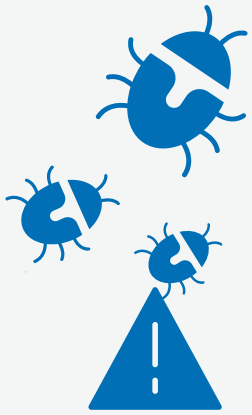
Zurich Cyber Solution: Security and Privacy Liability Policy

Protecting your critical data and digital assets

For most organizations, a serious and potentially damaging cyberattack is more a matter of 'when', not 'if'. Only recently, 'Emotet' reminded us of lessons learnt from 'NotPetya' and how quickly malicious programs circle the globe, infiltrating networks, hijacking and locking down critical data, disrupting processes and supply chains, costing hundreds of millions of dollars. The strong trend of working from home has unveiled further vulnerabilities.



According to the 2019 **Cost of Data Breach Study: Global Overview** conducted by the Ponemon Institute, the average total cost of an individual data breach is now USD3.92 million.[1] The same study now estimates the average cost per lost or stolen record at USD150 and the average size of a data breach was roughly 26,000 records. Multiply that cost by the number of records that could be lost if your organization were hit by a serious data breach and theft. How will you quantify the long-term impact on customer trust?

[1] Ponemon Institute. 2019 Cost of Data Breach Report: Sponsored by IBM Security. https://www.ibm.com/Security/DataBreach

ZURICH

Comprehensive insurance coverage, to help protect against cyber risks

Zurich Cyber Solution provides a streamlined, simple and clear policy structure. We have added new coverages focusing on Business Income loss extensions, have deleted or clarified exclusions, and have also revised our catalog of available endorsements.

We focused on meaningful extensions that enable us to tailor coverage to each customer's individual needs. Additionally, we have simplified our terminology and aligned it with market standards.

Key coverages and benefits

First-party covers

Breach costs, including:

- Forensic investigation expenses
- Legal and public relations expenses
- Expenses to restore reputation
- Credit and identity monitoring costs
- Expenses to notify customers and regulators after a breach
- Call center costs

Business income loss, dependent business income loss and extra expense

Digital asset replacement expense

Cyber extortion threats and reward payments

System failure and dependent system failure

Cyber fraud and social engineering (optional endorsement)

Emergency costs

Third-party covers

Security and Privacy Liability (including General Data Protection Regulation (GDPR))

Regulatory proceedings defense costs

Civil fines and penalties associated with Payment Card Industry (PCI)

Internet media liability

Additional policy highlights

Optional endorsements for IT hardware replacement (bricking), goodwill campaigns and telephone hacking

Business interruption coverage if a breach requires a voluntary shutdown of operations or a regulator ordered shutdown

System failure resulting from administrative errors

Affirmative coverage for wrongful data collection

Affirmative General Data Protection Regulation (GDPR) coverage

Definition of insured person extended to include temporary employees, volunteers or interns

Definition of extra expenses amended to include forensic expenses

Betterment included as standard if unavoidable and necessary

Broad definition of computer system, including industrial control systems (ICS) and bring-your-own-device (BYOD)

No vendor restrictions – Free choice of post-breach vendors (subject to terms & conditions)

Zurich Cyber Security Services

Cyber Risk Engineering services

Effective and robust cyber security requires an information security management system, built on three pillars: **People, Processes and Technology**. Zurich Cyber Risk Engineering can support your organization to align with these three pillars and help to develop and maintain an effective cyber security program.

Cyber Risk Assessments

Zurich Cyber Risk Engineers can help you to understand your risk by carrying out a cyber risk assessment.
The assessment will:

- analyze your core business processes or cyber exposure
- find weaknesses in your setup of controls
- benchmark the maturity of your cyber posture to industry peers
- identify and prioritize countermeasures to improve your cyber security.

