Chicago IT Company CEO Stephen Taylor Warns of Denied Cyber Insurance Claims Due to Incomplete MFA/2FA


Stephen Taylor - CEO

CHICAGO, IL, UNITED STATES, June 3, 2026 /EINPresswire.com/ -- IT company and cybersecurity provider LeadingIT (600 W Jackson Blvd, Chicago, IL 60661, (815) 308-2095) CEO Stephen Taylor has one thing he wants you to read before your next cyber insurance renewal. According to the NAIC's 2025 Cybersecurity Insurance Report, in 2024 nearly three times as many cyber insurance claims were closed without payment as were paid. 28,555 were denied. 9,941 were paid. (Source: NAIC 2025 Cybersecurity Insurance Report.)

If you have cyber insurance and you think you are covered, those numbers are worth sitting with. The most common reason claims are being denied is not fine print and it is not bad luck. According to Coalition's 2024 cyber claims data, 82% of denied claims involved organizations that did not have MFA fully implemented across their environment. MFA is the second login verification step, the code on your phone or the authenticator app prompt. Not having it enforced everywhere, not just on email but on every VPN, every remote access point, every admin account and privileged account, is the gap the bad guys walk through and the same gap insurers use to deny your claim.

What has changed in 2026 is how insurers find that gap. Marsh McLennan's 2025 Cyber Insurance Market Report found that 99% of cyber insurance applications now include specific questions about MFA implementation, and 41% of applications are denied on first submission. But the bigger shift is what happens at renewal and after a breach. Carriers have moved from self-reported questionnaires to technical audits of your actual environment. Some are running security scans before binding coverage. You can no longer answer yes on an application and assume that is the end of it. LeadingIT, a trusted technology partner for Chicago-area businesses,

works with clients across the Loop, River North, West Loop, and Cook County as a managed service provider delivering managed IT services, cybersecurity, and IT support/outsourcing solutions built to hold up when that technical audit actually happens.

So what do the cyber insurance MFA requirements look like right now? First and foremost, MFA needs to be enforced on everything, and the method matters. Insurers now want authenticator apps or a hardware token rather than SMS, which can be intercepted and is no longer considered sufficient coverage. Second, get endpoint detection on every device. EDR works like a security camera inside your machine watching for suspicious behavior in real time, not just blocking threats it already recognizes. Third, make sure you have tested backups stored separately from your primary systems, centralized logging, and a written incident response plan. Get all of this layered up and you protect your cyber coverage. S&P Global is forecasting a 15 to 20% premium increase in 2026. Organizations that fully implement and document these controls have seen premiums fall 50 to 60% compared to those without them. (Source: S&P Global Ratings, 2026 Cyber Insurance Market Outlook.)

“Over the last year or two, insurance companies have paid out huge claims for ransomware incidents and these cyber threats, and now they’re really taking a hard look at frankly just controlling their losses. The application process now is very much looking for ‘do you have multi-factor on?’ and if you don’t, we’re seeing more non-renewals, or not even offering a quote, or even cancellations of current policies. Insurance carriers can no longer absorb these kinds of risks.” said Stephen Taylor, CEO of LeadingIT.

This is not about fear. It is about being in control. A denied claim means legal fees, regulatory fines, and the full recovery bill land on your business with no safety net. For a Chicago-area business with 30 to 150 employees, that starts in the six figures. Chicago businesses looking to review their managed IT services setup and cybersecurity posture before their next renewal can get a straight answer at LeadingIT's Chicago office. Find out more at LeadingIT or view open IT positions on the team.

About LeadingIT

LeadingIT is a managed IT services and cybersecurity firm serving Chicago, IL and surrounding areas including the Loop, River North, West Loop, Lincoln Park, Fulton Market, and businesses throughout Cook and DuPage counties. Located at 600 W Jackson Blvd, Chicago, IL 60661, LeadingIT specializes in managed IT services, cybersecurity, IT help desk support, cloud solutions, and network security for small and mid-sized businesses. For inquiries, call (815) 308-2095 or visit goleadingit.com

Laura Piekos
LeadingIT
+1 815-308-2095
marketing@goleadingit.com