make it easy to initiate contact and to ensure a prompt response – often vital when it comes to handling cyber events.

In addition, the insured will have access to expert assistance at handling the event (not just the claim) right from the outset. That's thanks to the Breach Coach Helpline, which offers up to 30 minutes of immediate initial support, followed by a prompt triaged response from Travelers and Pinsent Masons, our breach response partner.

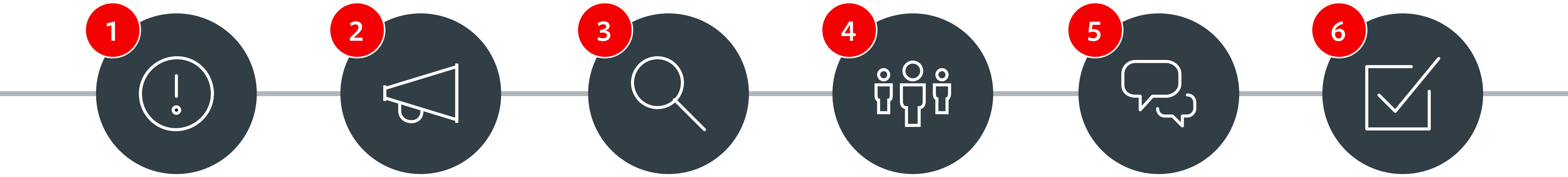
Pinsent Masons will coach the insured through all stages of a cyber event, including assessing the legal responsibilities of the situation and recommending a correct course of action. They will also ensure the retention of all necessary response providers, such as computer forensics experts to assess and, if necessary, mitigate computer breaches, and public relation firms to manage communications.

Our claim professionals can also call on global resources, including IT experts and technicians with the background and experience to investigate any loss scenario.

In addition, as a global top five cyber insurer, Travelers can call on a vast repository of technical information gathered during thousands of claim investigations. It also means that our claims professionals are able to provide the necessary guidance, assistance and reassurance for insureds as required.

The result is a seamless process – and one in which, at all stages, you and your client will be kept informed as the situation is being resolved.

A straightforward six-step process



Discovery

Insured discovers a suspected cyber event.

Alert

They contact the Pinsent Masons Breach Coach Helpline, which is available24/7/365.

All Travelers Insureds have access to a 30-minute consultation call with Pinsent Masons free of charge, in the event of an actual or suspected cyber event.

Assessment

A member of the Travelers claim team will contact you to discuss your cyber event to agree next steps and priorities in conjunction with Pinsent Masons.

Engagement

Travelers establishes a dedicated team from a network of industry leading vendors in order to respond quickly and effectively to the cyber event.

As well as the Breach Coach, these can include:

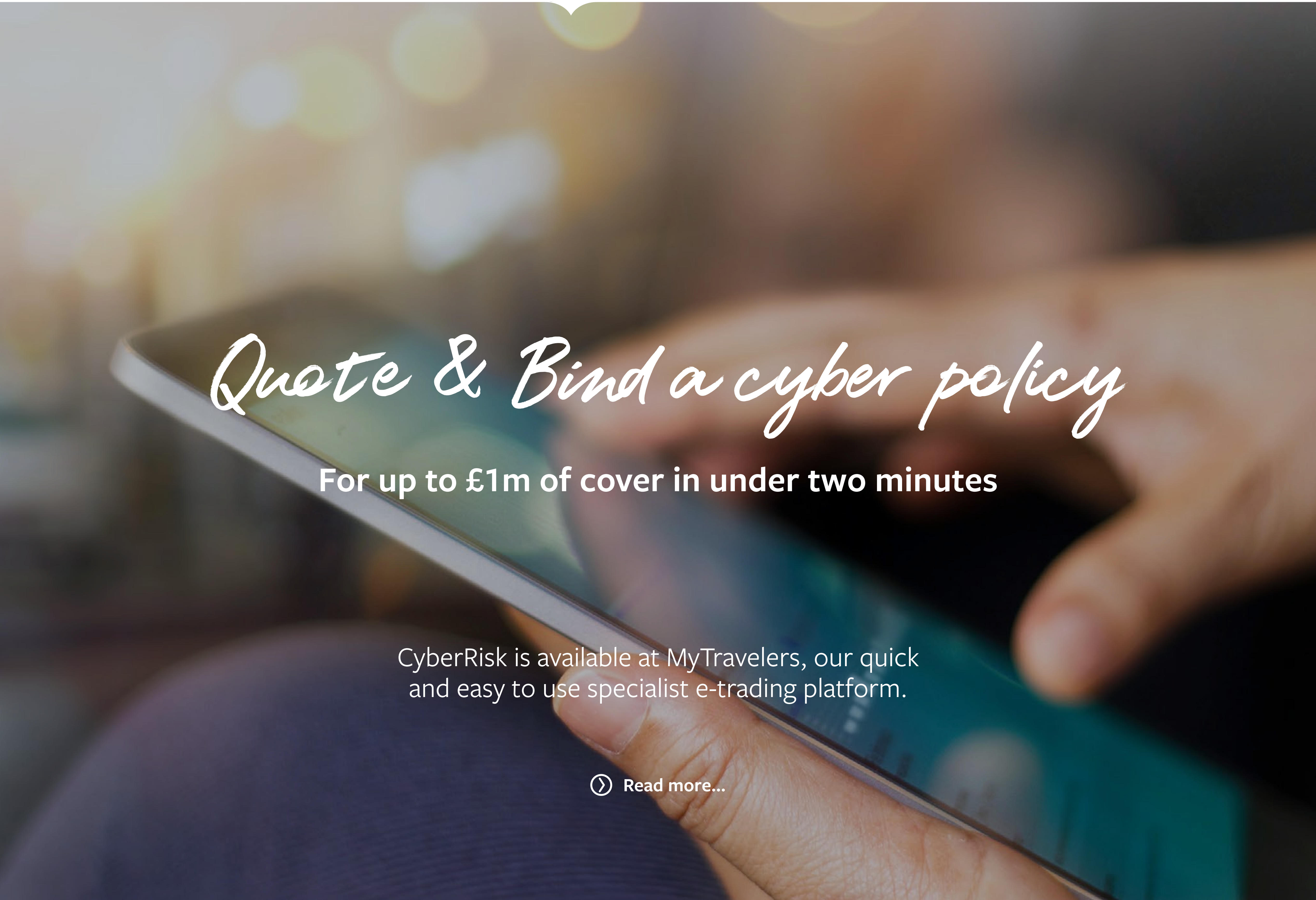
- Forensic investigators
- Public relations firm
- Notification vendor
- Call centre vendor
- Credit monitoring service

Communication

Both you and the insured are kept informed throughout the process with direct and regular contact with the Travelers cyber claim professional during business hours.

