



Be cyber
confident

TRAVELERS 

Broker sales pack

CyberRisk insurance

Contents

Cyber Appetite Summary	3
CyberRisk Coverage Highlights	4
Why your clients need our protection	6
What's new?	8
MyTravelers	9
Claim Scenarios	10
Working together to understand risk	13
Cyber Acronyms	15
For your clients	17
How well do you know your business' cyber exposures?	18
Multifactor Authentication (MFA)	20
SentinelOne offer	22
HCL Technologies Cyber Security Awareness Training	23
Travelers Pre-Breach Services Provided By HCL Technologies	24
Breach Coach cheat sheet	25
Cyber Security Training for Employees	26
Building Resilience to Cyber Risk	28
Five Steps Towards Cyber Resilience	29

Cyber Appetite Summary

Trade	Cyber Appetite
Accountants	▶
Construction	▶
Consultancy	▶
Education	▶
Hotels / Restaurants	▶
Manufacturing	▶
Other Professions	▶
Property / Real Estate	▶
Public Administration	▶
Retail	▶
Solicitors	▶
Wholesale	▶

Trade	Cyber Appetite
Financial Institutions	⏸
Mining / Utilities	⏸
Publishing / Broadcasting	⏸
Transport	⏸
Technology*	⏸

Corporate Restrictions	◻
Healthcare	◻
Security / Defence Activities	◻

Registered brokers can obtain quotes through the MyTravelers portal for company's with turnover up to £/€50m. New brokers and turnover beyond this will refer directly to an underwriter.

* We have a dedicated Global Technology underwriting team who we work closely with in identifying specific appetite for the Technology sector.

▶ Strong appetite for this business ⏸ We'll need to ask a few more questions than normal ◻ It's not you; it's us



CYBER FACTSHEET EUROPE

CyberRisk Coverage Highlights



Why you need the protection

It takes only one cyber event or data security breach to impair your company's financial results, or even potentially put you out of business. One resourceful hacker, virus, or system glitch can shut down your entire network within minutes, paralysing operations and your ability to earn income. One successful hack, lost laptop, or lost paper record can cause a data breach impacting the privacy of customers, employees, and others. Travelers has you protected from every angle... pre-breach, post-breach and always.

Coverage highlights

CyberRisk coverage is specifically designed to help in the event of a cyber breach. It's available for businesses of all sizes as a stand-alone policy or as part of a management liability suite of coverages. CyberRisk provides more solutions with options that include coverage for forensic investigations, litigation expenses associated with the breach, regulatory defence expenses/fines, crisis management expenses, business interruption and cyber extortion. And now, CyberRisk protection doesn't end after a breach occurs. New to CyberRisk is Betterment – an insuring

clause that provides 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. In addition to coverage, Travelers provides policyholders innovative value-added pre-breach and post-breach risk management services at no additional cost.

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.
- **HCL Technologies™ 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 SCORM-compliant 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.

Travelers Breach Coach®:

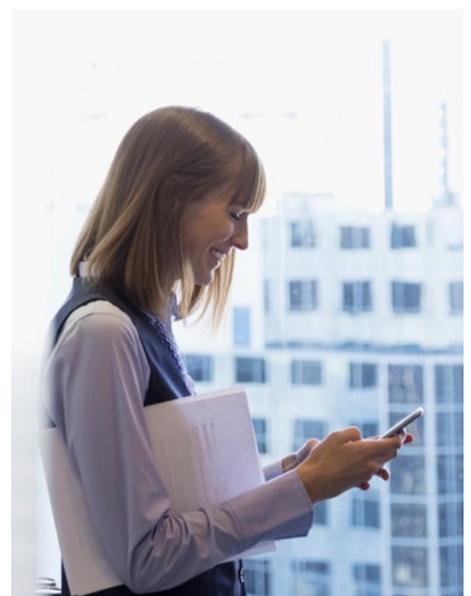
Should you experience a data breach event, you may choose to call the Breach Coach listed in the Travelers eRisk Hub portal for immediate triage assistance.

Your initial 30-minute consultation is at no additional charge.

Please be aware that the Breach Coach service is provided by a third-party law firm. Therefore, contacting the Breach Coach does NOT satisfy the claim or notification requirements of your policy

Risk Management Whitepapers:

Topical insights and expertise on current cyber related trends, risks and threats that face organisations in today's business environment. These resource guides will help with your organisation's preparedness when it comes to cyber related events.



Travelers CyberRisk coverage includes the following insuring clauses:

**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.

Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.

Why your clients need our protection

Travelers CyberRisk coverage is a critical component of an overall insurance protection package for any organisation. The following checklist illustrates key coverages and features every insured should have as part of their cyber insurance programme.

