yubico

WHITE PAPER

Meeting enhanced cyber insurance requirements with strong authentication

Raising the bar on security with phishing-resistant MFA

Contents

2 Table of contents

3 Cyberattacks increase demand for cyber insurance

4 What is cyber insurance?

5 The evolution of cyber insurance coverage

5 New coverage terms

6 Changing cybersecurity requirements

8 The critical need for phishing-resistant MFA

10 Modern, phishing-resistant authentication with YubiKeys

11 Simplified procurement and distribution of strong security at scale

11 Summary

Cyberattacks increase demand for cyber insurance

$4.35 million

cost of data breach[1] in 2022

97.1%

increase in cyber insurance rates for top 25% of companies in 2021Q4[2]

57%

of healthcare organizations say cyber insurance **harder to secure**[3]

50%

of education organizations need higher level of cybersecurity to qualify[4]

Most attackers don't hack in, they log in.

Most ransomware attacks result not just from employees or users clicking on questionable links, but from hackers stealing credentials and logging into a company's systems and downloading malware, letting the damaging process play out long before it is detected.

Despite best efforts across the globe, cyberattacks continue to rise in both frequency and severity. The average organization now faces a 32% year-over-year increase in the number of cyberattacks per week,[6] including ransomware, phishing, and Man-in-the-Middle attacks. Compromised credentials continue to be the most common attack entry point—61% of data breaches traced back to stolen credentials in some way.[7] Most recently, more than 130 companies were compromised by the 'Oktapus' phishing breach, with attackers using compromised credentials for one service to breach another.[8] When it comes to ransomware, compromised credentials and phishing are still the most common paths leading into the organization, followed by vulnerabilities and botnets.

Not only are cyber threats increasing, cyberattacks are also more disruptive and costly than ever before, including expensive business interruptions, a greater number of and cost associated with ransomware, and increasing long-tail risks associated with litigation and more stringent regulations. Ransomware demands alone can run in the millions, including the $4.4 million ransom demanded in the Colonial Pipeline attack.[10]

Cyber risk is becoming an ever-greater business liability, with 40% of business leaders reporting cyber threats as the No. 1 business risk—one with the potential to decimate an organization and, in the worst cases, make recovery impossible.[11] As a result, organizations have increasingly turned to cyber insurance to help them recover from damage or minimize impact. According to the US Government Accountability Office (GAO), the global take-up rate for cyber insurance rose from 26% in 2016 to 47% in 2020.[12]

At the same time as organizations turn to cyber insurance, that insurance has become harder to secure. The average settled cyber claim is $4.88 million, with this high claim severity and claim frequency leading carriers to change their policies to limit losses—or to leave the cyber insurance market altogether. A GAO investigation noted that cyber insurers and the Terrorism Risk Insurance Program (TRIP) are both "limited in their ability to cover potentially catastrophic losses from systemic cyberattacks."[13] A Canadian Federal report on insurers found that insurers faced a 113% loss ratio on cyber insurance policies for the first half of 2021, with net claims exceeding net premiums.[14]

Cyber risk is becoming an ever-greater business liability, with 40% of business leaders reporting cyber threats as the No. 1 business risk—one with the potential to decimate an organization and, in the worst cases, make recovery impossible.

As a result of the potential for loss, cyber insurance premiums have gone up as much as 300% across high risk industries,[15] with new sub-limits and exclusions. Further, underwriting questions and audits have become more commonplace as insurers better attempt to quantify and control for loss.

American International Group (AIG) increased its premiums by 40% globally, with CEO Peter Zaffino sharing with analysts that it is continuing to “carefully reduce cyber limits and are obtaining tighter terms and conditions to address increasing cyber loss trends, the rising threat associated with ransomware and the systemic nature of cyber risk generally.”[16] Insurer Allianz Global has made clear its own position on cyber risk, stating that “purchasing cyber insurance should be one of the final points in a company’s plan to enhance its cyber resilience.”[17]

As insurers react to the changing threat and regulatory landscape, organizations should be prepared to provide evidence of cyber risk mitigation efforts, including multi-factor authentication (MFA) to address the very high prevalence of credential-involved attacks, in order to qualify for cyber insurance.

