SECUREAUTH
Welcome to Better Identity.

Getting the Most Value out of Cyber Insurance through Best-in-Class IAM Solutions

Contents

OPTIMIZE CYBER INSURANCE INVESTMENTS WITH PASSWORDLESS AND INVISIBLE MFA TO:

- Reduce cyber insurance premiums
- Increase likelihood of getting a binder
- Offer negotiation power for creating a better plan (reducing exclusions)
- Future-proof policies from being rescinded
- Make claims more bulletproof

EXECUTIVE SUMMARY
Is Your Organization Cyber Insurable?

Company boards have spoken: they require their firms to carry substantial cyberinsurance policies to help manage the financial risk of cyber attacks.

It's a sound safeguard and an obvious choice for businesses large and small. As the scale and scope of high-profiles data breaches and cyber attacks mount, and the costs of these breaches and ransomware skyrocket, cybersecurity has now become a major influence to the bottom line.

At the same time, though, cyber insurers are clamping down on coverage. They're increasing premiums, introducing more limits to their payouts, denying claims on existing coverage, and carving out exclusions. For example, while most companies seek cyber coverage specifically to buffer them from ransomware coverage, cyber insurers are making it difficult to insure for ransomware events.

Given the constraints, organizations must act swiftly to ensure that they can remain cyber insurable in a tightened market. They are going to be called to prove that they're invested in a robust set of security controls to show the underwriters and adjustors that they're worthy of a solid cyberinsurance policy.

One of the most frequently called for controls by cyber insurance companies are invisible multi-factor authentication (MFA) and passwordless capabilities. Insurers understand that passwords are notoriously insecure and are low-hanging fruit for hackers. They want their insured to prove they're using superior authentication. Read more to understand the importance of cyber coverage today and the role that invisible, phishing-resistant MFA plays in affordably signing a policy.

State of Cyber Insurance in 2024

Insurance experts agree that the last several years have been tough ones for cyber insurance companies. After a decade of promoting the burgeoning cyber market, these companies are being called to pay the bills as breach and ransomware costs mount. Recent reports show that as a result cyber insurance companies have significantly increased premiums over the last several years.

Not only that, but they're also contracting the coverage they offer and seeking every opportunity to deny claims and rescind policies to firms that don't meet a certain standard for security controls.

> Years of handing out policies like Oprah handing out free cars, followed by an exponential increase in claim frequency and severity, has left insurers in a profitability pickle and diligently seeking to limit their risk exposure.
>
> **–Alla Valente, Forrester Research[1]**

RANSOMWARE AND BREACH COSTS MOUNTING

$30B in ransomware losses expected in 2023[2]

75% of cyber insurance claims are ransomware-related[3]

INSURER LOSSES MOUNTING

12% increase in cyber insurance claims frequency in 2023[4]

42% increase in cyber insurance claims severity in 2023[4]

PREMIUMS ARE INCREASING

67% of companies say their cyber insurance premiums increased 50–100% since their last renewal[5]

86% of firms say premiums increased for same level of service in 2023[6]

COVERAGE IS CONTRACTING

52% of firms said coverage terms grew more restrictive in 2023[7]

ADJUSTORS ARE GROWING TOUGHER

30% of organizations say their cyber insurance policy didn't cover full financial losses sustained by their firm[8]

SECUREAUTH

> Businesses are facing a more demanding underwriting process. Insurers are more thoroughly examining a company's security controls, internal processes, and procedures concerning cyber risk.
>
> **— National Association of Insurance Commissioners (NAIC) report on cyber insurance market**[9]

Cyber Insurance Underwriting Grows Rigorous

Security controls matter more than ever as cyber insurers must financially rationalize their offering and reduce their risk exposure. As a result, organizations should expect a lot more scrutiny from their cyber insurance underwriters in the coming years.

Organizations seeking policies should increasingly expect to see underwriters:

- Deny coverage if bare minimum controls aren't in place
- Tie premiums to the maturity of security controls
- Employ more conditions and limitations on policies based on policyholder security posture and the controls in place when an event occurs.

Underwriters are being pushed by their executives to become more sophisticated about the kinds of controls they ask for and to start questioning the status quo on certain checkbox items.

Evolving Underwriting Will Scrutinize Authentication Security

Authentication Security is one of the most likely places that this evolving underwriting process will continue to focus on in the coming years.

Insurers have already laid down the law about policyholders using single factor authentication. Most insurance carriers won't extend coverage to organizations that don't use MFA throughout their enterprise.