Coverage	Travelers policy	Their policy
Privacy and Security coverage for defence against allegations of: <ul style="list-style-type: none"> - failure to prevent a privacy breach - failure to comply with its privacy policy - failure to provide notification required by law - unlawful collection of data - failure to prevent a security breach that resulted in <ul style="list-style-type: none"> - alteration or deletion of confidential information - transmission of virus - participation in a denial-of-service attack - failure to provide access to a computer system 	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Media coverage for defence against allegations of the following within the insured's content: <ul style="list-style-type: none"> - unauthorised use of specified intellectual property rights of others - improper deep-linking or framing - misappropriation of ideas under implied contract - violation of an individual's right to publicity - harm to the reputation or character of any person or entity 	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Regulatory Proceedings <ul style="list-style-type: none"> - defence costs for allegations by any governmental entity - coverage for regulatory fines and penalties - coverage for violation of the General Data Protection Regulation (GDPR), including the resulting fines and penalties, where insurable by law 	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Privacy Breach notification costs for an actual or suspected incident include: <ul style="list-style-type: none"> - 24 months of credit or identity monitoring, or longer where required by law - Printing and delivery of notice - Purchase of an ID Fraud policy - Call centre services - Other services to mitigate loss - Rewards paid 	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Cybercrime coverage: <ul style="list-style-type: none"> - Computer Fraud - Funds Transfer Fraud, including social engineering fraud and vendor or client payment fraud - Telecom Fraud 	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Full Prior Acts coverage provided	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Computer and Legal Experts to respond to an actual or suspected incident	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Public Relations costs to help prevent negative publicity	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Costs to restore or recover damaged or destroyed programmes, software, or data	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Coverage	Travelers policy	Their policy
Betterment: Coverage to purchase hardware or software to improve a system after a breach to reduce the chances of the breach reoccurring	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Cyber Extortion - Expenses to respond to actual or threatened compromise of the insured's network or data - Includes a threat against the insured entity's own confidential information as well as information of others	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
Business Interruption coverage includes: - System Failure and Security Breach Triggers - Forensic Accounting Costs to establish a proof of loss - Dependent Business Interruption for technology providers - Dependent Business Interruption for other organisations that an insured relies on to run their business - Coverage for voluntary shutdown of the insured's computer system - Reputation Harm following a media report or data breach notification	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Broad definition of confidential information includes: - Electronic or paper data - The insured's own information - Data stored with service providers, including the cloud	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Other Insurance - Breach Response and Business Interruption Insuring Clauses are primary to other insurance	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Computer System includes: - personal devices used to conduct the company's business - cloud services, software-as-a-service, and computer systems operated by other IT providers	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
Coverage available for fines, penalties, and assessments as a result of a payment card breach	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Bodily injury exclusion uses "for" wording	<input checked="" type="checkbox"/>	<input type="checkbox"/>
No exclusion for emotional distress	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modified War exclusion	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Includes pay on behalf language for Cyber Liability, Privacy Breach Notification, Computer and Legal Experts, Cyber Extortion, Data Restoration and Public Relations insuring clauses	<input checked="" type="checkbox"/>	<input type="checkbox"/>
The definition of money includes virtual currency	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Extra Expense includes costs to replace bricked equipment following a security breach	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Innovative value-added pre-breach and post-breach services	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Nil Excess when notification is provided within 72 hours (for firms with turnover £50m and below)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document.



Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.



Cyber

What's new?

The world of cyber risk is constantly evolving and we have made a number of enhancements to our policy wording to further help businesses prepare for and overcome the ever increasing cyber challenges.

New Coverages

- Betterment – covers cost to improve Insured's system security following a breach
- Social Engineering Fraud
- Vendor and Client Payment Fraud
- Reputation Harm – covers lost business income due to damage to reputation caused by privacy or security breach

Enhancements to Business Interruption coverage

- System Failure trigger
- Voluntary Shutdown trigger
- Extra Expenses includes replacement of Non-Functional Equipment (often referred to as 'Bricking' coverage)
- Accounting Costs to calculate amount of business income loss

Increased standard limits

- Payment Card Expenses (PCI): 50% policy aggregate → 100% policy aggregate
- Computer Fraud: £25k → £100k
- Telecom Fraud: £25k → £100k
- Funds Transfer Fraud: £25k → £100k or 10% of policy aggregate, whichever is less
- Dependent Business Interruption: £10k → £100k or 10% of policy aggregate, whichever is less
- Damage to Computer System: £10k → 100% policy aggregate (when covered as Extra Expense)
- Higher limits available upon discussion

Other proposition enhancements

- Nil Excess for Breach Response Covers when notification is provided within 72 hours of discovery of First Party Event (for insureds with turnover \leq £50 or €50)
- Third Party Liability insuring clauses now automatically extend to Independent Contractors and Additional Insureds (third parties which the Insured Organisation agrees to name as insureds via agreement)
- Virtual Currency covered as Money
- Simplified policy wording, with number of pages reduced from 18 to 15 pages, even including all above enhancements
- Enhanced suite of risk management materials provided by cyber security leader HCL Technologies and available to all CyberRisk Insureds, including:
 - Cyber resiliency assessment, followed by access to HCL Technologies Security Coach Helpline to discuss results and how to best improve the Insured's cyber security
 - HCL Technologies Cyber Security Awareness Training, provided via HCL Technologies's cloud-based learning management system
 - HCL Technologies Service Discounts

The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document. Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.

