ZURICH

Security, Solutions, Simplicity.

Zurich Cyber Security & Privacy Liability Policy

A cyberattack impacts your business: A question of 'when', not 'if'.

In 2017, organizations around the world were hit by the WannaCry and NotPetya malware attacks. Both malicious programs quickly circled the globe, infiltrating networks, hijacking and locking down critical data, disrupting processes and supply chains, and creating digital havoc costing hundreds of millions of dollars. Will these isolated events be repeated? It's likely in today's rapidly evolving, increasingly threatening cyber risk environment. For most organizations, a serious and potentially damaging cyberattack is more a matter of 'when', not 'if'.

Security against the growing threat of costly cyberattacks

Solutions programmed to respond to an evolving risk environment

Simplicity in protecting against risk with one convenient program

According to the 2018 *Cost of Data Breach Study: Global Overview* conducted by the Ponemon Institute, the average total cost of an individual data breach is now USD3.86 million, an increase of 6.4% from the 2017 report.[1] The same study now estimates the average cost per lost or stolen record at USD148. Multiply that cost by the number of records that could be lost if your organization were hit by a serious data breach and theft. An attack targeting your organization need not be as wide-ranging as the infamous 2017 malware attacks to damage your network, business and reputation. How will you quantify the long-term impact on customer trust?

A convenient, single solution to help protect against cyber risks

The Zurich Cyber Insurance Policy can help you protect against the risks of a serious data breach. The program brings together features often attached to other commercial policies as coverage extensions by endorsement.

Key coverages and benefits

Liability coverages

- Security and Privacy Liability
- Regulatory proceedings defense costs
- Civil fines and penalties associated with Payment Card Industry (PCI) and General Data Protection Regulation (GDPR)
- Internet media liability

Non-liability coverages

- Privacy breach costs, including:
  - Forensic investigation expenses
  - Legal and public relations expenses
  - Credit and identity monitoring costs
  - Identity restoration and identity theft insurance costs
  - Call center costs
- Business income loss, dependent business income loss (i.e., loss insured incurs due to a vendor's network security event) and extra expense
- Digital asset replacement expense
- Cyber extortion threats and reward payments
- System failure and dependent system failure
- Reputational damages
- Social engineering funds transfer
- Claims mitigation costs

Additional policy highlights

- Coverage limits available up to USD25 million
- Business interruption coverage is triggered if a breach requires a voluntary shutdown of operations or a regulator ordered shutdown
- System failure and administrative errors can also trigger coverage
- Affirmative coverage for wrongful data collection
- Affirmative European General Data Protection Regulation (GDPR) coverage availability
- Definition of insured person extended to include temporary employees, volunteers or interns
- Definition of extra expenses amended to include forensic expenses

[1] Ponemon Institute. 2018 Cost of Data Breach Study: Global Overview. Sponsored by IBM Security. 11 July 2018. https://www.ibm.com/Security/DataBreach

- Broad definition of computer system, including industrial control systems and bring-your-own-device (BYOD) programs
- No vendor restrictions – you may seek assistance from the post-breach vendors of your choice

Cyber Risk Engineering services

On a fee-basis, Zurich's Cyber Risk Engineering team can also assist in the ongoing development and maintenance of a robust information security management system built on three essential pillars: people, process and technology.

People

- Board of directors and C-suite education
- User awareness training, including phishing, social engineering, password standards and management and business email compromise
- Security team training
- Hiring practice security guidelines
- Access management (i.e., users, vendors, privileged users and remote users)

Process

- Cybersecurity strategy
- Capability road map
- Policy and procedure development including, but not limited to, acceptable use, asset management, vulnerability and patch management, risk assessment, vendor management, incident response and disaster recovery
- Management metrics for cybersecurity

Technology

- Recommendations for a range of specialized technology solutions with leading external security vendors and consultants

ZenOpz – 24 / 7 / 365 Network Monitoring

An optional service available to organizations selecting the Zurich Cyber Security & Privacy Liability Policy.

In association with a leading managed security service provider (MSSP), Zurich delivers the following value-added services on an opt-in basis, included within policy premium:

- A complimentary, one-time 360-degree technical assessment of your network and all devices connected to it
- Real-time, 24/7 monitoring of up to 50 connected devices on your network, such as servers, workstations, firewalls and other log generating devices
- On a weekly basis, a full vulnerability scan of all devices in your agreement, with full status reports and patch recommendations to mitigate revealed vulnerabilities
- Ability to add devices for monitoring beyond the initial 50 for a fee

Protection for your business 24 / 7 / 365

DigitalResolve is a crisis management service, provided under your Zurich Cyber Security & Privacy Liability Policy, offering a global one-stop shop that harnesses and manages the resources you need to recover from a damaging cyber event.

If an incident occurs, you can call our multilingual team, day or night. A dedicated Incident Manager will then appoint and coordinate cyber experts to support your business. They will remain in place from notification to conclusion, managing the services and acting as your main point of contact throughout.

01	Contact DigitalResolve whenever an incident occurs, 24/7 365 days a year.
02	Incident Manager appointed immediately.
03	IT forensic experts appointed (if required) – they locate and act to resolve the event, and report to the Incident Manager.
04	Incident Manager consults with you and appoints other experts as required, such as lawyers and PR consultants.
05	Regular discussions between your business and all parties to agree best approach.
06	Other experts appointed where necessary, for example, notification and credit- monitoring specialists.
07	Comprehensive summary document issued at service conclusion.

Assigning your expert team

Each expert is carefully selected from a global panel of trusted providers covering:

- IT forensic experts and consultants
- Legal experts in data protection, cyber breaches, fraud and security
- PR consultants
- Credit monitoring
- Forensic accountants
- Cyber extortion ransom negotiators
- Public notifications including call center
- Internal forensics
- Regulatory notifications

Every panel member has been chosen for their proven track record and expertise, dedicated teams, global reach and established networks. The members also subscribe to our stringent standards and reporting structures. This provides you with the confidence of knowing your appointed team has the experience, resources and quality required to resolve a major cyber event.

Resolving your issues globally

DigitalResolve experts deal with incidents within the locations in which they occur. This local approach ensures your business doesn't suffer further incidents as a result of having to move data and information across geographical boundaries.

Setting up your DigitalResolve service

Our ideal approach is to work closely with you even before an incident occurs, providing advice and training if required. This will enable us to align our services with your own incident management processes to ensure the most effective, efficient and coordinated response.

Protecting you from breach, attack and failure

DigitalResolve from Zurich will:

- Locate and rectify the source of the attack, failure or breach.
- Help safeguard your business from further attacks and disruptions.
- Assess your financial losses by providing a dedicated forensic accountant.
- Protect your brand and reputation by deploying PR consultants.
- Ensure your business complies with any applicable regulations by providing legal support.
- Negotiate cyber ransoms, with legal supervision as required.
- Notify data subjects for regulatory and PR purposes.
- Undertake credit monitoring for data subjects and businesses.
- Seek to recover losses from negligent third parties.
- Risk manage your business to prevent or minimize future threats.

173005573 (03/19) TCL

ZURICH®