Resolution

Thanks to our experience and the industry leading experts we call on, Travelers ensures that the event is resolved as quickly and smoothly as possible, allowing the insured to get back to normal business operations.



Quote & Bind a cyber policy

For up to £1m of cover in under two minutes

CyberRisk is available at MyTravelers, our quick and easy to use specialist e-trading platform.

Read more...

How to obtain a CyberRisk quote

The best route for obtaining a quote is via MyTravelers, our specialist e-trading platform. This is the easiest and quickest way, with the ability to generate **a quote and bind up to £1m of cover in under two minutes.** That's great news for brokers and customers alike. There is also a wealth of other information and benefits available on MyTravelers.

MyTravelers – your e-trading platform for a range of useful and secure applications.

As well as online quotes and claims statistics , you can find industry-specific risk control information as part of our comprehensive suite of bespoke risk management services . It's also the place where we will send you details of new products and services whenever they become available.

In the next section, you can find a quick guide on how to quote and bind a CyberRisk policy in under two minutes.

MyTravelers: our e-trading platform

MyTravelers set up and login

Get set up on MyTravelers in four simple steps.

1. Enter your account details plus your postcode, broker agency code and email.

2. Add your personal details, including title, first name and last name, with the option of including your telephone number or mobile.

3. Enter your business address.

4. The final step to set up your MyTravelers account is the security section.

You will need to confirm whether you are an existing user, plus enter your email address and password, as well as your security question and answer.

To refresh your MyTravelers login, click here: **www.mytravelers.travelers.co.uk/wps/portal/trv/login/forgotten**

If you are already registered for MyTravelers, you can access the platform by clicking on the '**Login**' link found at the top righthand side of Travelers.co.uk

Bespoke quotes in under two minutes

We've cut the need for referrals down to an absolute minimum and created a streamlined four-step process. This allows you to generate quotes of up to £1m cover in under two minutes and bind your client's coverage in just one click.

1. Insured search

The process begins when you either input the insured's company details or search for them by company registration number. Once the company is identified, the system will automatically populate the details.

2. Insured details

Next, you'll find your details and the insured's details for you to validate. You can check the insured's business activity, turnover, year of incorporation and company structure to ensure these are accurate.

3. Tailor cover

Now you can choose the cover you want. You can also select the limits and length of policy term. In addition, you'll be prompted to check a number of material facts about the insured company, including claims history.

Finally, you state when you want cover to begin.

4. Receive quote

The fourth step will provide your quote and the date to which it is valid. There is confirmation of the insured with summaries of each of the covers. Any of these can be removed and the commission adjusted, as required.

There is also a link to the quote schedule and policy wording which can be emailed or copied into another document or system in plain text.

While quoting for CyberRisk you can also consider adding a Management Liability policy, which includes Crime, Directors and Officers, Employment Practices Liability and Pension Trustee Liability. There are buttons during the user journey that let you do this easily.

Finally, check the last summary before confirming and binding the policy.

Bind

Once the policy is bound, you'll find a quote reference number along with the Insured's policy reference. The policy schedule and wording are automatically emailed to you, but you'll also be able to download these from MyTravelers as necessary.

〉 Read more...

MyTravelers: our e-trading platform

The little extras

Our streamlined quote & bind journey offers a flexible, intuitive experience with all the support and extras you need to keep track of everything.

It allows you to:

- Generate multiple bespoke quotes in a few clicks
- Save as you go and amend information at any time
- Exit the system whenever you like and get straight back to where you left off
- Choose from multiple limit options
- Tailor the end date to align with your other policies
- Adjust your commission settings
- Copy and paste quotes directly from the system to other documents
- Create multiple quote options and bind only the parts you need
- Access the Live Chat function throughout your journey, giving instant access to underwriters

And remember, the online quote & bind process for cyber cover of up to £1m can take under two minutes.

How to use it

The first time you log in, you'll be able to take an interactive tour through the system which highlights its features.

How we will support you

We know how referrals can delay and hinder getting quotes, so we've invested a lot of effort in designing a system that is flexible enough for your more complex or non-standard risks. As a result, referrals have been cut down to an absolute minimum.

We have also added convenient new features to make sure you can get our support at any point while using the system.