However, given the evolving nature of the underwriting process, don't expect that bottom floor to stay still. Not all MFA technologies are created equally and underwriters have gotten wise to that. There is a reckoning coming where underwriters are increasingly flagging easily exploitable, legacy MFA methods as grounds for higher premiums or non-renewals.

84%

Most underwriters are well aware of the fact that **84% of breaches today are credential-related.**[10]

> Today, MFA is to cyber insurance what sprinkler systems are to commercial property insurance: a must-have.
>
> **—Steve Robinson, national cyber practice leader for the broker Risk Placement Services**[11]

SECUREAUTH

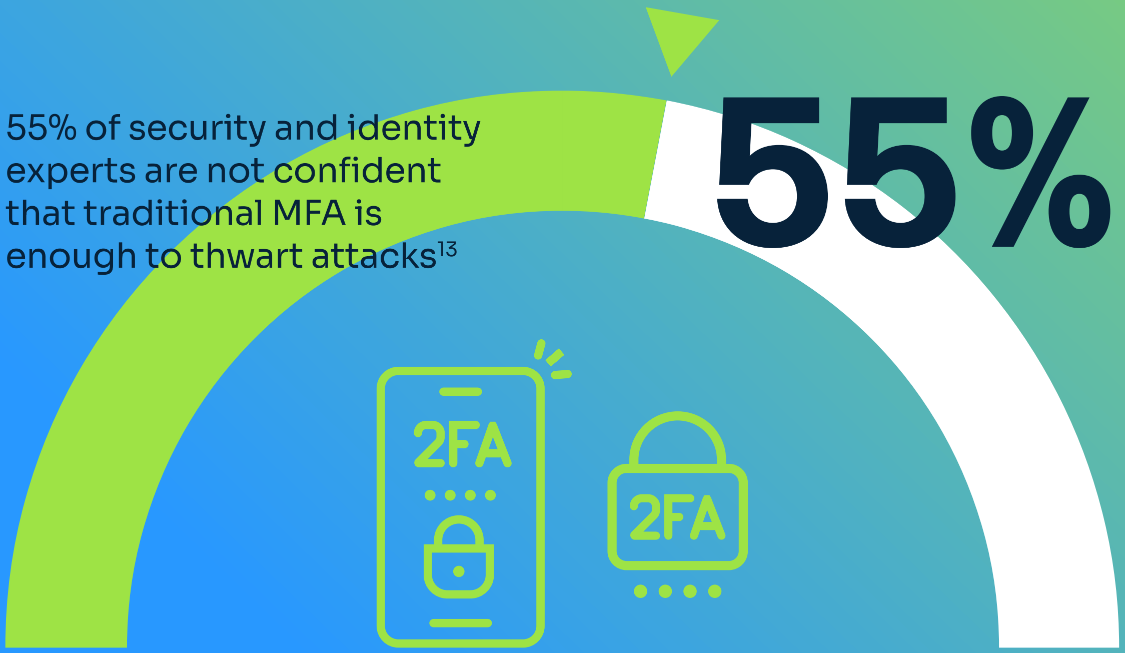
The Insurance Industry's Disillusionment with Traditional MFA

> These technologies are still easily exploitable with 'MFA bombing,' 'man-in-the-middle,' and other attacks. It is time for organizations to move beyond legacy forms of MFAs.
>
> **— Andrew Shikiar, executive director of FIDO Alliance**

As insurers tighten up their underwriting and more rigorously tie it to specific security controls, traditional MFA has come under the microscope. Most insurers think it doesn't reduce the risk exposure enough for them to offer favorable cyber insurance policies to those who use it.