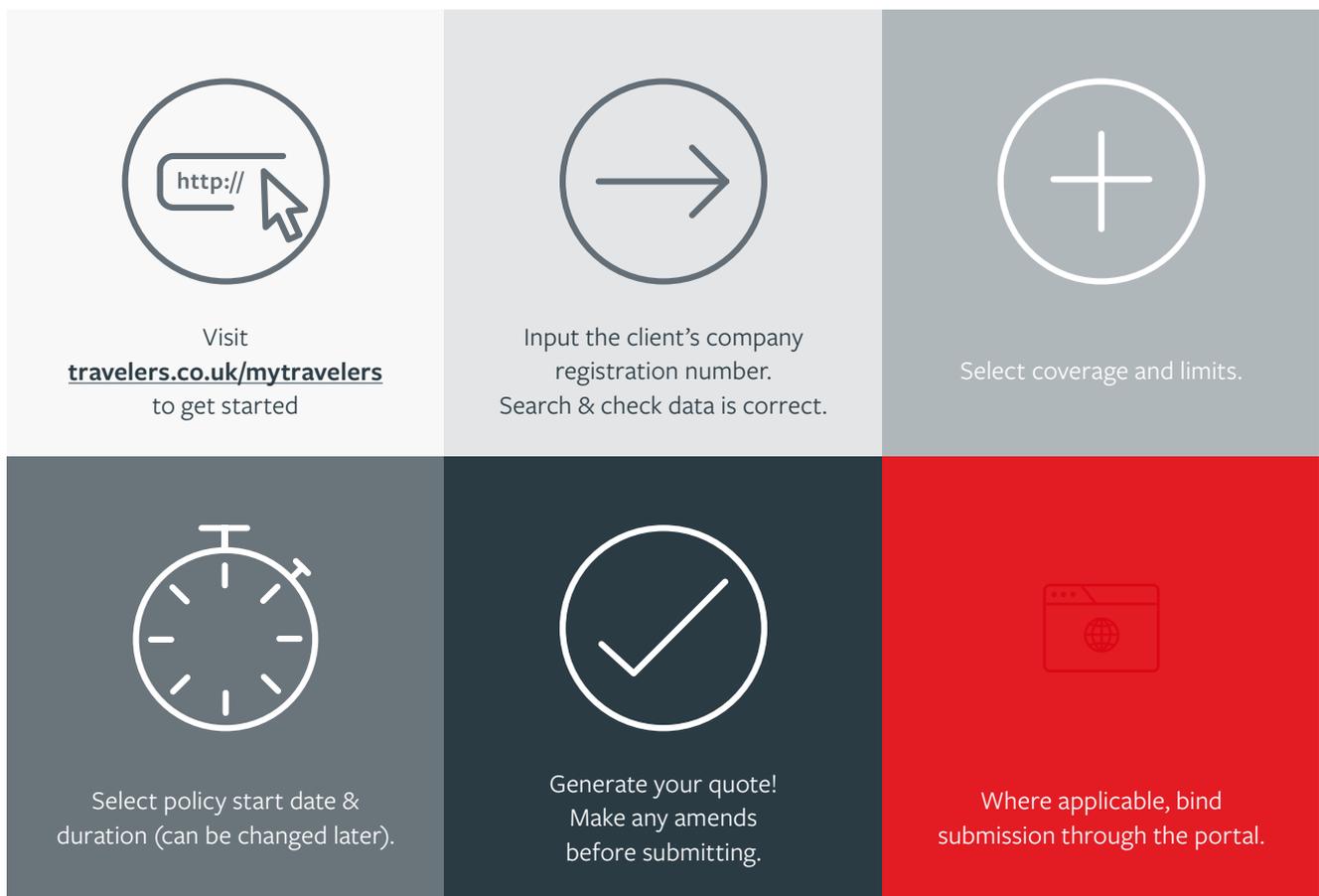
MyTravelers Broker Portal

MyTravelers is the online gateway to access a range of useful and secure applications and services – from online quotes and claims statistics to important industry-specific control information.

The Quotes Platform

This is a dashboard of all the new business quotes, existing policies, mid-term adjustments and renewables linked to your account. In the online quotes section you will be able to digitally generate quotes and bind policies across a range of products.

How to get a Quick Quote



The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document. Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.



CLAIM EXAMPLES

How CyberRisk responds to assist and protect our Insureds

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

Definition

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

Definition

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

Definition

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

Definition

Coverage for ransom and related costs associated with responding to threats made to attack 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

Definition

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

Definition

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.



Rewards

Definition

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.

Claim Scenario

The insured offers a £10,000 reward for information following a break in where customers' personal data was stolen. Information received leads to the conviction of the burglar.

Coverage Response

Reimbursement of the reward paid.

Cyber Crime Insuring Agreements



Computer Fraud

Definition

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

Definition

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

Definition

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

Definition

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 dispatched 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

Definition

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

Definition

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

Definition

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

Definition

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

Definition

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 operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.

travelers.co.uk travelers.ie



TRAVELERS

Working together to understand risk



CyberRisk

CyberRisk coverage is specifically designed to help in the event of a cyber breach. It's available for businesses of all sizes as a stand-alone policy or as part of a management liability suite of coverages. CyberRisk provides more solutions with options that include coverage for forensic investigations, litigation expenses associated with a privacy or security breach, regulatory defence expenses/fines, crisis management expenses, business interruption and cyber extortion. And now, CyberRisk protection doesn't end after a breach occurs. New to CyberRisk is Betterment – an insuring agreement clause that provides 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. In addition to coverage, Travelers provides policyholders innovative value-added pre-breach and post-breach risk management services at no additional cost. Should a cyber incident occur, policyholders can also take advantage of a 24/7 cyber helpline where a Travelers claim professional and a breach coach from our expert partners Pinsent Masons triage

the situation with the Policyholder and agree next steps.

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.

- HCL Technologies 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 SCORM-compliant 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

Visit travelers.co.uk/cyber or speak to a member of the travelers team for more information.



Management Liability

Management liability insurance can provide peace of mind to a company's directors, officers, senior managers and others whose professional leadership roles expose them to scrutiny from shareholders, employees and other parties. Our products cover a range of risks, including:

- Directors and Officers
- Commercial Crime
- Employment Practices Liability
- Pension Trustees' Liability

Visit travelers.co.uk/managementliability or speak to a member of the travelers team for more information.