Cyber insurance premiums have gone up by as much as 300% across high risk industries.

What is cyber insurance?

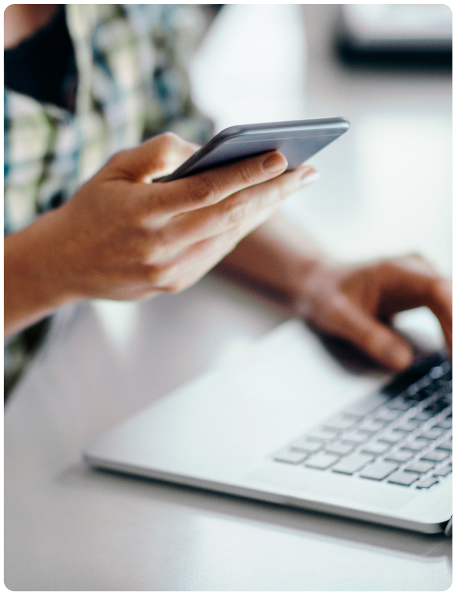
Cyber insurance, also referred to as “cyber risk insurance” or “cyber liability insurance,” is a form of business insurance designed to protect a policyholder against digital risk, compensating for losses resulting from covered incidents such as malware, ransomware attacks or data breaches. Losses could be either direct or indirect costs associated with data loss, business interruption or extortion, fraud, or liability. Policies draw a distinction between first-party damages (eg. losses to the company itself) and third-party damages (eg. losses to customers or vendors).

Cyber insurance coverage varies widely in terms of when, why, and how much it pays out, how much it costs, and what it takes to obtain coverage. When a company experiences a loss, the insurance provider will investigate the claim and either pay to cover the costs, up to the coverage limit, or dispute the settlement. Most cyber liability insurance will exclude attacks caused by human error or cybersecurity mismanagement.

As cyberattacks become more prevalent and more expensive, carrying adequate amounts of cybersecurity insurance becomes an important component of enterprise risk management and, for some organizations, a requirement under law or contract.

The evolution of cyber insurance coverage

> “Some insurance providers have left the market as it has simply become unprofitable for them. Those that remain are looking to reduce risk and exposure. They are also pushing up prices considerably.
>
> With fewer organizations providing cyber cover, it’s a sellers’ market. They call the shots and they can be selective about which clients they cover. Having strong cyber defenses will significantly improve an organization’s ability to secure the cover they need.”
>
> Sophos Report, 2022[18]



Shifting risks and higher-than-anticipated losses have been reflected in the changing face of cyber insurance coverage. As a result, during the past year, premiums grew 18% in the first quarter of 2021 and 34% in the fourth quarter of 2021 to help stabilize the market and more accurately reflect long-term risk.[19]

Some insurers are also reducing coverage or changing other terms both generally, as well as to reflect risk specific to industries or organizations. For example, 46% of healthcare organizations say they have exclusions or exceptions in their policies for ransomware, a gap that exposes these organizations to the full cost of an attack.[20]

New coverage terms

Brokers and carriers have responded to risk with greater scrutiny, risk selection, and terms that could include:

- **Higher premiums**
- **Higher retentions** (e.g. business interruption minimum)
- **More exclusions**
- **Limits and sublimits** (e.g. ransomware payouts, regulatory costs)
- **Co-insurance requirements**
- **Stricter cybersecurity requirements**
- **Expert support**

As some traditional insurers leave the cyber insurance marketplace, new cyber insurance startups are appearing on the scene to fill the gap. These new startups (and some traditional brokers and carriers) include expert support before, during and after cyber incidents—a process to reduce exposure to risk and/or to increase resolution time. Some insurers also work with, or provide, continuous analytics to better respond to risk.