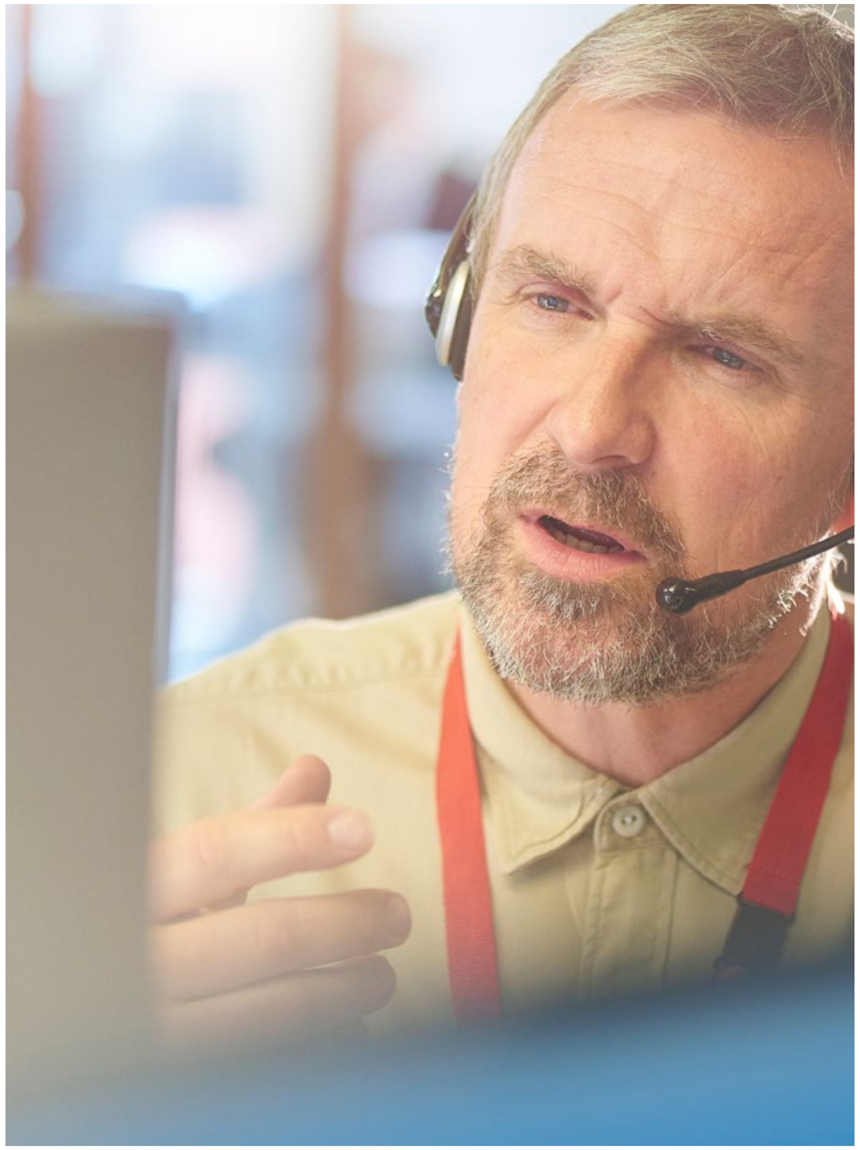
Live chat

We offer a Live Chat feature which you can use as much as you want during your quoting journey. It allows you to chat directly to a member of the Cyber Team between 9am and 5pm Monday to Friday.

48 hr referral resolution

Should you be referred, a member of the Cyber Team will get back to you within 48 hours to resolve the issue. If the matter is urgent, however, please give us a call on 020 3207 6185 and we will work with you to resolve the issue.

Read more...



MyTravelers: our e-trading platform

By registering on MyTravelers, you will access this set of 'open applications' (visible to all), viewable once you log in.

Account Management

View and update your details or change your password. If you are designated as an administrator, then you can also use the Account Management section to add or remove users.

Claims Reports

This is a reporting tool for all claims linked to the broker agency code of the account. It provides a list of options for users to build and customise the Microsoft Excel report themselves. It can then be partly or completely downloaded as required.

Risk Control

Within this section of MyTravelers, our Risk Control team provides peace of mind for customers by helping them understand the various risk exposures. Information and resources here include sector guides, technical bulletins, useful checklists, factsheets, sample forms and webinars.

Our industry experience and knowledge allow us to provide guidance and best practice controls, making businesses more resilient to loss and disruption.

Sales & Marketing

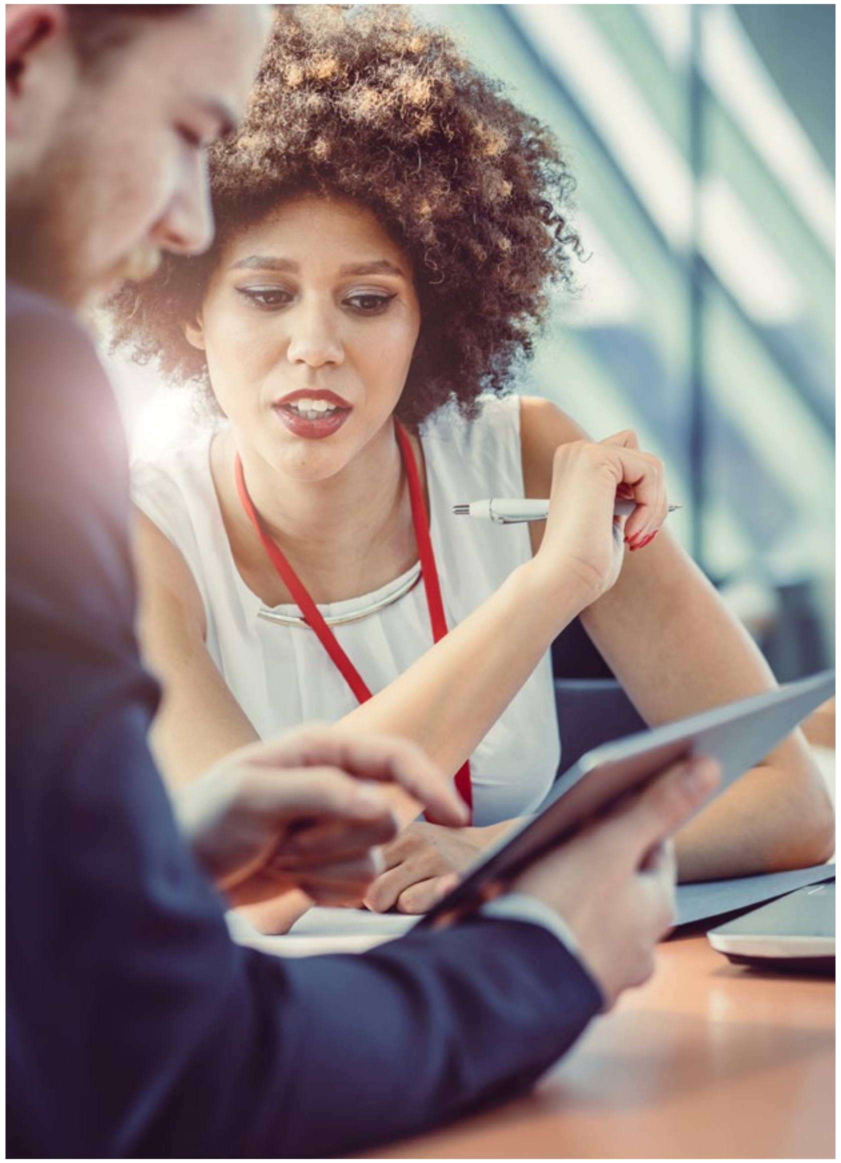
This holds materials, guides and instructions specifically for brokers, to help you grow your business.