Cyber breach claim examples

Here are three examples of cyber breach claims we have seen at Travelers. These case studies explain the different types of breaches, how Travelers breach response responded to each situation, and the cost of these claims covered by the policy.

Case study 1 – International Ransomware Attack

The Policyholder (“PH”) reported that it discovered that its IT system had been infected with malware. It was subsequently discovered that the malware was ransomware identified as “ransomcrypsam.D”, a new strain of ransomware that PH’s antivirus detection system was unable to detect. The virus quickly infected and encrypted systems throughout PH’s organisation, including offices in the United States and the United Kingdom. All systems were locked and the PH closed all of its field offices and operations at its headquarters were significantly impacted.

The PH received a “ransom” demand of £10,000 in bitcoin to unlock the encryption. The ransom was paid but the encryption key was not released. As a result, the PH was required to restore system operations from its backup files. Although the PH had backup files that were only a few days old, restoring full capacity system-wide took over two weeks.

In addition, there was some indication of compromise of confidential information stored within PH’s system. As a result, it was necessary to conduct a forensic investigation to determine the extent of the intrusion. There were ultimately no third party claims. The total insured loss was over £70,000. The major expense items were: (1) breach coach (lawyer), (2) forensic consultant, and (3) business interruption and extra expense.

Case study 2 – Municipal Ransomware Attack

A police employee from the Policyholder (“PH”) discovered this incident when she attempted to access data and was unable to open an application. Ultimately, all PH software applications were impacted and locked out, including all Microsoft Windows applications and all mainframe applications. The PH then received a “ransom demand.” At the time of the demand, all of PH’s system applications were locked-out, including emergency services and local authority systems.

A forensic investigation confirmed that the malware placed on the PH’s systems was designed only to encrypt – there was no exfiltration of data and no access to or acquisition of personally identifiable information. The PH received an email from the cyber-criminals containing a ransom demand and subsequent follow up confirmed that the cyber-criminals were located outside of the UK. The cyber-criminals demanded a ransom of £5,000 - £8,000 payable in Bitcoin. The ransom was ultimately negotiated and paid through use of a breach coach and the decryption key was released, allowing the PH to restore full system functionality.

The total insured loss was over £25,000. The major expense items were: (1) breach coach (lawyer), (2) forensic consultant, (3) payment of the ransom, and (4) expense to restore damage to the PH’s system.

Case study 3 – Phishing Attack

This matter arose from a “phishing” attack that occurred when cyber-criminals posing as Microsoft employees tricked a Policyholder (“PH”) employee into granting remote access to its system. Once access was granted, the cyber-criminals accessed over 12,000 individual patient records dating to 1994. The PH’s Information Technology department and a forensic investigator confirmed that the personally identifiable information of current and former clients had been stolen including driver’s licence numbers, dates of birth and national insurance numbers. A breach coach was retained and coordinated notice and communication with the ICO and other relevant authorities. In addition, the breach coach coordinated notice to the impacted individuals. The notice required a press release, individual written notice, staffing of a call centre and credit monitoring for clients who elected the coverage. There were no third party claims made before or after notice to the current and former clients.

The total insured loss was over £50,000. The major expense items were: (1) breach coach (lawyer), (2) forensic consultant, (3) public relations expenses (press release), (4) notice and call centre expenses and (5) the cost of credit monitoring for clients who requested the same.

The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document.



Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.

travelers.co.uk travelers.ie

Cyber Acronyms

Acronym	Definition
 CISO	Chief Information Security Officer The executive responsible for an organisation's information and data security. Increasingly, this person aligns security goals with business enablement or digital transformation. CISOs are also increasingly in a "coaching role" helping the business manage cyber risk. Can also be known as a DPO (Data Protection Officer) or CIO.
 DDoS	Distributed Denial of Service Attacks Is a type of cyber attack which floods a network with fake traffic to prevent legitimate users from accessing the network. The incoming traffic flooding the victim originates from many different sources, often from thousands of hosts (such as an IoT) that have been infected with malware, which instructs the IoT to bombard the victim's website.
 DLP	Data Loss Prevention A DLP (system) focuses on monitoring and blocking the unauthorised movement of sensitive data. It can scan external emails and stop any such transfer that it has been set up to recognise, for example, any files that are labelled confidential or for internal-use only. It can prevent both inadvertent disclosures by employees, and malicious exfiltration of data by a hacker or malware designed to transmit data. One additional component of a DLP system is that it can be used to scan, identify, and catalogue where sensitive data is stored on the network. A DLP is particularly valuable for companies that have sensitive unstructured data, such as data stored in email or spreadsheets rather than in a more controlled database environment.
 DNS	Domain Name System A DNS is the phonebook of the Internet. It connects URLs (web address) with their IP address (their unique "telephone number"). For example, if you type www.travelers.co.uk into your browser, the DNS system will convert this into the correct IP address, e.g. 104.78.163.166.
 DRP/BCP	Disaster Recovery Plan / Business Continuity Plan A DRP and BCP provides guidance on mitigating damage and recovering from an event that impairs the assets used by a company during normal business operations. A DR or BC plan traditionally addresses events such as fire or flood, but now it is also important for companies to prepare for damage or destruction to IT systems and infrastructure.
 EDR	Endpoint Detection & Response Endpoint Detection & Response is a security solution that is designed to detect and respond to any suspicious activity by providing real-time monitoring. Whereas antivirus software will block malicious-looking files based on a known database, EDR will go beyond this and can protect against files that demonstrate malicious behaviour, for example, attempting to access administrative rights. Thus EDR can be critical to prevent recently-created malware from causing damage, which may not yet be included in known antivirus databases.