Changing cybersecurity requirements

Avoiding an attack will always be preferable to recovering from one, even with cyber insurance. What's more, lax cybersecurity practices could violate the terms of the cyber liability insurance policy and negate settlement opportunities. For many reasons, it's important to maintain robust cybersecurity and rely on cybersecurity insurance only as a means to round out risk management. To put it differently, a cyber insurance policy is a strong last line of defense, but it can't be the only line of defense.

Today's cyber insurance policies are designed with that premise in mind. Nearly all insurers today require verification, by questionnaire or audit, of some preventative cybersecurity controls which could include:

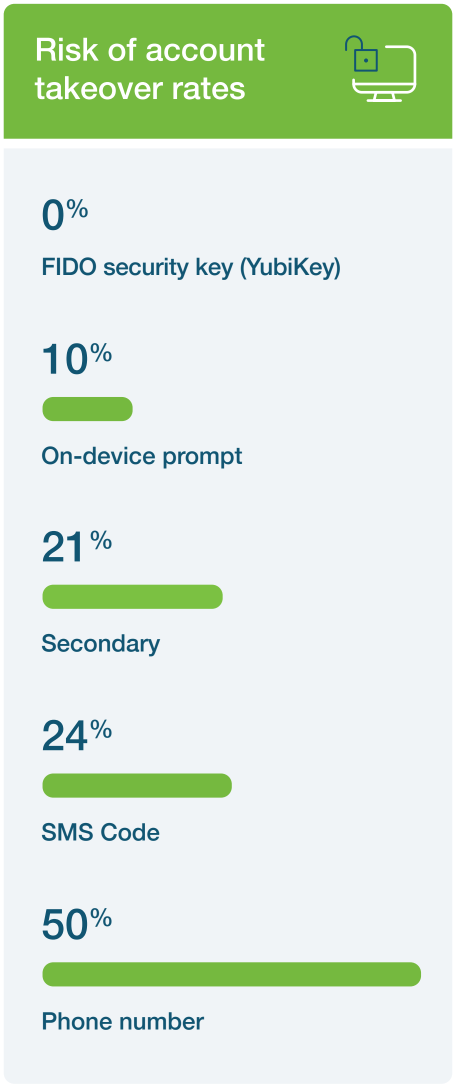
- Multi-factor authentication (MFA)
- Patch management
- Employee training
- Effective back-up strategy
- Endpoint detection & response
- Network security
- Incident response planning

Organizations that do not meet baseline cybersecurity requirements could struggle to secure coverage or secure coverage that is more expensive with poorer terms. The good news is that for organizations that do invest in cybersecurity controls such as MFA, there are opportunities for better rates.

Organizations of all sizes and across all industries face these new requirements, although some industries more acutely than others. Those sectors facing the highest level of risk, particularly those targeted by ransomware, those with complex cyber insurance requirements (e.g. education), or those organizations with the highest levels of third-party and/or supply chain risk (e.g. manufacturing) will face the highest pressure to strengthen their cybersecurity.

> If you don’t have MFA in place, there’s a very good chance you’re not even going to get a quote, so that’s probably the most important”
>
> –John Farley, Managing Director, Gallagher Global Brokerage cyber practice[21]

The critical need for phishing-resistant MFA



Google: How effective is basic account hygiene at preventing hijacking attacks

Historically, cyber insurance coverage could be extended to any organization willing to pay the premium and was often used to address risks that were too expensive or difficult to solve technologically. As the old cyber insurance models buckle under the pressure of increased risk, organizations today face new terms and requirements in order to gain the desired level of coverage and/or avoid additional premiums.

Organizations with insufficient security will likely be denied for some, if not most or all, cybersecurity insurance policies—a situation which has negative repercussions for business viability. However, the “healthiest” organizations are likely to receive the lowest risk scores—and, in turn, the most favorable rates or terms.

