Whistling Past the Graveyard: Businesses Claim They Aren't Very Worried About a Cyberattack

October 23, 2023 at 9:00 AM EDT

Source: James Edgar, Chief Information Security Officer

Each October, we conduct a survey that provides an industry pulse in support of Cybersecurity Awareness Month, which was first declared by the President of the United State and Congress starting in 2004. Coined the FLEETCOR State of Business Cybersecurity Report, the 2023 survey provides an intriguing snapshot of the cybersecurity landscape for U.S. companies. While the fear of falling victim to a cyberattack is palpable, it seems that many businesses aren't necessarily taking steps that reflect that concern. A look at the survey results of 316 CIOs and IT decision makers reveals a surprising discrepancy between perceived cybersecurity readiness and the actual experience of cyberattacks.

What Me Worry?

The most striking finding in the report is the low number of companies that reported experiencing a cyberattack in the past 12 months, at only 7%. This figure stands in contrast to the prevalent concerns of businesses about the looming threat of cyberattacks in the future, with 51% being very or somewhat concerned. And yet, 61% said they are very or somewhat comfortable with their current cybersecurity posture and capabilities.

This leads to an interesting question: Why do so many companies feel comfortable with their current cybersecurity defenses when so few haven't directly experienced a cyberattack? I have to wonder if more companies have been attacked than are letting on, considering a cyberattack could be phishing, ransomware, DDos, BEC, etc. Maybe they were attacked and didn't know it. Perhaps it's a case of "ignorance is bliss."

Yes, You Should Worry

Businesses should not underestimate the threat of cyberattacks. While the percentage of companies that are comfortable with their cybersecurity posture is significant, it's essential to remember that confidence can sometimes lead to complacency. Cybersecurity is not a "set it and forget it" affair. It requires continuous vigilance, adaptability, and a proactive approach to stay ahead of evolving cyber threats. The absence of a direct attack shouldn't lull companies into a false sense of security. It should instead serve as a reminder to maintain and fortify their defenses – when it comes to cyber-attacks, it's not a matter of "if", but "when".

One of the most troubling aspects of this situation is that despite the concerns about future cyberattacks, few businesses are translating their fears into concrete actions. The report indicates that most companies are not increasing their cybersecurity budgets or planning to deploy Artificial Intelligence (AI) as a resource. This may be a case of the classic "it won't happen to us" mentality, which can prove to be a costly mistake in the world of cybersecurity.

Better Safe Than Sorry

A bright light in the survey findings is that most companies acknowledge that if attacked, the loss of profitability and/or disruption to their operations would be their biggest concern. Given that, they would do well not to take the threat lightly. Cyber defense is a proactive investment in the long-term security and stability of a business. Cyberattacks can lead to significant financial losses and operational disruptions, causing more harm than many businesses might anticipate. That's why, despite the relatively low number of companies experiencing cyberattacks so far, the focus on cybersecurity should remain sharp, with continued investments in technology, training, and policies to safeguard against future threats.

In conclusion, the FLEETCOR State of Business Cybersecurity 2023 Report provides a valuable wake-up call to the business world. The low levels of direct experience of cyberattacks and high levels of confidence about companies' cybersecurity suggest a laissez faire approach to the subject that could be costly in the end. Businesses should be aware of the unpredictability of cyber threats and the importance of staying ahead of the game. Cybersecurity is not something to be deferred for another day. It's an essential aspect of modern business operations that requires constant attention and investment to ensure a safe and secure future. After all, in the realm of cybersecurity, it's always better to be safe than sorry.