ZURICH
Resilience Solutions

Business Continuity and Cyber Risk Services

Integrated solutions to address critical exposures and build resilience

When disaster strikes, it's only natural to wish you could turn back time.

Threats to business continuity, such as cyberattacks, can disrupt critical systems, supply chains, and product transportation, bringing your entire operation to a standstill.

Zurich Resilience Solutions' Business Continuity and Cyber Risk specialists can help mitigate business and supply chain disruption threats taking a holistic approach to risk assessment, impact analysis and response planning, and more.

Business disruption risks are growing and evolving at the same lightning speed as technological advancements. Cyberattacks, Pandemics and natural hazards are just a few of the threats impacting businesses today. Among business continuity risks Cybersecurity is a top concern for senior management and boards.

The average cost of a data breach continued to rise in 2022, reaching an average of **$4.4 million globally** and **$9.4 million in the United States,** with **83% of companies** suffering more than one breach.[1] Total losses were over $10 billion, shattering 2021's total of $6.9 billion. Business interruption represents 60% of these claims.[2]

96% of corrupt downloaded software has an updated and fixed release available.[3]

Zurich's holistic solution

Zurich Resilience Solutions can provide comprehensive business continuity/cyber-focused services to address critical exposures and vulnerabilities that help you protect your business. Our Business Continuity Risk and Cyber specialists work closely with businesses of all sizes, from the middle-market to publicly traded companies to assess their unique digital environment and the effectiveness of current cyber defenses, mitigation, and response strategies.

Zurich provides a holistic view of your company's controls and analysis of your vulnerability to breaches, malware, ransomware, and other cyber threats and works with you to identify the best mitigation tools and strategies to address critical exposures and prevent business interruption.

Tailored services

Zurich takes a customized, consultative approach when assessing your current business continuity vulnerabilities and preparedness to help you develop and implement a cost-effective strategy that aligns with your objectives and meaningfully reduces your cyber and business disruption risk.

How customers benefit from our experience

- Advance your business continuity and cyber maturity to mitigate risks that were previously undiscovered.
- Know how you compare to your industry peers through our benchmarking capabilities.
- Make informed decisions from a cost-benefit perspective through our strategic advice.
- Prepare for emerging business disruption risks through forward-looking insights.
- Achieve stronger collaboration between Risk Management and Information Security / IT teams.

Services to address your needs

Objective evaluation of your business continuity strategy

Risk Health Check	Risk Gap Analysis and Strategic Roadmap	Business Impact Analysis
A comprehensive evaluation of your entire business continuity and cybersecurity program, including guided assessments of maturity, vulnerabilities, threat and business impact assessment for business and supply chain continuity, cybersecurity, and insurance value verification. The deliverable is a tailored report based on proprietary risk grading with a holistic analysis of your organization's risk health status and includes a summary of findings, strengths, weaknesses, and risk improvement actions that can be used to prioritize risk actions.	Using the Risk Health Check findings, we perform an analysis of your current controls and business practices and identify areas of vulnerability. Based on your vulnerabilities and threat landscape, we recommend improvements to your controls and business practices and create a customized roadmap.	A collaborative analysis with quantification of vulnerabilities and mitigation opportunities, including reviews of application and operating system access controls throughout your digital environment. This analysis helps organizations educate stakeholders, prioritize vital functions, resources, and process interdependencies via a facilitated, interactive session. Deliverables include risk profiles of vital activities and/or systems; potential resilience actions; and supporting equipment, personnel, and records necessary to perform critical functions.

Strengthen tactical areas of your cybersecurity program

Virtual CISO (vCISO)	Incident Response Plan Evaluation and Tabletop Exercise	Other Tailored Services, including:
Retain an experienced cyber professional to develop and execute your information security program. This can include creating and driving the roadmap, supporting implementation, and ongoing program management. This is ideal for mid-size companies without a Chief Information Security Officer.	A thorough review of your company's existing incident response plan, including policies, testing, and communication. This is often followed by an executive or technical tabletop exercise or both. Utilizing the same tool sets used for our IR investigations, we have the ability to deploy our SOCaaS to establish real-time monitoring of your environment and respond to threats on endpoints, servers, and a variety of cloud applications.	• Ransomware Threat Assessment • Vendor and Supply Chain risk management reviews • Security & Awareness training • Red Team exercises

Technical tools and services to help strengthen your business continuity program

Business Continuity Maintenance & Testing	24/7 Security Operations Monitoring & Response	Rapid Incident Response (IR) & Recovery
Business Continuity specialists conduct maintenance, testing and ISO Standard reviews, outline testing strategies, and conduct table-top exercises to ensure ongoing effectiveness of business continuity protocols. Cyber-counterintelligence engineers assess security controls by simulating attacks from the public internet and from an internal perspective, probing all systems for vulnerabilities. Upon completion, our recommendations help your business harden its overall security posture.	Working with a leading supply chain risk management software provider, Zurich provides an early warning tool for monitoring and 24/7/365 notification of all sites, with real-time alerts should your supply chain become compromised. This allows for a rapid response to reduce operational impact. Our experienced cybersecurity engineers and analysts actively monitor customer environments, engage in ransomware threat hunting, and remediate malicious activity in real-time. We deploy a fully managed security platform, to engage various threats around the clock.	In the event of a cybersecurity incident, our SOC team can deploy tools and personnel to remediate the ongoing threat, restore business operations, and complete digital forensics analysis. Our IR services include 45 days of 24/7 network monitoring, and a comprehensive report.

[1] IBM Ponemon Institute, IBM Cost of Data Breach Report 2022
[2] FBI Internet Crime Complaint Center (IC3), FBI 2022 Internet Crime Report
[3] Sonatype, 9th Annual State of the Software Supply Chain, 2023.

Contact us:

Zurich Resilience Solutions
800-982-5964
zrs.esg@zurichna.com
zurichna.com/risk/supply-chain-risk-services

The Zurich Services Corporation
Zurich Resilience Solutions I Risk Engineering
1299 Zurich Way, Schaumburg, Illinois 60196-1056
800.982.5964 www.zurichna.com

A1-P0676925-A (12/23) P0676925