Tamara Ashjian Shares 2026 Outlook on Cyber Risk and Readiness

Tamara Ashjian, a Los Angeles–raised cyber claims leader, outlines what individuals should expect as cyber threats grow more frequent and complex.

New York City, New York May 23, 2026 (Issuewire.com) - As cyber threats continue to evolve, insurance claims leader Tamara Ashjian is offering a clear, practical outlook on what individuals should expect over the next year—and what they can do now to stay prepared.

With nearly 20 years in insurance and close to a decade focused on cyber and technology claims, Ashjian has seen how quickly the landscape can shift.

“Cyber risk doesn’t stand still,” she says. “It changes faster than most people expect, and that’s where the gap starts.”

What Changed Recently in Cyber Risk

Over the past few years, cyber threats have become more widespread and more personal. What was once seen as a corporate issue now affects individuals and small businesses every day.

- Over 70% of cyber attacks now target small businesses
- Ransomware attacks increased by more than 90% in recent years
- The average global data breach cost is over $4.4 million
- Phishing attacks account for over 80% of reported cyber incidents
- Nearly 60% of small businesses close within six months of a major cyberattack
- Human error is responsible for over 80% of breaches
- Multi-factor authentication can reduce risk by up to 99%

“The biggest shift is how widespread it has become,” Ashjian explains. “It’s no longer isolated. It touches almost everyone in some way.”

What People Are Still Getting Wrong

Despite growing awareness, many individuals still underestimate their exposure.

“People hear about breaches, but they don’t connect it to their own lives,” Ashjian says. “That’s the disconnect.”

She points out that many incidents stem from simple oversights—weak passwords, outdated systems, or lack of basic security habits.

“I don’t believe in overcomplicating things,” she adds. “But ignoring the basics is where problems start.”

What Is Likely to Get Harder

Looking ahead, Ashjian expects cyber threats to become more sophisticated and more persistent.

Attackers are targeting individuals through email, mobile devices, and even social platforms. At the same time, recovery is becoming more complex due to regulatory requirements and data sensitivity.

“Every case is different,” she says. “You might be dealing with a ransomware issue one day and a data breach the next. That unpredictability is what makes it harder.”

She also notes that the emotional and financial impact on individuals is often underestimated.

“It’s not just about systems,” Ashjian explains. “It’s about disruption, stress, and trying to rebuild trust.”

What Will Actually Work

Ashjian’s outlook is grounded in simple, consistent action rather than complex solutions.

“Start with the basics,” she says. “Understand your risks, then build from there.”

She highlights habits that remain effective:

- Use strong, unique passwords
- Enable multi-factor authentication
- Keep systems and software updated
- Back up important data regularly
- Be cautious with emails and links

“These are simple habits,” she adds. “But they make a real difference when something goes wrong.”

Three Scenarios for the Next Year1. Optimistic Scenario: Increased Awareness, Lower Impact

More individuals adopt basic protections. Incidents still occur, but damage is reduced.

Best Actions:

- Enable multi-factor authentication across all key accounts
- Use a password manager
- Regularly review account activity

2. Realistic Scenario: Continued Growth in Attacks

Threats increase steadily. Most people improve slightly, but gaps remain.

Best Actions:

- Update all devices and software regularly
- Back up critical data weekly
- Stay alert to phishing attempts

3. Cautious Scenario: Higher Frequency, Greater Impact

Attacks become more targeted and disruptive. Individuals without preparation face serious consequences.

Best Actions:

- Audit all personal and business accounts for security gaps
- Limit data sharing across platforms

- Create a response plan for potential breaches

A Practical Outlook

Ashjian's message is not alarmist. It is practical.

"You don't need to be an expert," she says. "You just need to pay attention and take a few consistent steps."

Her experience across environmental, legal, and cyber claims has shaped that perspective.

"You focus on doing the job well," she adds. "In this case, the job is protecting your own information."

Call to Action

Tamara Ashjian encourages readers to choose one of the three scenarios that best fits their current situation—optimistic, realistic, or cautious—and take the recommended steps today.

"Start small," she says. "But start now. The sooner you act, the better positioned you are."

About Tamara Ashjian

Tamara Ashjian is an experienced insurance claims leader with nearly 20 years in the industry. She most recently served as Vice President of Cyber & Tech Claims at Tokio Marine HCC, where she led the handling of complex cyber and technology-related claims. She previously held leadership roles at NAS Insurance Services, Ironshore Insurance, and AIG, and began her career as a litigation attorney. Ashjian holds a BA from UCLA and a JD from Whittier Law School and is a member of the California and New York State Bars. She is known for her practical approach, leadership, and deep expertise in cyber risk.

Media Contact

Tamara Ashjian

*********@tamara-ashjian.com

https://www.tamara-ashjian.com/

Source : Tamara Ashjian