Acronym	Definition
 IDS	Intrusion Detection System A system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. An IDS provides real-time monitoring for activity that is indicative of a security compromise.
 IoT	Internet of Things Is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.
 IPS	Intrusion Prevention System An IPS is a system that monitors a network for malicious activity such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.
 IRP	Incident Response Plan A written plan in place which details how a company plans to respond to a network intrusion or a data breach and is specifically designed to minimise or contain associated damage.
 MFA	MultiFactor Authentication An authentication tool that combines “something you know” (such as a password), “something you have” (such as a text message), and “something you are” (such as a fingerprint scan) to create a stronger access control than only requiring a password. MFA can prevent intruders from spreading across a network from a single compromised computer.
 PCI-DSS	The Payment Card Industry Data Security Standard An information security standard for organisations that handle branded credit cards from the major card schemes. Breaches of the standard can lead to significant contractual monetary fines and penalties.
 PII	Personally Identifiable Information Any data that could potentially be used to identify a data subject. Examples include a full name, email address, national insurance number, driver’s license number, bank account number, passport number etc.
 SSO	Single Sign-On A system which enables users to securely authenticate themselves with multiple applications and websites by logging in with a single set of credentials.
 VPN	Virtual Private Network A virtual private network is a specific way of providing remote access to a company’s network, in which encryption is used to provide a secure communication channel between the remote device and the network. Use of a VPN protects, for example, against eavesdropping when the remote device is using a public wi-fi access point.



The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document. Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.



Be cyber
confident

TRAVELERS^U

For your clients

CyberRisk insurance

How well do you know your business' cyber exposures?

1. Does your business retain physical or electronic records of employees or other third parties with any of the following?

- a. National Insurance numbers Yes No
- b. Drivers' licence information Yes No
- c. Tax identification numbers Yes No
- d. Birth dates Yes No
- e. Medical/health records Yes No
- f. Court records Yes No
- g. Police records Yes No
- h. Banking information (current/savings accounts) Yes No
- i. Email addresses or home addresses Yes No

FACT: If you answered yes to any of the above your organisation is in control of "Personally identifiable information," and therefore, required to protect that data subject to data breach notification laws.

2. Does your business have employees? Yes No

FACT: Most data breaches involve an employee mistake. They can lose a mobile device, laptop or paper records, or make costly errors such as opening an unauthorised email containing malware. In addition, they can even intentionally steal data.

3. Does your business have an active website? Yes No

FACT: Material posted electronically, or in written format, may lead to copyright or trademark infringement, or defamation litigation. If the website is transactional, additional exposures include possible hacking or disruption of your business via denial of service attacks.

4. Does your business use third-party vendors (e.g. cloud, IT services)? Yes No

FACT: Businesses in possession of personally identifiable information may be held liable for privacy breaches caused by their vendors or other third parties. As the owner of the data, your business is ultimately responsible for protecting it.

5. Does your business use mobile technology (e.g. smartphones, tablets, laptops)? Yes No

FACT: Loss of mobile devices and the electronic content contained therein is one of the leading causes of data breaches today.¹

6. Does your business accept credit card payments, other electronic payments or have online bill pay? Yes No

FACT: Over 25% of all data stolen is credit card and other payment information.² This is a category of data that is highly desired by criminals for resale on the black market.

7. **Does your business allow employees to use personal devices to connect to your network?** Yes No

FACT: Personal devices may not have the same security software and connectivity procedures as company-provided devices. As a result, when these personal devices are connected to your network, there may be a higher exposure to virus or malware threats.

8. **Does your business train employees on proper email use and other privacy issues?** Yes No

FACT: Employee negligence and/or errors are one of the top three contributors of lost/stolen data.³

9. **Does your business store your customers' corporate confidential information?** Yes No

FACT: Companies face liability for failing to protect their customers' and business partners' confidential information.

10. **Does your business have access to online cyber risk management tools?** Yes No

FACT: Travelers eRisk Hub® is an information portal to help your business successfully prevent and respond to cyber events. It includes reference material, news updates and other tools, as well as access to a Breach Coach® for a 30-minute consultation if you have a data breach event.

If you answered "yes" to one or more of questions 1-9, your business has exposures which may lead to cyber-related claims or loss. Can you afford to self-insure these exposures?

At Travelers, we understand the complexity of cyber threats and have solutions to help protect your assets.

To learn more about our cyber capabilities, visit travelers.co.uk/cyber or contact your Travelers representative or insurance broker

¹ Ponemon Institute 2018 Cost of Data Breach Study

² NetDiligence® 2018 Cyber Claims Study

³ Ponemon Institute 2018 Cost of Data Breach Study

The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document.



Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.

travelers.co.uk travelers.ie



Best Practices for Travelers Cyber Policyholders

Multifactor Authentication (MFA)

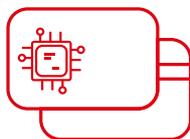
What is MFA?

Multifactor Authentication (MFA) is the use of two or more authentication factors. MFA is successfully enabled when at least two of these categories of identification are required in order to successfully verify a user's identity **prior** to granting access.



1. Something you know

A password or passphrase is something you know.