Closed Applications

There is also a range of 'closed applications', accessible if they are relevant to your business. They include:

The Quotes Platform

This is a dashboard of all the new business quotes, existing policies and renewals linked to the account. In the online quotes section, you will be able to digitally generate quotes and bind policies across a range of products, including CyberRisk and Crime as part of our Management Liability Package.



Claim Scenario

Our CyberRisk solution has been proven to be effective across different sectors, organisations and businesses

Read more...

CyberRisk: How Our Coverage Responds For Private, Nonprofit And Public Companies

Liability Insuring Agreements

Privacy and Security

What is covered
Coverage for claims arising from unauthorised access to data, failure to provide notification of a data breach where required by law, failure to destroy confidential information, failure to comply with a privacy policy, wrongful collection of private or confidential information, failure to prevent a security breach that results in the inability of authorised users to gain system access, the participation in a DDoS attack, or the transmission of a computer virus.

Claim Scenario
A hacker obtains sensitive personal information from the insured's computer system. As a result, a number of customers bring a claim against the insured for allowing access to their personal information.

Coverage Response
Damages and defence costs for covered lawsuits.

Media

What is covered
Coverage for claims arising from copyright infringement, plagiarism, defamation, libel, slander, and violation of an individual's right of privacy or publicity in electronic and printed content.

Claim Scenario
A third party brings a lawsuit against the insured alleging that the insured plagiarised the third party's online content and organisational branding as well as infringed upon its trademarks.

Coverage Response
Damages and defence costs for covered lawsuits.

Regulatory

What is covered
Coverage for administrative and regulatory proceedings, civil and investigative demands brought by domestic or foreign governmental entities or claims made as a result of privacy and security acts or media acts.

Claim Scenario
A hacker obtains sensitive personal information from the insured's computer system. As a result, the Information Commissioner's Office bring a regulatory action against the insured.

Coverage Response
Costs for responding to regulatory claims stemming from the data breach, including any resulting fines or penalties (where insurable by law)

Breach Response Insuring Agreements

Privacy Breach Notification

What is covered

Coverage for costs to notify and provide services to individuals or entities who have been affected by a data breach. Examples include call centre services, notification, credit monitoring and the cost to purchase identity fraud insurance.

Claim Scenario

A fraudster hacks into the insured's internal processing system. Names, addresses and National Insurance numbers for more than 50,000 of the insured's customers are captured from the system, requiring notification to all 50,000 customers.

Coverage Response

Costs to deliver notice to impacted customers, and to provide credit monitoring, a call center, and an ID fraud policy for impacted individuals.

Computer and Legal Experts

What is covered

Coverage for costs associated with analysing, containing, or stopping privacy or security breaches; determining whose confidential information was lost, stolen, accessed, or disclosed; and providing legal services to respond to such breaches

Claim Scenario

An insured suspects that a fraudster hacked into its internal processing system when the police notifies them of identity theft impacting a number of the insured's customers.

Coverage Response

Costs to engage a forensics provider to contain the breach and determine its scope and legal costs to determine the insured's notification obligations under relevant privacy laws and provide other services to assist the insured in responding to and managing the breach.

Betterment

What is covered

Coverage for costs to improve a computer system after a security breach, when the improvements are recommended to eliminate vulnerabilities that could lead to a similar breach.

Claim Scenario

The insured's computer system is compromised by ransomware. Forensic providers contain the virus and determine that the source of the infiltration is a vulnerability in the insured's computer system. Upon recommendation from the forensic provider, the insured purchases new software to improve its system security.

Coverage Response

Costs to purchase new software to address the system vulnerability.

Cyber Extortion

What is covered

Coverage for ransom and related costs associated with responding to threats made to at-tack a system or to access or disclose confidential information.

Claim Scenario

The insured's system is infected with a virus that encrypts the insured's data. A ransom payment is demanded to unlock the system.

Coverage Response

Costs to manage and mitigate the incident, and if necessary, payment of the ransom demand.

Data Restoration

What is covered

Coverage for costs to restore or recover electronic data, computer programs, or software lost from system damage due to computer virus, denial-of-service attack or unauthorised access.

Claim Scenario

A computer virus corrupts the insured's software and data.

Coverage Response

Costs for recovery and restoration of the insured's electronic data and computer programs.

Public Relations

What is covered

Coverage for public relations services to mitigate negative publicity resulting from an actual or suspected privacy breach, security breach, or media act.

Claim Scenario

The insured's chief financial officer has his laptop stolen. The laptop contains more than 100,000 customer records, including National Insurance numbers.

Coverage Response

Costs for hiring a public relations firm to mitigate negative publicity generated from the incident.

Cyber Crime Insuring Agreements

Computer Fraud

What is covered
Coverage for loss of money, securities, or other property due to unauthorised system access.

Claim Scenario
An organised crime ring gains unauthorised access to the insured's accounts payable in their computer system and alters the bank routing information on outgoing payments resulting in a £100,000 transfer to the crime ring's account.

Coverage Response
Reimbursement of the insured's funds

Funds Transfer Fraud

What is covered
Coverage for loss of money or securities due to fraudulent transfer instructions to a financial institution.

Claim Scenario
A fraudster obtains the insured's information and uses the information to impersonate the insured to its financial institution. The fraudster requests a £100,000 transfer from the insured's bank account.

