yubico

Cyber insurance requirements raise the security bar

Critical role of phishing-resistant MFA to deliver the strongest security

The evolution of cyber insurance and escalating premiums

In 1995, when the first cyber insurance policy hit the market, few people besides IT insiders understood the true risk and cost implications of digital disaster. Not anymore. Since then, cyber attacks have become ubiquitous, sophisticated, high-profile, and in some cases devastating. Rarely a month goes by without a major attack capturing headlines and redefining expectations for cybersecurity. And with the recent rise of ransomware, the stakes have never been higher – cyber crime led to $6 trillion in losses in 2021 alone, growing at 15% year over year.

The result, not surprisingly, has been increased demand for cyber insurance. But just as companies have struggled to keep their IT assets safe from ever-evolving attacks, insurance companies have struggled to effectively underwrite cyber risks. Some see the potential losses as too great and have stopped offering cyber insurance entirely. Those that remain have raised premium prices by 150-300% in many cases.

Higher premiums offset the risk for cyber insurance providers, but not by much. In order to make cyber insurance a viable product in a world of skyrocketing cyber risk, the probability of successful attacks must drop dramatically. Back in 1995 when the biggest risk was hardware failure, anyone with a pulse and a credit card could obtain a policy. Now, however, companies need to prove they are meeting minimum cybersecurity standards and taking cyber hygiene and resilience seriously. Obtaining coverage (at any price) depends on it. Therefore, any company that wants to get or keep cyber insurance needs to evaluate and possibly upgrade their own security posture.

Bare minimum security will no longer get cyber insurance coverage

Every insurance provider devises its own cyber insurance coverage requirements, but the vast majority will expect coverage seekers to have email security controls, endpoint detection and response tools, next-gen antivirus protections, and backup and recovery capabilities at minimum. Important as those may be, however, the cyber insurance industry considers multi-factor authentication (MFA) to be the single most important defense. In fact, cyber insurance may be *impossible* to obtain without MFA in place.

These new and heightened security requirements make perfect sense. No other security control does more to reduce cyber risk than MFA, because it not only mitigates risk associated with an evolving cyber threat landscape, but can also minimize risks associated with poor user behaviors and errors. Without it, private accounts and sensitive assets are highly vulnerable to attack regardless of what other protections are in place. By requiring extra layers of authentication, companies can stop phishing and ransomware attacks, which is enough to deter the many hackers seeking the path of least resistance. And for the determined few that remain, compromising two or more authentication layers represents a formidable obstacle.

For anyone seeking cyber insurance, the first priority is implementing MFA across the entire organization. And while the perceived fastest, cheapest, or easiest solution, such as SMS or mobile authentication, might seem sufficient, insurance providers might see it differently. They want to cover companies that are most immune to attack, especially as providers become more risk averse. Therefore, the right choice for MFA is the one that offers best-in-class protection, now and into the future. Anything less only escalates risk for the company and the insurance provider – so anything less will be increasingly unacceptable for obtaining or maintaining cyber insurance.

Phishing-resistant MFA more critical now than ever before

Multiple authentication factors are always more secure than a single factor. That said, some forms of MFA are significantly less secure than others. For example, MFA products that send a one-time-password (OTP) to someone's phone or email addresses, while more secure than passwords alone, are still vulnerable to phishing attacks. All a hacker must do is convince a person to authenticate to a fake site that looks identical to the real site where the hacker gathers the user credentials and MFA codes. And once they have them, they can easily authenticate themselves and continue with their attack under the guise of an authorized user, which can delay detection until it's too late with massive repercussions.

Phishing-resistant MFA works differently. Instead of authenticating users based on "something they know" like an OTP, it authenticates users based on "something they have" like a security key that they plug into the USB port of their device. Remotely exfiltrating the secrets of a hardware-based security key is nearly impossible compared to how easily SMS codes and other methods can be easily intercepted by remote and man-in-the-middle attacks, as proven by many incidents in the news. As a result, true phishing-resistant MFA is an approach that is extremely hard to compromise so companies, and their cyber insurance providers, can rest easy knowing that only the right users are gaining access to sensitive resources.

All federal agencies were recently mandated to adopt phishing-resistant MFA, and it's becoming a requirement with State and Local agencies as well as with the private sector. And to be truly phishing-resistant, these organizations are urged to adopt MFA based on FIDO/WebAuthn or Smart Card/PIV protocols. Anything less is not phishing-resistant, and is below the acceptable standard for security-conscious organizations. Companies that adopt this modern security approach are at a drastically lower risk of a successful cyber attack. Therefore, not only are they the most appealing candidates for cyber insurance coverage with possibly lower insurance premiums, they are also the most secure from financial, legal, and reputational damage that no amount of coverage could fix.

YubiKeys–phishing-resistant MFA that positions you well for new cyber insurance requirements

Yubico has been a leader and innovator in the field of strong authentication for over a decade. Our signature product, the YubiKey, is considered a best-in-class solution by many security experts and cyber insurance providers alike.

> " Yubico's role in the industry is unique, the solutions that Yubico offers today are the next generation of identity security. The rest of the world needs to catch up with Yubico and not the other way around.
>
> Steve Brasen, Research Director, Enterprise Management Associates

Modern security: Time and extensive studies have proven that YubiKeys stop phishing and other strategies for account takeovers in their tracks. YubiKeys support multiple authentication protocols on a single security key, such as legacy authentication protocols such as OTP, but also the modern security protocols that offer true phishing-resistance such as FIDO U2F and FIDO2/WebAuthn as well as Smart Card/PIV. By offering multi-protocol support, YubiKeys enhance the security posture of organizations no matter where they are on their authentication journey, and across a variety of legacy on-premises and modern cloud infrastructures.

Risk of account takeovers

0% Security key (YubiKey)

10% On-device prompt

24% SMS code

21% Secondary email

50% Phone number

Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.

Fast and easy user experience: The simplicity of YubiKeys is another key differentiator. YubiKeys do not require client software to be installed and they require no batteries or a cellular connection. So users can just plug it into a USB port and touch the button, or tap-n-go using NFC for secure authentication. The user self-service capabilities enable organizations to quickly and easily empower users to self-provision their YubiKey without heavy involvement from IT or a need to come into the office. Phishing-resistant MFA can be set up in minutes and the YubiKey functions effortlessly across laptops, tablets, and smartphones, even operating as a smart card depending on the company's needs and policies to access certain systems.

Reduce financial, legal and reputational risk: The cost of global cybercrime is expected to be $10.5 trillion by 2025 despite companies spending hundreds of billions of dollars to strengthen their cybersecurity postures. YubiKeys have you covered by offering the strongest levels of phishing defense delivered by purpose-built hardware security keys that protect your business and its users by side-stepping modern cyber risks.

Summary:

A cybersecurity breach can have catastrophic implications for the affected organization. It translates to downtime and lost opportunity, and significantly impacts cyber insurance providers as well. Stay protected and set yourself up for the best position by considering an MFA approach that can stand up to current threats, as well as one that is future-proofed to handle increasingly sophisticated ones. YubiKeys secure a wide array of environments and provide the convenience needed to support today's modern in person, hybrid, and remote employees. And offers a consistent, strong, phishing-resistant MFA approach for the modern ways organizations and their users work.