2. Something you have

A token or smartcard is something you have.



3. Something you are

Biometric identification through a fingerprint or retina scan establishes something you are.

There is flexibility regarding which authenticators are used by a business to validate a user's identity without undue inconvenience.

99.9%

of account compromise attacks can be blocked by MFA¹

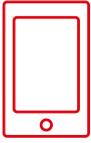
94%

of ransomware victims investigated did not use MFA²

Why is MFA critical?

MFA helps protect a business by adding an additional layer of security making it more difficult for cyber criminals to access a business' systems. Credentials like user IDs and passwords can be the weakest link in a business' cybersecurity as they are frequently compromised and posted on the Dark Web. And passwords are growing more insecure as users connect to more systems that require a user ID and password, they tend to get lazy. They create simple easy-to-guess passwords, use the same password for different sites, share them and sometimes inadvertently give them to the attacker.

What should be protected with MFA?



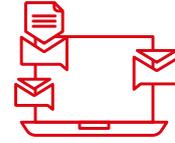
Remote Network Access

MFA for remote network access is an important security control that can help reduce the potential for a network compromise caused by lost or stolen passwords. Without this control an intruder can gain access to a business network in a similar manner to an authorised user.



Privileged/Administrative Access

MFA for both remote and internal access to administrative accounts helps to prevent intruders that have compromised an internal system from elevating privileges and obtaining broader access to a compromised network. This can prevent an intruder from gaining the level of access necessary to successfully deploy ransomware across the network, erase activity logs, create bogus user accounts or even turn off anti-malware protection.



Remote Access to Email

When accessing e-mail through a website or cloud-based service on non-corporate devices MFA can help reduce an intruder's ability to gain access to a user's corporate email account. Threat actors often use email access to perpetrate various cybercrime schemes against businesses, as well as the businesses' clients and customers.

HCL Technologies

How does a business start to implement MFA?

An extra layer of security in the form of multifactor authentication is important but the options can vary from one solution to the next. To learn how a business can start to implement MFA and increase their cyber defenses, Travelers offers its Cyber policyholders access to a one-hour consultation with a HCL Technologies Security Coach who can provide much-needed expertise and help pave the way for a stronger cybersecurity program.

For direct access to the HCL Technologies Security Coach please contact Glen Carl at **0800 587 8366** or via email at sed.cicsecuritycoach@hcl.com

The Security Coach is on call utilising the toll free number listed above. Please leave a voicemail message and a cyber security expert from HCL Technologies will contact you within 48 hours of your request.

Travelers Cyber policyholders may also access many other pre-breach services and risk management resources by logging onto [Travelers' eRiskHub portal, powered by NetDiligence®](#).

1 Source: <https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/>

2 Source: Arete Presentation "Ransomware Cards" 7-31-2020



The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document. Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.

Protect Against Cyber Risks as Employees Return to Work

Why your business needs protection

Organisations of all sizes and in all industries now have unprecedented numbers of employees working remotely, often with little advance warning or preparation. As most home computer networks are considerably less secure than corporate networks, it may not matter how cautious employees have been during their time working from home. Cybercriminals may have gained access and have been lingering on work from home devices for months. And when that laptop is put back onto the corporate network, the scope of potential damage that may result – and the potential profit for a cybercriminal – increases dramatically.

Increase your defenses with an EDR Solution

An Endpoint Detection and Response (EDR) solution can provide far greater capabilities than a traditional antivirus solution. EDR can help

protect and monitor every asset in an enterprise network by identifying suspicious activity before the rest of the corporate network is exposed to unnecessary risk.

EDR Solution Benefit for all Travelers Cyber Policyholders

Travelers is offering its current cyber policyholders access to the SentinelOne™ Platform for 60 days at no additional cost. This platform delivers the defenses to prevent, detect and undo known and unknown threats that may be lurking on the enterprise's network.

In addition, policyholders that choose to continue the service and subscribe to the SentinelOne Platform after the trial period ends will receive an exclusive discount of 25% off the list price.

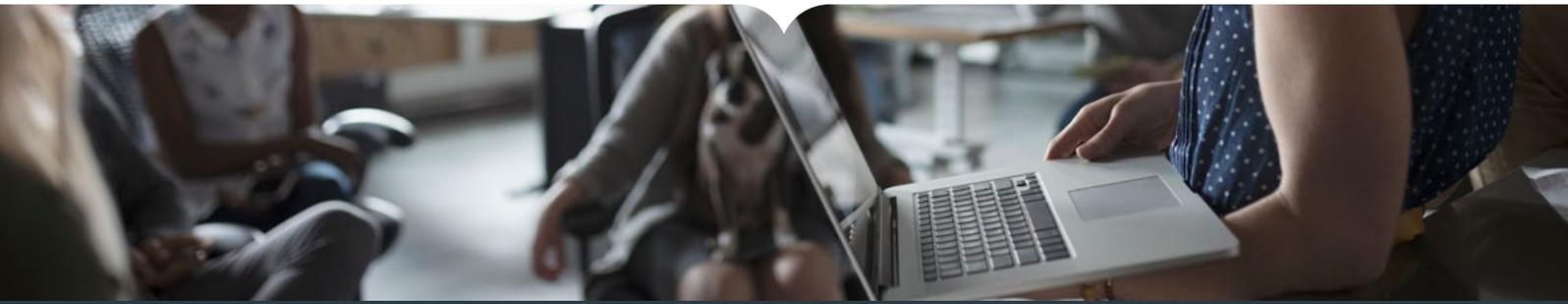
Access to SentinelOne™ Platform for 60 days at no additional cost for current cyber policyholders.