According to the 2022 March and Microsoft Global Cyber Report, 41% of organizations say that insurers’ requirements are “influencing decisions to augment existing controls or adopt new ones.”[22]

For any organization seeking or renewing cyber insurance, the first priority is implementing MFA. 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 the best security—and not all MFA is created equal.

Modernize MFA to address security and cyber insurance requirements

Here’s a truth we all accept: passwords are no longer enough. But other familiar forms of MFA such as mobile-based authenticators, including SMS-based one-time password (OTP) or push apps, also fall short on security.

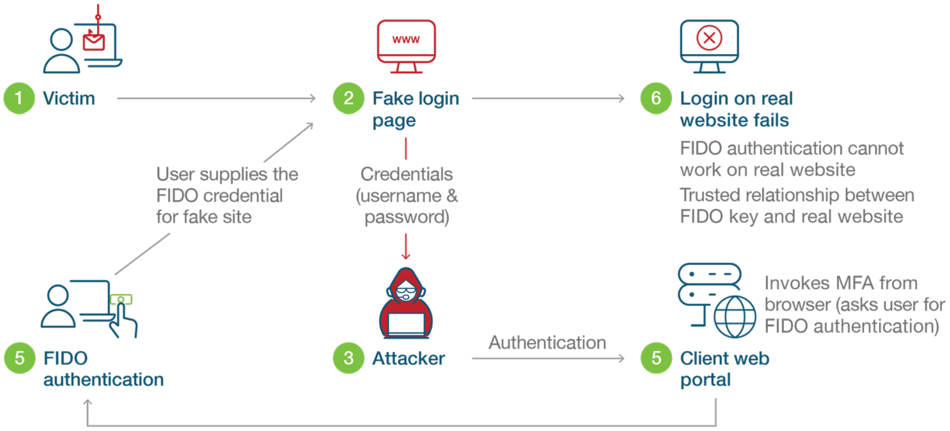
While any form of MFA offers more security than passwords alone, each still relies on passwords as the first factor. Further, mobile-based MFA ties the second factor to the mobile device, which offers no guarantee that the private key ends up on a secure element on the mobile device, the OTP code or private key could be intercepted in some way, and it is impossible to ensure proof of possession; or in National Institute of Standards and Technology (NIST) terms—impossible to prove it is phishing-resistant.

Research by Google, NYU, and UCSD, based on 350,000 real-world hijacking attempts, revealed that a SMS-based OTP only blocked 76% of targeted attacks and a push app only blocked 90%.[23] That’s, at minimum, a 10% penetration rate. Any penetration rate above 0% only escalates risk for the company and the insurance provider and will become increasingly unacceptable for obtaining or maintaining cyber insurance.

Phishing-resistant MFA refers to an authentication process that is immune to attackers intercepting or even tricking users into revealing access information. The only two standards that are considered phishing-resistant are the Federal Government’s Personal Identity Verification (PIV) / Smart Card standard and modern FIDO/WebAuthn. The FIDO (Fast IDentity Online) modern authentication standard enables strong two-factor, multi-factor, and passwordless authentication.

Phishing-resistant authentication can put a halt to ransomware entry that relies on stolen or phished credentials. Here is how phishing-resistant MFA stops a ransomware attack:

How phishing-resistant MFA stops a ransomware attack


1 Victim
2 Fake login page
6 Login on real website fails
FIDO authentication cannot work on real website
Trusted relationship between FIDO key and real website
User supplies the FIDO credential for fake site
Credentials (username & password)
www
Invokes MFA from browser (asks user for FIDO authentication)
5 FIDO authentication
3 Attacker
Authentication
5 Client web portal

