CYBERSECURITY AWARENESS MONTH

IMPACTS OF CYBER THREAT LANDSCAPE ON INSURERS AND POLICYHOLDERS

by Lynn Rohland and Darin Brooks

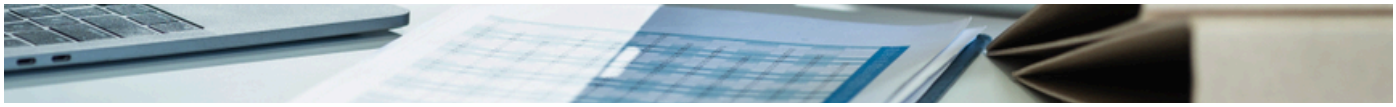
As cyber threats continue to evolve and increase, insurers are responding by imposing stricter requirements on policyholders to obtain and maintain coverage. This shifts how businesses should implement, manage, and oversee IT departments and cybersecurity programs in preparation for cyber risks.

Insurers are tightening policy requirements, such as mandating multi-factor authentication and strengthening incident response plans, to address the increasing costs of cyber claims driven by sophisticated threats like ransomware.

How These Measures Manage Risk and Impact Claims

Cybercriminals attempt network attacks every 39 seconds, with 4,000 ransomware attacks occurring daily, or one attack every 2 seconds. In 2024, 1.73 billion personal data records were breached in the U.S.

CYBERSECURITY AWARENESS MONTH



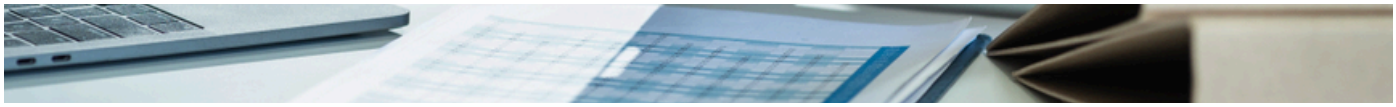
By requiring companies to upgrade cybersecurity defenses and raise resiliency expectations, insurers aim to reduce the frequency and severity of claims in an increasingly volatile cyber threat environment. By aligning with these updates and more rigorous expectations, businesses can secure comprehensive cyber insurance coverage and strengthen their overall cybersecurity posture to mitigate risks more effectively.

The new requirements and stricter mandates introduced in recent years aim to raise awareness and, more importantly, reduce the risk of attacks on their policyholders and potential claims. It's done by encouraging policyholders to update and improve IT security policies and cybersecurity practices, ensuring comprehensive coverage. For example, insurers now require businesses to implement multi-factor authentication (MFA) for all access points, including user and administrative accounts, as well as remote and privileged access, to reduce the risk of unauthorized access. Failure to do so may result in coverage denials, reduced coverage, or higher premiums.

Incident Response and Recovery Plans

For example, formal incident response and recovery plans, along with regular testing, are vital components of most policies. Companies need to develop and routinely test a comprehensive incident response plan through tabletop exercises and cybersecurity drills, as insurers increasingly reject claims if businesses cannot demonstrate proactive preparedness. Enhanced endpoint detection and response (EDR) solutions are also essential for monitoring and responding to threats in real time. Failure to do so can result in policy exclusions, limited coverage, or increased costs.

CYBERSECURITY AWARENESS MONTH



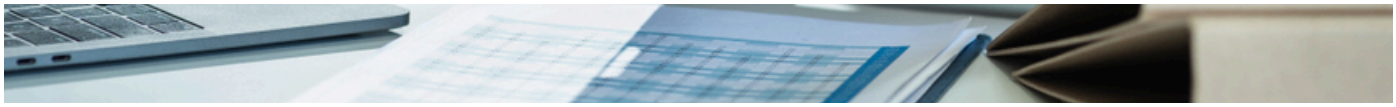
Third-Party Risk Management

Insurers are also compelling businesses to take decisive steps to enhance how they evaluate partners by enforcing stricter standards for third-party vendor risk management. Companies will increasingly need to demonstrate robust risk management programs, including cybersecurity assessments of third-party providers, because insurers might deny coverage for breaches caused by supply chain vulnerabilities resulting from inadequate evaluation or oversight.

Vulnerability Scanning and Patch Management

Another requirement that insurers expect is continuous vulnerability scanning and patch management. This means insurers want policyholders to regularly conduct vulnerability scans and quickly patch known issues. Coverage may be denied or limited if incidents happen due to unpatched systems.

CYBERSECURITY AWARENESS MONTH



AI-Based Threat Detection and Response Technologies

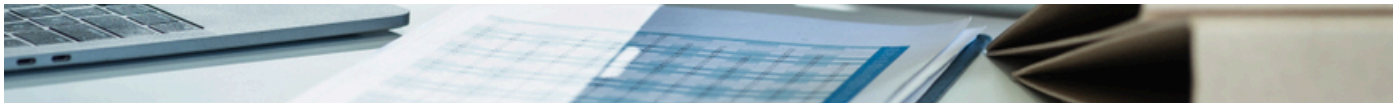
On a more positive note, as AI-powered cyberattacks increase, insurers are rewarding businesses that adopt AI-driven cybersecurity tools for real-time threat detection, often providing premium discounts to those using these advanced defenses. By implementing AI-based threat detection and response technologies, policyholders and insurers can benefit from reduced risks and minimized financial impacts from most attacks.

Regulatory Compliance

Finally, businesses are increasingly required to provide proof of compliance with data protection laws such as the Texas Data Privacy and Security Act (TDPSA), the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), or the Security and Privacy Rules under the Health Insurance Portability and Accountability Act (HIPAA). Although these laws are based on mandates at the state or regional level, most industry leaders and insurers recognize that they also serve a dual purpose. Specifically, their design also functions as a regulatory compliance framework that increasingly demands proof of adherence to avoid coverage gaps, fines, or penalties.

Recognizing the surge in cyberattacks over the past decade and the increasing sophistication of these attacks by criminals, both insurers and policyholders can benefit from improved outcomes stemming from businesses fortifying their networks, hardware, and software, as well as adopting industry-leading practices.

CYBERSECURITY AWARENESS MONTH



Insurers are reinforcing their expectations with current and prospective policyholders to safeguard their business models and bottom lines through mandates such as MFA, EDR, and comprehensive incident response plans, mitigating legal and reputational risks. In short, insurers attempt to limit financial losses from payouts by decreasing the frequency and severity of claims amid an unpredictable threat environment. This improves their ability to offer policyholders more competitive premiums for compliant businesses. Likewise, by deploying strategic and tactical enhanced protections, policyholders make themselves less susceptible to cyberattacks and align with evolving regulatory standards. Ultimately, policyholders benefit from improved risk management, minimized business disruptions, and reduced financial impacts resulting from fines, breach responses, or retrofitting cyber defenses.

Contact Us

Lynn Rohland
Gray Reed Advisory Principal
703.801.6075 | lrohland@grayreedadvisory.com

Darin Brooks
Gray Reed Partner and Insurance Practice Group Leader
713.398.7585 | dbrooks@grayreed.com