Local Policies: Cyber Liability

Specific Considerations

Nicole Stecker
Technical Underwriting

Local Policies: Cyber Liability-specific considerations

 Jurisdiction-Specific Cyber Threats	• **Localized Threat Landscape:** Different regions may face unique cyber threats (e.g., specific types of malware, ransomware, or cyber espionage) that require tailored coverage. • **Industry-Specific Risks:** Certain countries may have a higher concentration of specific industries (e.g., technology hubs) that face distinct cyber risks.
 Regulatory Requirements for Cyber Security	• **Data Breach Notification Laws:** Different countries have specific requirements for data breach notifications that must be complied with in the event of a cyber incident. • **Cybersecurity Regulations:** Some jurisdictions have stringent cybersecurity laws (e.g., General Data Protection Regulation (GDPR) in Europe, Lei Geral de Proteção de Dados (LGPD) in Brazil) that mandate specific security measures and impose hefty fines for non-compliance.
 Coverage for Local Third-Party Service Providers	• **Vendor Risk Management:** Coverage for cyber incidents involving local third-party service providers, which may vary in terms of contractual obligations and cybersecurity practices. • **Cloud and IT Services:** Ensuring that policies cover incidents related to local cloud and IT service providers, who may operate under different regulations.

Local Policies: Cyber Liability-specific considerations

 Local Incident Response and Forensics	• **Availability of Local Expertise:** Access to local incident response teams and forensic experts who understand the local cyber threat landscape and regulatory environment. • **Coordination with Global Teams:** Ensuring smooth coordination between local incident response efforts and the global cybersecurity team.
 Cultural and Behavioral Factors	• **Employee Awareness and Training:** Different levels of cybersecurity awareness and training among employees in various regions, necessitating customized risk management and training programs. • **Local Cyber Hygiene Practices:** Variability in cyber hygiene practices across different countries, affecting the overall risk profile.
 Insurance Market Maturity	• **Availability of Specialized Coverage:** The maturity of the local cyber insurance market can affect the availability and quality of specialized cyber coverage. • **Local Underwriting Expertise:** Leveraging local underwriters who have a deep understanding of the regional cyber risks and regulatory landscape.

Local Policies: Cyber Liability-specific considerations

 Cross-Border Data Transfers	• **Compliance with Data Transfer Regulations:** Ensuring that policies address the complexities of cross-border data transfers, especially in regions with strict data localization laws. • **Impact on Cyber Incident Response:** Managing the impact of cross-border data transfer restrictions on incident response and forensic investigations.
 Reputation Management and Legal and Compliance Support	• **Local Media and Public Relations:** Addressing the reputational impact of cyber incidents in local media and managing public relations in accordance with cultural norms. • **Stakeholder Communication:** Effective communication with local stakeholders, including customers, regulators, and partners, during and after a cyber incident. • **Local Legal Expertise:** Access to local legal counsel experienced in cyber liability and regulatory compliance to navigate the aftermath of a cyber incident. • **Regulatory Investigations:** Coverage for costs associated with regulatory investigations and fines, which may vary by jurisdiction.
 Technological Infrastructure	• **Regional Differences:** Variability in technological infrastructure and cybersecurity readiness across different regions, impacting the risk landscape. • **Cyber Insurance Innovation:** Leveraging innovative cyber insurance solutions tailored to the specific needs and technological landscape of each region.

ZURICH

Legal Disclaimer:

The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute advice (particularly not legal advice). Accordingly, persons requiring advice should consult independent advisors when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. We undertake no obligation to publicly update or revise any of this information, whether to reflect new information, future developments, events or circumstances or otherwise. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.