Coverage Response
Reimbursement of the insured's funds.

Social Engineering Fraud

What is covered
Coverage for loss of money or securities due to a person impersonating another and fraudulently providing instructions to transfer funds.

Claim Scenario
An employee in the insured's accounts payable department receives an email purportedly from an established vendor changing the vendor's banking instructions. The employee relies upon the fraudulent email instruction and transfers £50,000 from the insured's bank account to the fraudster. The insured discovers the fraud when the real vendor contacts the insured requesting payment.

Coverage Response
Reimbursement of the insured's funds

Vendor or Client Payment Fraud

What is covered
Coverage for loss of money or securities due to fraudulent delivery instructions.

Claim Scenario
A company contracts to provide a product to a customer, however the company's computer system is hacked and bogus delivery details are provided, thus diverting the dis-patched product to the fraudster rather than the customer.

Coverage Response
Reimbursement of the additional cost of supplying the product to the original customer.

Telecom Fraud

What is covered
Coverage for amounts charged by a telephone service provider resulting from an unauthorised person accessing or using an insured's telephone system.

Claim Scenario
An unknown third party gains unauthorised access to the insured's telephone system and uses the system to incur £50,000 in international charges.
The insured discovers the loss when it receives its monthly statement from its telephone provider containing the fraudulent charges.

Coverage Response
Reimbursement of the fraudulent charges the insured is required to pay to its telephone provider.

Business Loss Insuring Agreements

Business Interruption

What is covered
Coverage for loss of income and expenses to restore operations as a result of a computer system disruption caused by a virus or computer attack, including the voluntary shutdown of systems to minimise the business impact of the event.

Claim Scenario
An insured's computer system is infected by a virus and as a result, the insured's internal computer network is not available for an extended period of time.

Coverage Response
Payment to the insured for its lost income as a result of the disruption and expenses incurred to restore operations.

System Failure

What is covered
Coverage for loss of income and expenses to restore operations as a result of an accidental, unintentional, and unplanned interruption of an insured's computer system.

Claim Scenario
An organisation's computer system is rendered inoperable through employee negligence and as a result, the insured's business operations are shut down for an extended period.

Coverage Response
Payment to the insured for its lost income as a result of the disruption and expenses incurred to restore operations.

Dependent Business Interruption

What is covered
Multiple coverage options for loss of income and expenses to restore operations as a result of an interruption to the computer system of a third party that the insured relies on to run their business.

Claim Scenario
A cloud services provider's system is infiltrated by malware and rendered inoperable. As a result, the insured is unable to access its data and its business operations are shut down for an extended period.

Coverage Response
Payment to the insured for its lost income as a result of the disruption and expenses incurred to restore operations.

Reputation Harm

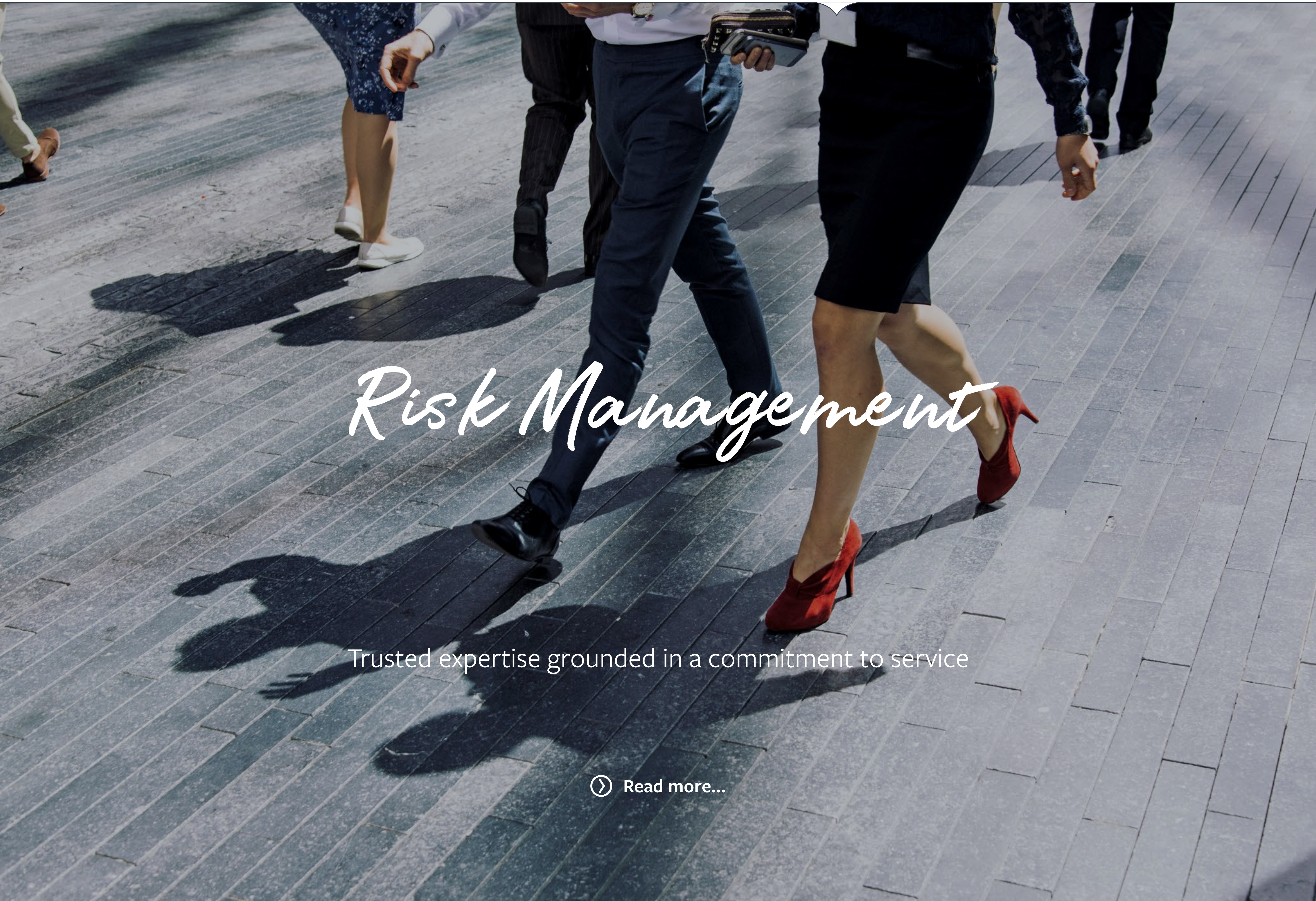
What is covered
Coverage for lost business income that occurs as a result of damage to a business' reputation when an actual or potential cyber event becomes public.