> [REGISTER HERE](#)

Policyholders need to sign up at sentinelone.com/lp/travelers-insurance/

Return to Work, Return to Cybersecurity with Travelers & SentinelOne

The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document. Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.



INFORM AND EDUCATE

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 negligence 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

Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.



INSURE AND PROTECT

Travelers Pre-Breach Services Provided By HCL Technologies

Travelers and HCL Technologies – a real plus for brokers 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 Technology & Medical Technology 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

24/7 Breach Hotline

If you're in the UK:

0800 587 8388

If you're in Ireland:

00353 1609 5601

If you experience a breach, please call this number as soon as possible.



1. Call the Breach Hotline and have the following information ready

- Have your Travelers policy number to hand, it can be found on your policy schedule
- Your telephone contact details
- Brief details and timeline of the incident, including any steps you have already taken



2. Travelers will call you back

- We'll contact you to understand more about what has happened
- We'll agree with you an appropriate time within the next 24 hours for the breach coach call



Whilst you wait for the breach coach call please start thinking about the following, which will help us deal with the breach as quickly as possible:

- Who else needs to be on the call with you? i.e. decision makers and those who know your IT systems
- What information has been accessed?
- Are your systems fully operational?
- Are your back ups secure?
- Due to the breach, it is good practice to arrange a forced Password reset for all users



3. The breach coach call

- During the breach coach call we'll set out an action plan which we will also help you put in place.
- Your designated claim handler and the appointed breach coach will guide you back to recovery every step of the way



We're here to help you every step of the way

Some of the ways we'll help as covered by your Travelers CyberRisk Policy

- **Ransom negotiation and costs** – if your systems are locked by a hacker demanding a ransom we'll negotiate on your behalf and cover the cost of the ransom
- **IT forensics** – a drains up investigation to see what the hacker has done and what kind of information they have accessed. We'll also cover 50% of the costs of improvements recommended by the IT forensics team.
- **PR Costs** – the cost of using a PR Company to help manage the message with clients
- **Data restoration costs** – to replace electronic data that has been lost or corrupted



TRAVELERS RISK CONTROL

Cyber Security Training for Employees

Empowering your employees to recognise common cyber threats can be beneficial to your organisation's computer security. Security awareness training teaches employees to understand vulnerabilities and threats to business operations. Your employees need to be aware of their responsibilities and accountabilities when using a computer on a business network.

New hire training and regularly scheduled refresher training courses should be established in order to instill the data security culture of your organisation. Employee training should include, but not be limited to:

Responsibility for Company Data

Continually emphasise the critical nature of data security and the responsibility of each employee to protect company data. You and your employees have legal and regulatory obligations to respect and protect the privacy of information and its integrity and confidentiality.

Document Management and Notification Procedures

Employees should be educated on your data incident reporting procedure in the event an employee's computer becomes infected by a virus or is operating outside its norm (e.g., unexplained errors, running slowly, changes in desktop configurations, etc.). They should be trained to recognise a legitimate warning message or alert. In such cases, employees should immediately report the incident so your IT team can be engaged to mitigate and investigate the threat.

Passwords

Train your employees on how to select strong passwords. Passwords should be cryptic so they cannot be easily guessed but also should be easily remembered so they do not need to be in writing. Your company systems should be set to send out periodic automatic reminders to employees to change their passwords.

Unauthorised Software

Make your employees aware that they are not allowed to install unlicensed software on any company computer. Unlicensed software downloads could make your company susceptible to malicious software downloads that can attack and corrupt your company data.

Internet Use

Train your employees to avoid emailed or online links that are suspicious or from unknown sources. Such links can release malicious software, infect computers and steal company data. Your company also should establish safe browsing rules and limits on employee Internet usage in the workplace.

Email

Responsible email usage is the best defence for preventing data theft. Employees should be aware of scams and not respond to email they do not recognise. Educate your employees to accept email that:

- Comes from someone they know.
- Comes from someone they have received mail from before.
- Is something they were expecting.
- Does not look odd with unusual spellings or characters.
- Passes your anti-virus program test.

Social Engineering and Phishing

Train your employees to recognise common cybercrime and information security risks, including social engineering, online fraud, phishing and web-browsing risks.

Social Media Policy

Educate your employees on social media and communicate, at a minimum, your policy and guidance on the use of a company email address to register, post or receive social media.

Mobile Devices

Communicate your mobile device policy to your employees for company-owned and personally owned devices used during the course of business.

Protecting Computer Resources

Train your employees on safeguarding their computers from theft by locking them or keeping them in a secure place. Critical information should be backed up routinely, with backup copies being kept in a secure location. All of your employees are responsible for accepting current virus protection software updates on company PCs.

The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document.



Travelers operates through several underwriting entities through the UK and across Europe.
Please consult your policy documentation or visit the websites below for full information.

travelers.co.uk travelers.ie

Building Resilience to Cyber Risk

Cyber Security + Cyber Insurance = Cyber Resilience

Cyber risk has emerged as one of the most important risks facing businesses in the 21st century. In 2009, there were 2.4 million new pieces of malware created. In 2015, more than 430 million new pieces of malware were discovered—over a million new pieces of malware each day.¹ Targeted attacks increased by 55% in 2015, and adversaries increasingly targeted smaller businesses, which were subjected to 43% of all spear phishing attacks.² Data breaches and business interruptions due to cyber attacks have become a key concern for businesses, when their systems and networks are hit.