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)

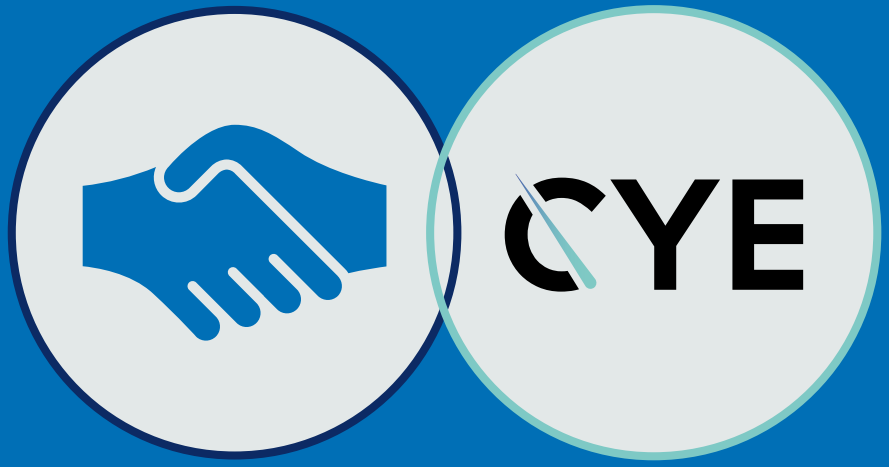
Processes

- Cyber security 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 cyber security

Technology

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

Strategic agreement with CYE



Since March 2020, we work with CYE, a highly qualified partner selected after a thorough 18-month worldwide scouting process, to extend Zurich Cyber Security Services.

Passive Cyber Risk Assessment Report and preferred rates

Each **Cyber insurance customer** will benefit from our collaboration with CYE and receive a comprehensive, technology-driven, passive risk assessment report evaluating your organization's posture regarding cyber threats.

In addition, your organization will also benefit from preferred rates on subscriptions to other CYE services.

Find out more about Zurich Cyber Security Services ›

Cyber Claims Response

DigitalResolve provides an optional incident response service, provided under your Zurich Cyber Solution policy, 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.

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

Resolving your issues globally

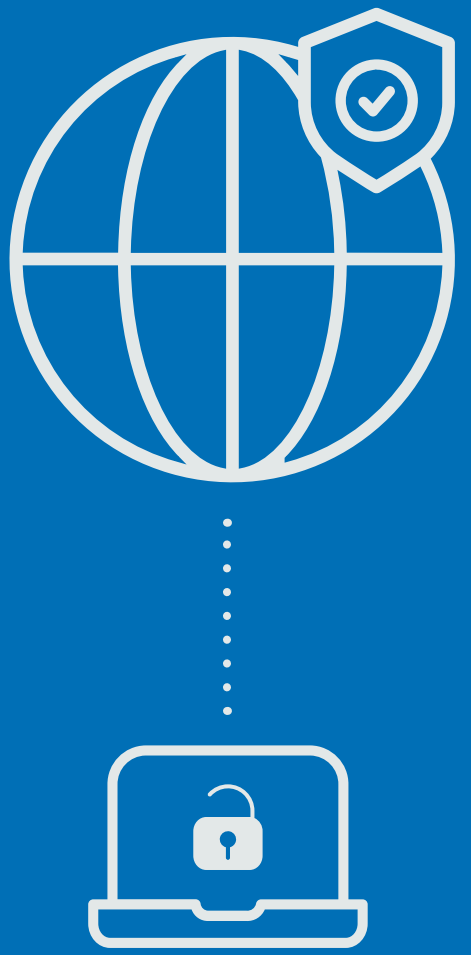
DigitalResolve experts deal with incidents within the locations in which they occur. This local approach ensures your business doesn't suffer further incidents as a result of having to move data and information across geographical boundaries.

Protecting you from breach, attack and failure

DigitalResolve 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.

Find out more about Zurich Cyber Security Services ›



ZURICH

Zurich Insurance Group Ltd.
Mythenquai 2
CH-8002 Zurich – Switzerland
www.zurich.com

173007320 (02/21) TCL