

Retail's most valuable asset isn't inventory, it's trust.

Friday, June 19, 2026

Today's top story, from reporter Euny Hong:

When a cyberattack disrupts a retailer's supply chain, the damage extends well beyond delayed shipments and lost revenue. For brands that have spent decades—or even centuries—cultivating a reputation for quality, a breach can undermine something far harder to restore: customer trust.

That risk is growing. Cyberattacks against supply chains have increased fourfold in just the past five years, according to the 2026 X-Force Threat Intelligence Index.

"If you're Hermès or Louis Vuitton, your history goes back centuries," IBM's Elaine Parr, Senior Partner and Consumer Products and Retail Industries Leader for the EMEA region, said in an interview with IBM Think. "They pride themselves on 100% perfection."

A security breach, Parr said, can affect the entire value chain, from logistics to manufacturing to the customer experience.

The dilemma is that while customers obviously expect quality, they also want the convenience of technology, according to Parr. "From a brand's perspective, screwing this stuff up is much riskier than it's ever been. After COVID, customers want it now, and they are less sympathetic to a bad experience." Furthermore, she added, "customers want a frictionless life. [When buying online], they want a seamless omnichannel experience."

But the quest for convenience can come at a cost, IBM Distinguished Engineer Jeff Crume said in an interview with IBM Think. Many e-commerce sites, for example, still rely on the one-step password login, but that isn't secure. "We've been saying for a while that the bad guys have realized it's easier to log in than hack in," Crume said, noting that threat actors can easily obtain user credentials through spoofed websites or phishing attacks.

The barrier of access to vulnerable systems is lowering. According to the Threat Intelligence Index, the past year has seen a 44% increase in the number of security breaches arising from the exploitation of public-facing applications, such as company websites or customer portals.

A good solution, he said, is passkeys. "Passkeys are phishing-resistant," he explained. "If I steal your password, I can log back in as you any number of times. But a passkey is only good for a certain specific period."

While some companies might balk at the expense and work involved in implementing a passkey system, Crume said, the long-term savings far outweigh any upfront costs. "People don't forget their passkeys, because they didn't know what they were in the first place," he said. "This will reduce the number of calls to the help desk, and that will be a huge savings."