yubico

CASE STUDY

GENERALI

Industry

Insurance and asset management

Benefits

Reduction in the probability of negative cyber events–even with just 10 YubiKeys

Introducing cybersecurity best practices to Polish enterprises

Protocols

FIDO2

FIDO U2F

Products

YubiKey 5 NFC

Deployment info

10 YubiKey Starter Kit to every new CyberRED customer

Discounted price to extend deployment through MCX Group

Generali Poland delivers innovative cyber insurance solution and reduces risk for organizations with the YubiKey

Global insurer partners with Yubico and MCX group through innovative cyberRED policy

Generali Poland creates CyberRED policy to reduce risk for customers in the fight against cyberattacks

In 2024, Poland became the most cyber-attacked country in the world, the result of its geopolitical position as a NATO and European Union member country and Russia's ongoing war against Ukraine.[1] Increasingly sophisticated attacks target the information technology (IT) and operational technology (OT) systems of government and critical infrastructure providers, impacting national security and resulting in costly production outages and financial losses.

"There have been more and more serious and broad-scale attacks in our country," says Michal Balwiński, Senior Underwriter and Cyber Practice Leader for Generali Poland, a part of the Generali Group. "There are risks arising from political actions and political motives, including cyberwarfare and cyberterrorism."

Generali Group, one of the world's largest insurance companies, provides insurance and investment products to individuals and commercial entities in over 180 countries. Generali has been present in Poland since 1998, offering life insurance, P&C, pension, investment products and, more recently, cyber insurance solutions and partnerships to proactively manage and mitigate cyber risk.

Although Poland has worked to strengthen its cyber defenses, currently ranking 6th in the globe for its commitment to cybersecurity collaboration, policies and regulations,[2] cyber readiness remains low for most organizations, with only 43% of enterprises having implemented a formal cyber risk review.[3] As insurers, Generali Poland must consider the implications and management of cyber risk for its clients, which Balwiński notes is the "most rapidly growing risk, in insurance terms."

> "Our vision is to not just provide the policy itself, but to be a partner to our customers."

Marcin Gajkowski | Director of the Third Party Liability Insurance Department | Generali Poland

Given the risk landscape and the growing needs of its customers, Generali Poland began offering a comprehensive cyber insurance solution, CyberRED, in 2021. Cyber insurance is much more comprehensive than standard civil liability insurance, as it covers losses associated with incident response, including downtime and system recovery, as well as any civil or regulatory liabilities associated with a data breach. CyberRED is a customizable policy, with up to ten categories of coverage, as well as 24/7 cybersecurity support to mitigate and respond to cyber attacks.

64%

Within Poland, at least 64% of cyber attacks are linked to **phishing** and **credential theft.**

Cyber insurance risk models all share the same basic tenet: that premiums remain commensurate to risk, with companies at highest risk paying the highest premiums—or not qualifying at all. Like with other global insurers, to qualify for CyberRED coverage, organizations must adopt a base level of risk management practices, including the use of strong multi-factor authentication (MFA). In fact, strong MFA plays such a critical role in protecting against cyber attacks that CyberRED policies now come with a starter bundle of FIDO2 YubiKey security keys from Yubico, reinforcing Generali Poland's commitment to helping its customers in the fight against cyber attacks.

Strong MFA a base requirement for cyber insurance

Generali Poland recognizes that cyber insurance is the last line of defense in effective risk management, but it cannot be the only line of defense. In order to quantify and control for loss, the insurer looks at company size and business sector, as well as organizational security policies and postures, in order to create an individualized insurance package detailing coverage terms, premium and potential sub-limits, exclusions or high deductibles.

Within Poland, at least 64% of cyber attacks are linked to phishing and credential theft.[4] As such, legacy authentication methods such as usernames and passwords and mobile-based authenticators present unacceptable levels of risk for most insurers. In fact, independent research has demonstrated that SMS-based OTPs block only 76% of targeted attacks and push apps block only 90%.[5]

When examining security policies, Generali Poland collects, evaluates and analyzes the level of the client's contribution, their retention of risk, from open-source intelligence (OSINT) as well as by questionnaire. Based on this information, a contract is offered only to organizations that demonstrate good risk management.

"We treat cyber insurance as the proverbial icing on the cake," says Marcin Gajkowski, Director of the Third Party Liability Insurance Department, Generali Poland, "No organization is 100% immune from attack. So, if you have a risk management system and you manage risk sensibly, then insurance is a safeguard if something goes wrong."

While each insurer has its own guidelines as to what businesses it will insure, Generali Poland requires a minimum of two technical standards: regular backups and the use of MFA, ideally phishing-resistant MFA. Phishing-resistant MFA refers to an authentication process that is immune to attackers intercepting, or tricking users into revealing, access information, which today includes either Smart Cards or the modern FIDO2 (passkeys) authentication standard.

"It's important that if an organization allows remote or hybrid working, we require the use of an encrypted channel, for example a VPN, and that MFA be used, ideally phishing-resistant MFA," says Balwiński. "It's a red flag for us if clients don't have MFA for remote work at all. Strong, phishing-resistant MFA is a technology that is in line with the risk and the dynamics that we see in the market. Despite the addition of a second-factor, entering a code from an SMS or a token from an application is still leading to unauthorized logins, and these are very common scenarios. Strong MFA prevents these scenarios."

Generali Poland looks closely at MFA implementations to determine premiums, looking not only at the strength of MFA but also use cases. In particular, the insurer examines those connections that carry the most risk such as remote work and privileged accounts that have elevated access to data, devices or systems (e.g. IT admins, developers, C-suite, finance or sales).