Ransomware grew by over 485% in 2020

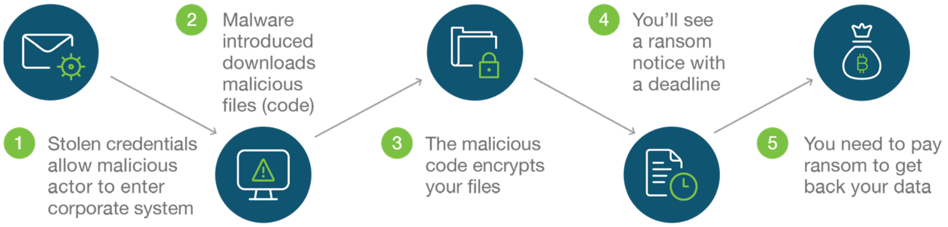
The new ransomware-as-a-service (RaaS) model of profit-sharing in exchange for ransomware tools has proven to be effective.

The anatomy of a ransomware attack

A ransomware attack is the result of a chain of events, and not a singular event. That chain of events begins with infiltrating an organization through stolen credentials, phishing attack (often also targeting credentials), or direct attack. With stolen credentials, the attacker walks in disguised as a legitimate user, making this type of attack difficult to detect.

Once inside, the attacker has a path to collect data before “executing” the ransomware attack. Thus, the best way to combat the growing threat of ransomware is to improve patching and to implement phishing-resistant MFA so that attackers cannot steal credentials as easily as they do with passwords or legacy MFA such as SMS and mobile authentication apps.

How ransomware works


1 Stolen credentials allow malicious actor to enter corporate system
2 Malware introduced downloads malicious files (code)
3 The malicious code encrypts your files
4 You’ll see a ransom notice with a deadline
5 You need to pay ransom to get back your data

By executive order, federal agencies and private sector organizations serving these agencies are required to modernize cybersecurity, as part of Zero Trust initiatives, with phishing-resistant MFA.[24] Phishing-resistant MFA positions organizations well to meet new cyber insurance requirements, to negotiate for the best rates, and to put a stop to out-of-policy costs associated with data breaches.

Modern, phishing-resistant authentication with YubiKeys

Yubico has been a leader and innovator in the field of strong authentication for over a decade. The YubiKey, a hardware security key manufactured by Yubico, is considered a best-in-class solution by many security experts and cyber insurance providers alike – proven to stop phishing and account takeover attacks in their tracks.

The YubiKey offers easy-to-use two-factor, multi-factor, and passwordless authentication at scale to help organizations quickly and easily become cyber insurance ready.

The YubiKey supports multiple authentication protocols on a single security key, including legacy authentication protocols such as OTP as well as modern security protocols that offer true phishing-resistance such as FIDO U2F, FIDO2/WebAuthn, and Smart Card / PIV. By offering multi-protocol support, the YubiKey can quickly and easily enhance the security posture of organizations no matter where they are on their authentication journey—and across a variety of on-premises and modern cloud infrastructures.

The YubiKey is a cost-effective and scalable solution that works out-of-the-box with leading IAM and PAM solutions, major browsers, and hundreds of applications and services. The simplicity of the YubiKey also makes it an attractive, and effective, solution for end users, with no client software to be installed and no batteries or cellular connection. Users just plug the YubiKey into a USB port and touch the button or tap-n-go using NFC for secure authentication.

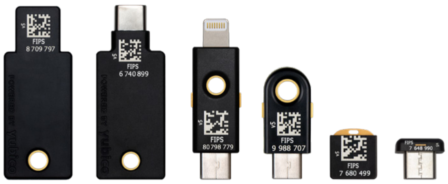
> “We believe that by using YubiKeys we’ve raised the standard of security for our employees beyond what was commercially available. The device works with Google’s Web browser Chrome, and works very seamlessly for people in their day-to-day workflow here at Google.”
>
> –Mayank Upadhyay, Director of Security Engineering, Google Inc.

The YubiKey

is the **only** solution that is highly phishing-resistant, and is proven to stop **100%** of account takeovers in independent research.

