

# CFOs: lowering your cyber insurance premiums depends on phishing-resistant MFA

Your CISO shouldn't be the only executive in charge of your cyber security strategy. As CFO, you're the gatekeeper for data that is highly attractive to cyber criminals: budgets, investment strategies, M&A details, and pre-public financial results.

While SEC reporting requirements mandate significant transparency into your cyber strategy, the average CFO isn't as engaged in understanding cybersecurity implications as they should be:



of CFOs are confident in their organizations' cyber security capabilities, but only 66% of CISOs are (Source)



CFOs are not regularly briefed by their cybersecurity teams (Source)



Annual cyber insurance premiums are expected to **grow from \$12 billion globally to \$60 billion globally** in the next five to ten years (Source)



of small and medium-sized enterprises with a cyber insurance policy say that their insurance provider helped them avoid potential incidents (Source)

# Protecting your organization with cyber insurance is a must, but qualifying for it has never been harder

As cyber attacks like phishing and ransomware get more pervasive and sophisticated, cyber insurance premiums get higher and underwriting requirements get stricter. Ensuring your organization is seen as a viable and trusted business entity, and covered financially in the case of a ransomware attack, rests not only with your CISO but you as well.



of businesses say they would reconsider entering into a partnership or agreement with another business or supplier if the organization did not have comprehensive cyber insurance (Source)



of companies that have cyber insurance coverage have used it, and 50% have used it more than once (Source)



of small and medium-sized enterprises without cyber insurance say that a major cyberattack could destroy their business (Source)



The average cost of a ransomware attack in 2022—excluding the ransom itself (Source)



of reported incidents in 2022 involving a phishing attack (Source)

# Reduce cyber risk and cyber insurance cost with phishing-resistant MFA

“When my premiums are down by a third and others are going up by 20% or higher, that’s a really big win.”



**Brent Deterding**  
AFNI CISO  
[Yubi.co/afni](https://yubi.co/afni)

Cyber insurance should not be your only line of defense because it is limited in its ability to cover potentially catastrophic losses from systemic cyberattacks. You need to prevent cyber attacks before they happen, which is why cyber insurance providers are increasingly requiring that multi-factor authentication (MFA) be in place before they write new policies.

Not all MFA is created equal, though. Phishing-resistant MFA, delivered by modern hardware security keys, makes it easier to qualify for cyber insurance and, in some cases, cheaper. Just ask Afni, which saved 30% on its premiums by using YubiKeys.

Read our [cyber insurance whitepaper](#) to learn how to navigate the rapidly changing landscape and higher qualification requirements—and why phishing-resistant MFA is a critical component.

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passkey authentication to customers in 160+ countries. For more information, visit: [www.yubico.com](https://www.yubico.com).

© 2024 Yubico

 **Contact us**  
[yubi.co/contact-us](https://yubi.co/contact-us)

**yubico**