"In situations where MFA has been implemented throughout the company, particularly across top management activities and privileged users in the IT team, that can translate into a bonus in insurance premiums," says Balwiński. "A broad MFA implementation demonstrates a higher level of security and a higher level of awareness of risk on the part of the customer. That's very important for us."

> "It's a red flag for us if clients don't have MFA for remote work."
>
> **Michal Balwiński** | Senior Underwriter and Cyber Practice Leader, Generali Poland

Generali Poland includes YubiKeys with CyberRED contracts, reducing risk of negative events by 50%

Generali Poland is continually re-evaluating risk and working with customers in the fight against cybersecurity attacks. "We want CyberRED to be forward-looking," says Gajkowski. "Risks change and it's important to be dynamic to those changes."

Generali Poland wants to ensure that insured parties see them as a partner, going beyond just policy reminders to provide added value in helping to prevent cyber events. Recognizing that the strength of MFA directly correlates to the risk of cyber attacks, Generali Poland worked with cybersecurity solution group MCX Group and Yubico to include a starter package of ten YubiKey 5 NFC security keys to customers who sign a CyberRED insurance contract. CyberRED customers who choose to expand their YubiKey deployment will be able to take advantage of a discounted rate offered by MCX Group.

"Our cybersecurity team specializes in implementing solutions and services that support the detection, prevention and tailored response to cyber incidents," explains Paweł Olczak, CEO of MCX Pro. "By joining the CyberRED initiative, we have decided to leverage our expertise to provide Generali's clients not only with prevention tools but also with the necessary knowledge to implement MFA solutions in a convenient and effective manner. Utilizing our prepared starter package will effectively reduce the risk of phishing attacks, but we must remember that the threat landscape is much broader. As part of our ongoing collaboration, clients will also receive support from us in understanding current threats and effective risk reduction strategies in the cybersecurity area."

The YubiKey is a convenient and portable hardware security key, providing phishing-resistant multi-factor authentication and offering high-assurance security for both legacy on-premise IT and OT systems as well as modern cloud environments. Supporting multiple protocols including both Smart Card and modern FIDO2/ WebAuthn (passkeys), the Yubikey offers a bridge to passwordless authentication and scalable, future-proofed flexibility.

The YubiKey replaces weak passwords by requiring physical presence to authenticate on any device, through NFC proximity or a USB, making them ideal for logins to shared workstations, for remote work and for automation systems such as ICS SCADA, responding to the 150% global increase in attacks on OT systems that result in costly production outages, equipment damage and the potential for impact to human lives.[6]

> "Strong phishing-resistant MFA will eliminate the easiest and most profitable method for cybercriminals. Strong MFA is the future."
>
> 
>
> **Michal Balwiński** | Senior Underwriter and Cyber Practice Leader | Generali Poland

"The YubiKey addresses one of the main attack vectors," says Gajkowski. "If we want to encourage our customers to think about cyber risk management in general, and specifically cyber hygiene when it comes to passwords, or whether the password is required at all, giving a starter package of YubiKeys is a way to familiarize our customers with this technology."

The goal of the starter pack of ten YubiKeys is to open conversations about cyber risk and to expose customers to a technology they may not know about or may not have had a chance to try yet. "The YubiKey is a key part of risk prevention, in reducing the risk of attack," says Gajkowski, "As we familiarize our customers with technology that can reduce their risk and improve their situation, we also improve ours because we are partners who share the same fate."

With the implementation of just ten YubiKeys, Generali Poland can halve the occurrence of negative events:

> "Even the implementation of these ten keys in sensitive points of an organization is already able to address the risk of phishing in such a way that we can reduce the probability of occurrence of some negative event by up to 50%."
>
> **Michal Balwiński** | Senior Underwriter and Cyber Practice Leader | Generali Poland

After including YubiKeys in its cyber insurance package, CyberRED was named "Innovation of the Month" in November 2023 by Gazeta Ubezpieczeniowa, the Polish Insurance Journal. This award recognizes the "enrichment of insurance protection" offered by a "prevention tool that significantly reduces the risk of a cyber attack."

Generali Poland, Yubico and MCX: A strong cybersecurity partnership

Generali Poland continues to work to meet its customers where they are and to help them on their journey to raise cyber risk awareness and encourage cybersecurity best practices to protect against attacks. The continued innovation in its CyberRED product, and the inclusion of the YubiKey, helps provide organizations with both tools to protect against attacks and insurance to deal with the consequences of attacks.

Generali Poland believes that FIDO2 security keys are a critical solution to help their customers stay secure and to reduce the risk from sophisticated cyber attacks. Further, they recognize that selling cyber insurance begins with expanding discussions about cyber risks and cybersecurity best practices across Polish enterprises and right into the homes of employees.

"We all know from our own experience how burdensome it can be to remember passwords and deal with other forms of MFA," says Gajkowski. "If employees are using their YubiKey at home, they can quickly establish how useful it is for them and help them take a different approach to security for the company they work for."

The partnership between Generali Poland, Yubico and MCX Group isn't just creating a significant reduction in cyber risk for customers—it's also setting a new benchmark for cyber insurance policies worldwide now and into the future.

Learn more | yubi.co/customers | yubi.co/cyberinsurance

Sources

[1] International Trade Administration, Poland ICT the Most Cyber Attacked Country in the World (February 28, 2024)

[2] MIT Technology Review, The Cyber Defense Index 2022/23 (November 15, 2023)

[3] International Trade Administration, Poland ICT the Most Cyber Attacked Country in the World (February 28, 2024)

[4] CERT Polska, The Annual Report from the Actions of CERT Polska 2022

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

[6] Waterfall, 2023 Threat report - OT Cyberattacks with Physical Consequences (May 4, 2023),

yubico