Part of the solution is better cyber security, but when hackers can penetrate the networks of Fortune 500 companies and high-profile government agencies, no ordinary business or organisation can presume that it cannot be breached. For the

unprepared, the cost of a breach can be crippling. In 2015, the global average per-company cost of a data breach reached \$3.5 million.³ Cyber insurance provides a way for businesses and organisations to spread risk and, consequently, to be more resilient than they otherwise would be. By combining cyber security and cyber insurance, businesses and organisations can achieve greater cyber resilience against emerging cyber threats. A business or organisation is cyber resilient if: (1) it has implemented a cyber security programme that reasonably protects its information assets (taking into account the value of those assets and the surrounding threat environment), and (2) it has obtained cyber insurance that is reasonably sufficient to protect against residual cyber risks. Here are five critical steps towards achieving cyber resilience.



¹ <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>

² <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>

³ <https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF>

Five Steps Towards Cyber Resilience



1. Know your data, systems, and network

The first step towards cyber resilience is to “know thyself.” Know what (and where) data are being created, collected, and stored; maintain an accurate inventory of computer systems and software; and understand your network infrastructure. This will enable you to better identify and prioritise appropriate security controls, patch and maintain existing systems and software, and respond more effectively when an incident occurs.



2. Focus your cyber security efforts

Once you understand the data, systems, and network that you are trying to protect, you can focus on implementing (or improving) the security controls that would be most effective in light of your specific needs and resources. In doing so, you may want to consider the following:

- **What are your crown jewels?**

If you have adopted a data classification scheme, you may want to implement stronger security controls for the storage and transmission of data that are classified as more sensitive.

- **What are your vulnerabilities?**

A vulnerability assessment can help identify weak spots in your cyber security. If your organisation permits systems or network access to outside parties, such as contractors or vendors, understand that their vulnerabilities become your vulnerabilities.

- **What are the most likely threat scenarios?**

If you understand the threats that are most likely to impact your business or organisation, you can focus on meeting those threats.

Compliance with a particular cyber security standard is not a prerequisite to achieving cyber resilience, but it can be important in determining which security controls to implement. Businesses that handle payment card information, for example, must comply with the PCI Data Security Standard.



Email remains the medium of choice for cyber criminals. Phishing attacks were more targeted, and malicious emails grew in number and complexity.⁴



3. Educate your employees

Many cyber security incidents can be directly attributed to inadequate security awareness training. A training programme designed to empower employees to recognise common cyber threats and to notify the IT staff is a cost-effective way to reduce these threats.

A comprehensive training program should:

- Emphasise the importance of cyber security to the business or organisation’s success.
- Train employees to avoid information security risks.
- Explain how to protect laptops, mobile devices, and digital storage media.
- Encourage employees to report suspicious activity.

Employees should also receive training on policies and procedures that relate to cyber security. In many instances, explaining the rationale for restrictive “system use” policies will help to promote greater compliance.

⁴ <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>



4. Plan for incident response

Every business or organisation should plan for the unexpected, including a data breach or cyber incident. In fact, without an incident response plan, there is a greater likelihood of making mistakes in responding to the breach or incident—for example, by failing to comply with applicable laws and regulations. Such mistakes can cause damage to the business or organisation that goes beyond the damage directly caused by the attack. A well-designed incident response plan will make it easier to launch a rapid and coordinated response.

The incident response plan should provide a framework for action so that important decisions have been considered ahead of time and are not made under pressure. In particular, it is important for the incident response plan to provide procedures and guidelines on difficult issues, including identifying lines of authority and internal reporting obligations. The team should be focused on making the best possible decisions, not on figuring out how and by whom the decisions need to be made.

Once you have an incident response plan in place, it is important to test it regularly—annually, if possible. These “tabletop” exercises should involve the full incident response team, and the results of the exercise should be made available to senior management. It is better to address issues that might be raised by senior management about the incident response plan in connection with a tabletop exercise — not in the midst of an actual incident response effort.

The last five years have shown a steady increase in attacks targeting businesses with less than 250 employees.⁵

Not only can cyber insurance products help transfer some of the risks associated with cyber threats, but the insurance underwriting process can help identify cyber security vulnerabilities and improve cyber security.⁶



5. Insure against residual risk

Strong cyber security is just one part of the equation; obtaining cyber insurance is the other. According to UK Government’s Cyber Security Breaches Survey⁷, only 11% of all UK businesses have specific cyber insurance. This figure does increase for medium and larger firms, but only to 31% and 35%, respectively. According to the Association of British Insurers, “The rise in the number of large and medium sized firms having cyber insurance reflects greater awareness of the value of this cover, as insurers play a vital role in supporting customers to recover from an attack, and in helping them manage the cyber threat. But we need to do more to promote this insurance to smaller firms, who are often the least protected against cyber criminals.”⁸

Once a business or organisation knows its systems and data and understands its exposures, it will be well-positioned to work with an independent insurance agent or broker to evaluate its cyber insurance needs and to obtain coverage in this fast-growing insurance market.

⁵ <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>

⁶ http://www.aba.com/Tools/Function/Documents/2016Cyber-Insurance-Buying-Guide_FINAL.pdf

⁷ <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019>

⁸ <https://www.abi.org.uk/news/news-articles/2019/04/abi-responds-to-dcms-cyber-security-breaches/>



The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document. Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.