Claim Scenario
The insured's system is compromised by malware that permits an unknown third party to gain access to 100,000 customer records containing personally identifiable information. Following the insured's investigation, and notification to affected individuals, the local media runs an article about the event damaging the insured's business reputation.

Coverage Response
Payment to the insured for its lost income resulting from disclosure of the event.

Travelers CyberRisk coverage is offered as a stand-alone policy or as a cohesive part of the management liability suite of coverages available through our e-trading platform MyTravelers. CyberRisk helps protect organizstions from emerging cyber threats and now includes access to the following:

- Travelers' eRiskHub® – an information portal of risk management tools;
- A 24/7 cyber helpline and breach coach services from our expert partners Pinsent Masons;
- Access to HCL Technologies Cyber Resilience Readiness Assessment and Cyber Security Professional Consultation, Cyber Security Awareness Training, Risk Management Expertise and Discounts on services and solutions



Risk Management

Trusted expertise grounded in a commitment to service

Read more...

HCL Technologies Cyber Resilience Readiness Assessment And Cyber Security Professional Consultation

Preparation is key to mitigating a potential cyber-related event. To assist policyholders in achieving a higher level of cyber security for their organisations, Travelers offers its Cyber policyholders access to the HCL Technologies Cyber Resilience Readiness Assessment, including an official report and up to a one-hour consultation with a HCL Technologies cyber security professional.

Two online assessments are available and designed to quickly understand an organisation's current cyber security posture. Created using the combined experience of HCL Technologies's* 25,000 security professionals worldwide, these have been tailored to address specific security concerns faced by organisations today.

Each assessment will help an organisation to better understand how they compare to their industry peers, and to identify areas that could use some focus. Each assessment can be accessed through the Travelers eRisk Hub®. After the completion of each assessment, a final report will be generated which can be reviewed further during a consultation with a HCL Technologies cyber security professional to help improve areas of weakness or vulnerability.

Information Security Assessment

The Information Security Assessment is focused on foundational security, breaches from well-meaning insiders, malicious employees or accidental security breaches. The key areas of focus of this confidential assessment and report are:

- **Security Strategy** – Understanding if an organisation has the proper policies and best practices in place to ensure that the required standards and regulatory obligations are being met.
- **Security Operations** – Having the operational knowledge on how to securely minimise vulnerabilities and protect an organisation from being exploited is critical.
- **Network Security** – Preventing and monitoring unauthorised access to a network and the systems and data will help an organisation gain confidence that they are not being exploited.
- **Data Security** – Protecting data from being exfiltrated requires an understanding of how it is stored, protected, transported and monitored for changes.

Cyber Security Assessment

The Cyber Security Assessment is focused on security specific to malicious attackers and the types of security needed to defend against them. The key areas of focus of this confidential assessment and report are:

- **Preparation** – An organisation must plan for and understand how to respond during an incident, especially in regards to data loss and restoration capabilities.
- **Detection** – The ability to detect malicious activity by monitoring network traffic, detect intrusions, identify unauthorised system and configuration changes, and to leverage trusted threat intelligence.
- **Containment** – The ability to contain and quarantine malicious code from executing across a network by demonstrating the tools and capabilities to contain multiple threat types on a large cross-section of systems and devices.
- **Response** – Knowing how to contact incident response resources, legal counsel, and appropriately communicate details of a breach or incident externally are all necessary parts of a strategic cyber response.

*HCL Technologies, a Broadcom company

Travelers Pre-Breach Services Provided By HCL Technologies

Travelers and HCL Technologies – a real plus for agents and customers alike. By working with a leading provider of cyber security, Travelers now offers pre-breach services through HCL Technologies, in addition to the cyber coverage and post-breach services that are already provided to customers. That's good news for policyholders worried about cyber attacks that can shut down their organisations. Travelers plus HCL Technologies. Better together when it comes to cyber protection.

Preparation is key to mitigating a potential cyber-related event. To assist Cyber policyholders achieve a higher level of cyber security for their organisations, Travelers offers the following pre-breach services from HCL Technologies*, a global leader in cyber security solutions accessible through the Travelers eRisk Hub®:

HCL Technologies Cyber Resilience Readiness Assessment and Cyber Security Professional Consultation

An online assessment designed for an organisation to quickly understand their current cyber security posture and includes an official report and up to a one-hour consultation with a HCL Technologies cyber security professional to help improve areas of weakness or vulnerability. Created using the combined experiences of HCL Technologies's 25,000 security professionals worldwide and is tailored to address specific security concerns faced by organisations today.

HCL Technologies Security Coach Helpline

Professional cyber security advice to aid businesses and organisations in strengthening their cyber security programmes. This confidential consultation service is available for up to one hour, at no additional cost. The helpline will answer your business questions about general cyber security issues such as: What types of data should be encrypted? or What are some best practices for securing mobile devices?