The YubiKey 5 Series

From left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano



The YubiKey 5 FIPS Series

From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS

YubiKey Bio Series - FIDO Edition

From left to right: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition

Simplified procurement and distribution of strong security at scale

Yubico also offers YubiEnterprise Services, consisting of YubiEnterprise Subscription and YubiEnterprise Delivery, to help simplify procurement and distribution of YubiKeys for employees at scale across corporate and residential locations across 49 countries.

YubiEnterprise Subscription

With YubiEnterprise Subscription, organizations receive a service-based and affordable model for purchasing YubiKeys with benefits such as predictable spending, upgrades to the latest offerings, customer support and more. This is especially important for organizations experiencing business growth or employee churn.

YubiEnterprise Delivery

With YubiEnterprise Delivery, organizations experience turnkey authentication with shipping of YubiKeys, tracking, and returns processing of Yubico products handled seamlessly by logistics experts, so organizations can focus on what matters—securing the workforce and delivering great customer experiences.

Summary

The current cyber attack landscape has catastrophic implications for affected organizations, translating to downtime and lost opportunity and high recovery costs, as well as for insurance providers who take on great risk.

To navigate today's complex cyber insurance landscape, organizations that implement phishing-resistant MFA have taken a stand against current and future threats and are in an optimal position to lower their cyber risk score with insurers.

The YubiKey is an extremely robust and reliable solution (IP68 certified), offering high security to help organizations become cyber insurance ready.

Sources

[1] Bethan Moorecraft, Cyber insurance: Hard market drivers and how to mitigate them, (March 9, 2022)

[2] Sophos, The State of Ransomware in Healthcare 2022, (Accessed August 26, 2022)

[3] Sophos, The State of Ransomware in Education 2022, (July 12 2022)

[4] IBM, 2022 Cost of Data Breach Report, (Accessed August 12, 2022)

[5] Joe Galvin, 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack, (Accessed August 31, 2022)

[6] Check Point, Check Point Research: Weekly Cyber Attacks increased by 32% Year-Over-Year; 1 out of 40 organizations impacted by Ransomware, (July 26, 2022)

[7] IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021), (Accessed May 18, 2021)

[8] Robert Martinez, Rustam Mikasymov, Roasting Oktapus: The phishing campaign going after Okta identity credentials, (August 25, 2022)

[9] Verizon, Data Breach Investigations Report 2022, (Accessed August 31, 2022)

[10] Evan Perez et. al., First on CNN: US recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers, (June 9, 2021)

[11] PwC, PwC Pulse Survey: Managing business risks, (August 18, 2022)

[12] GAO, Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market, (May 20, 2021)

[13] GAO, Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Events, (June 2022)

[14] Greg Meckbach, How much Canadian insurers have lost on cyber liability so far in 2021, (August 31, 2021)

[15] Ryan Smith, Cyber insurers raising premiums, lowering coverage limits - report, (October 11, 2021)

[16] Reuters, AIG is Reducing Cyber Insurance Limits as Cost of Coverage Soars, (August 6, 2021)

[17] Allianz, Managing the impact of increasing interconnectivity: Trends in cyber risk, (March 2021)

[18] Sophos, The State of Ransomware in Healthcare 2022, (Accessed August 26, 2022)

[19] Stephen Lawton, Turbulent Cyber Insurance Market Sees Rising Prices and Sinking Coverage, (June 2, 2022)

[20] Sophos, The State of Ransomware in Healthcare 2022, (Accessed August 26, 2022)

[21] Bethan Moorecraft, Cyber insurance: Hard market drivers and how to mitigate them, (March 9, 2022)

[22] Marsh, Q2 2022 US and Canada Cyber Market Update, (June 29, 2022)

[23] Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)

[24] OMB, M-22-09, (January 26, 2022)

yubico

About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: www.yubico.com.