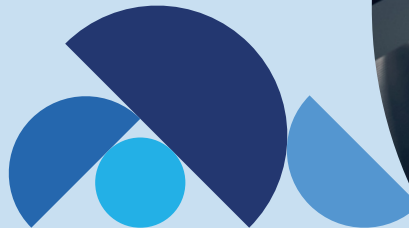


Zurich Resilience Solutions and SpearTip Cyber Risk Services

Zurich Resilience Solutions and SpearTip offer comprehensive cyber services to address critical exposures and vulnerabilities so you can protect your business.



The challenge

Cybersecurity is among the top concerns for senior management and boards, as companies are exposed to a wide variety of vulnerabilities that pose existential threats. Prioritizing investment in cybersecurity can be daunting, with risks evolving daily. The hardest part can be knowing where to start.

Our team can provide a holistic view of your controls and their adequacy concerning your exposure. The results will be presented in the context of business risk so various stakeholders understand them but with appropriate technical depth to target specific risk areas and shrink your overall attack surface.



Where do I start?

Our goal is to help you develop and implement a cost-effective strategy that meaningfully reduces your cyber risk. We take a consultative approach to understand your current position, actively assess your cyber security and make recommendations in line with your objectives. While each engagement is flexible and customized to your needs, the following page includes common starting points.

74%

of all breaches involve the human element: Error, Privilege Misuse, Stolen Credentials, or Social Engineering.¹

Who we are & how we deliver

Zurich's extensive experience in Cyber Risk Analysis and SpearTip's technical solutions have been combined to help customers address cybersecurity gaps by assessing their unique digital environment and the effectiveness of current cyber defenses.

Benefits you can expect

Your organization will benefit from our team's extensive experience and pragmatic approach.

Specifically, you will be better positioned in several ways:

- Advance your cybersecurity maturity and 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 cyber risks through forward-looking insights
- Achieve stronger collaboration between Risk Management and Information Security / IT teams

1. Verizon's 2023 Data Breach Investigations Report: <https://www.verizon.com/business/resources/reports/dbir/>

Services to Address Your Needs



Objective evaluation of my cyber security strategy

Cyber Risk Health Check

A broad comprehensive, interview-based assessment of your cyber security exposures and controls guided by the NIST Cyber Security Framework. The deliverable is a tailored report based on proprietary risk grading with specific recommendations for your organization.

Cyber Risk Gap Analysis and Strategic Roadmap

A comprehensive evaluation of your entire cybersecurity program, assessing maturity level for each of the 108 NIST CSF sub-categories. Based on your attack surface, threat landscape, and our findings, we will recommend improvements to your controls and business practices through a custom strategic roadmap plan.

Web Application Assessment

Our team reviews application and operating system access controls throughout your digital environment. We verify your security measures are aligned to your usage and security stack so only validated users can access critical systems and sensitive data.



Strengthen tactical areas of my cyber security program

Virtual CISO (vCISO)

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.

Incident Response Plan Evaluation and Tabletop Exercise

A thorough review of your company's existing IR plan, including policies, testing, and communication. This is often followed by an executive or technical tabletop exercise or both.

Other Tailored Services, Including

- Ransomware Threat Assessment
- Vendor and Supply Chain Risk Management Reviews
- Security & Awareness Training
- Red Team Exercises



Technical tools and services to help strengthen my cyber risk defenses

Penetration Testing

Cyber counterintelligence engineers assess your organization's 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.

24/7 Security Operations Center (SOC) Monitoring & Response

We deploy ShadowSpear, a fully managed security platform, to engage various threats around the clock. Our experienced security engineers and analysts actively monitor customer environments, engage in ransomware threat hunting, and remediate malicious activity in real-time.

Rapid Incident Response (IR) & Recovery

In the event of a security 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 continued network monitoring and a comprehensive report.

The Zurich Services Corporation

1299 Zurich Way, Schaumburg, IL 60196-1056
800 982 5964 www.zurichna.com

For further information, please contact the Zurich Cyber Risk Engineering Team at CyberRE@zurichna.com

This is a general description of certain types of managed security services, and/or other risk engineering or risk management services provided by Zurich Resilience Solutions, which is part of the Commercial Insurance business of Zurich Insurance Group and does not represent or alter any insurance policy or service agreement. Such services are provided to qualified customers by affiliates of Zurich Insurance Company Ltd, including but not limited to SpearTip, LLC, 1714 Deer Tracks Trail Suite 150, Saint Louis, MO 63131, USA; and The Zurich Services Corporation and Zurich American Insurance Company, each at 1299 Zurich Way, Schaumburg, IL 60196, USA. The opinions expressed herein are those of SpearTip, LLC as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any of its affiliated companies (collectively, Zurich Insurance Group) as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group. Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product nor will it ensure coverage under any insurance policy. No member of Zurich Insurance Group accepts any liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction. In the United States, managed security services are provided by SpearTip, LLC and risk engineering and risk management services are provided by The Zurich Services Corporation.