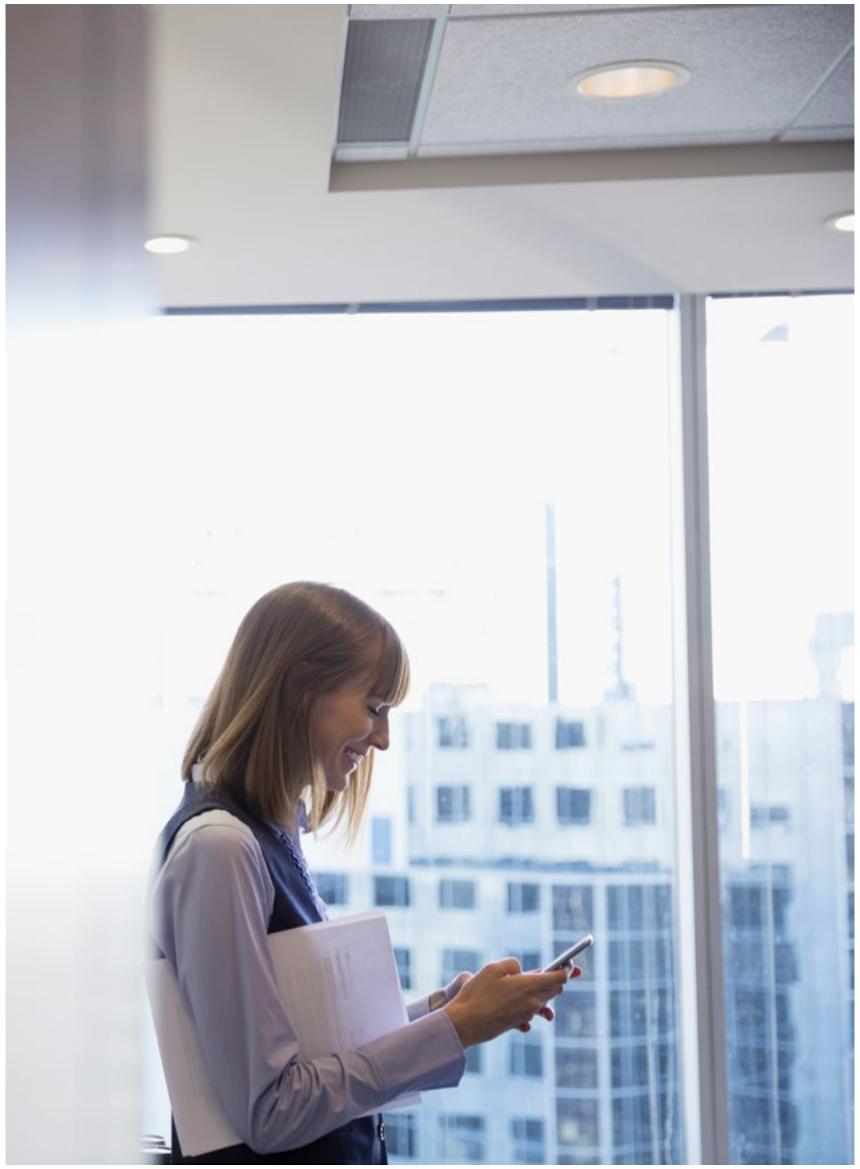
HCL Technologies Cyber Security Awareness Training

Educating your entire organisation not only helps to minimise potential attacks but can reduce internal security accidents. HCL Technologies offers innovative security literacy and role-based training designed to help companies defend against cyber security threats by promoting proactive employee behaviour. These courses can be provided via HCL Technologies's cloud-based learning management system or through an existing SCORM-compliant training platform, providing an easy way to supplement your existing employee training requirements.

HCL Technologies Service Discounts

Boost your cyber security readiness with discounts on many HCL Technologies services and solutions, including HCL Technologies Endpoint Protection (SBE), the DeepSight™ threat intelligence platform, HCL Technologies Managed Security Services, and HCL Technologies Incident Response Tabletop Assessment.

To find out more visit:
travelers.co.uk/cyber or travelers.ie/cyber



*HCL Technologies, a Broadcom company

HCL Technologies Cyber Security Awareness Training

Today, you need to protect not only against traditional security threats like hacking and exploitation of software vulnerabilities, but also against risks related to data breaches caused by internal inegligence and damage resulting from outside attacks targeted at your mobile devices. The best method of defence against these security threats is security awareness training of employees.

Why A Business Needs Cyber Security Awareness Training

Employees can be the strongest defence against both internal and external attackers. Educating your entire organisation not only helps in minimising potential attacks, but also in reducing internal security accidents.

A poorly trained workforce can significantly increase the risk of loss and disclosure of vital data such as Private personal data, bank account details and corporate intellectual property.

The immediate costs of these losses grab the headlines. But the largest impacts are the loss of reputation and trust, damage to an organisation's brand, and erosion of its customer base. Security-conscious companies realize that an effective security awareness program that touches all employees is as important as your firewall in defending against data breaches. Because such breaches can be addressed with appropriate security behaviour, most government standards, regulations and laws covering corporate governance, privacy and security best practices mandate that organisations provide employee security awareness training and show evidence thereof for compliance audits.

What Type Of Cyber Security Awareness Training Is Available?

As a recognised global leader in security intelligence and security training, HCL Technologies* is uniquely positioned to help organisations raise cyber security awareness with HCL Technologies Cyber Security Awareness Training that is available to Cyber policyholders through the Travelers eRisk Hub®.

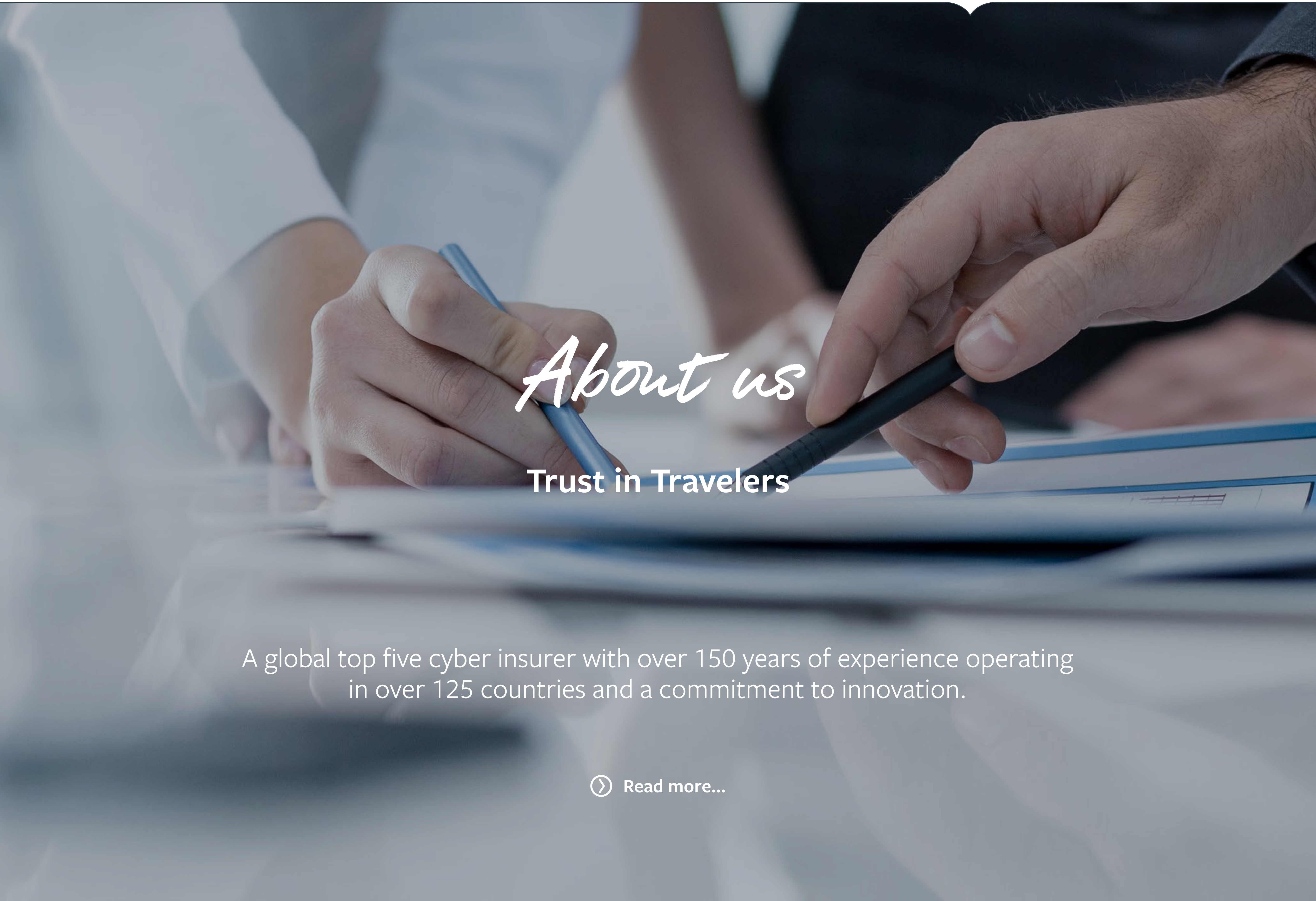
This collection of security literacy and role-based training is designed to help companies reduce vulnerabilities while creating an informed corporate culture, influencing employees to protect an organisation's critical information assets from exploitation, cyber attacks, unauthorised access and fraud. The HCL Technologies Cyber Security Awareness Training modules have been developed by professionals with backgrounds in security best practices and instructional design. This combination of expertise ensures both content quality and instructional presentation that minimises learning and retention.

Access dozens of HCL Technologies Cyber Security Awareness Training modules as a method of defence against cybersecurity threats to promote proactive employee behaviour, including:

- Password security
- How hackers get in
- Working remotely
- Role-based training videos designed for IT leadership and other professionals in your organisation

HCL Technologies Cyber Security Awareness Training can be accessed through a cloud-based learning management system hosted by HCL Technologies or on an existing SCORM-compliant LMS platform, providing an easily available solution regardless of your organisation's size and capabilities. These courses can be used to complement your employee training requirements.

*HCL Technologies, a Broadcom company



About us

Trust in Travelers

A global top five cyber insurer with over 150 years of experience operating in over 125 countries and a commitment to innovation.

Read more...

Market leading insurance expertise – across specialties, sectors and countries

Travelers Insurance Company Limited provides a broad range of property, liability and professional indemnity insurance and risk solutions for the private, public and institutional sectors. We are particularly known for our claims expertise, our expert underwriting, and our fast, fair and effective approach to claims handling.

We also offer extensive risk management expertise: Online, via MyTravelers; On-site, via visits to client premises; On-demand, via real-time online consulting; via Travelers Risk Academy and via regular free guidance and training courses.

In the UK and Ireland, our customers range from SMEs to large commercial and public service organisations. We also provide tailored insurance solutions to meet the needs of specialised businesses through our Lloyd's Syndicate.

As well as CyberRisk, Travelers can provide cover under the Management Liability Package for Crime, Directors and Officers, Employment Practices Liability and Pension Trustee Liability.

Other cover available includes:

- Combined Package
- Property & Business Interruption
- Property Owners
- Liability
- Motor Fleet
- Professional Indemnity
- Personal Accident
- Kidnap & Ransom

The company is part of The Travelers Companies, Inc. group – the third largest commercial property casualty insurer in the US. Our financial strength is also reflected in our Standard & Poor's AA rating.

As well as being a global top five insurer for cyber insurance, the group's success in the wider insurance industry reflects more than 150 years of experience and an ongoing commitment to lead positive change.

AA rated

Standard & Poor's has given Travelers an AA rating, a testament to our financial strength to pay out claims. Travelers is also one of only 30 select companies that comprise the Dow Jones Industrial Average.

Experienced

Through strategic alliances with leading insurers in over 125 countries, we protect the global operations of our insureds. With underwriters in six UK offices, we offer the assurance of local-market compliance matched with UK-based claims handling and risk management support.

Top five cyber insurer

Travelers is one of the world's top five cyber insurers and offers market-leading expertise across numerous specialties, sectors and countries.

Winning partnership

For Breach Coach services, we partner with Pinsent Masons, who have in-depth expertise and over 10 years' experience across hundreds of breaches.