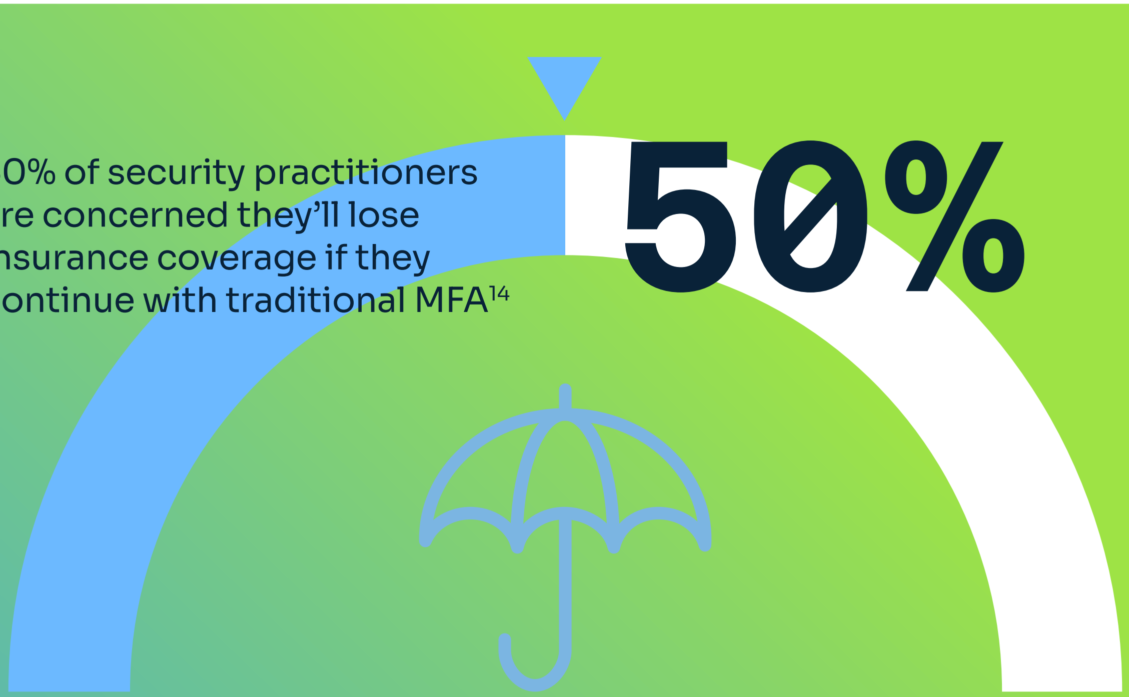
Leading insurers have recognized that legacy MFA technology that authenticates with factors like one-time passwords (OTPs) and personal identification numbers (PINs) are very much susceptible to hacks and phishing attacks. While once-revolutionary decades ago, legacy MFA is increasingly viewed as "better than nothing" in 2024. In other words, better than a password alone but problematic from a security perspective.

This is why top insurance agencies now include strengthened authentication recommendations/requirements in their coverage language. As underwriters keep bolstering their requirements to match these realities, cyber insurance buyers will need to prove they're using next-generation MFA methods that are non-phishable and hack-proof to get the best policy terms. This includes invisible MFA that does risk-based continuous authentication checking with factors and attributes like device trust status and account behavior.



55%

55% of security and identity experts are not confident that traditional MFA is enough to thwart attacks[13]



50%

50% of security practitioners are concerned they'll lose insurance coverage if they continue with traditional MFA[14]

Answering Underwriters' MFA Questions

Most cyber insurance applications today still depend on a self-attestation process that has applicants fill out questionnaires about their existing security controls. These questionnaires have grown lengthier and more technically detailed over the last several years.

Here are some sample questions from underwriters that organizations can expect to answer now, and some potential questions that could start cropping up as they require more robust forms of MFA.

MFA Questions Underwriters Are Asking Now

- Do you enforce MFA for all admin users on your network?
- Do you enforce MFA for ordinary users on your network?
- Do you permit users remote access to web-based email?
- If Yes, do you enforce MFA for access?
- Do you permit ordinary users local admin rights to their devices (laptops)?
- Do you provide your employees with password management software?
- Are you using MFA methods that bypass the use of passwords?

MFA Questions Underwriters Will Soon Ask

- Can you specify the MFA methods that you utilize? Are you using push to text and other non-secure methods?
- Do you use real-time risk scoring to continually authenticate users and accounts?
- Can you secure users post authorization?
- Do you utilize device trust for a more comprehensive security approach?
- What is your MFA adoption rate? Are you getting push-back from users due to MFA fatigue (i.e. too many prompts)?

Here Come MFA-Related Claim Denials Due to Lack of MFA Adoption

Insurance adjustors also play a big role in the reset of today's cyber insurance market. Insurance companies are using MFA failures as grounds for avoiding cyber insurance payouts.

They're increasingly denying claims and rescinding coverage when they investigate incidents and find evidence that policyholders don't have the level of controls claimed in their application for coverage.

As a result, insured companies have to be very careful about their controls to ensure that their attestation claims match reality—lest they risk having a claim denied or severely limited when an incident strikes.

Organizations need to be careful not to misrepresent their use of MFA. For example, only 28% of Microsoft users have MFA and cyber criminals take advantage of this vulnerability as thousands of attacks occur every second on unprotected accounts.

Only 28% of Microsoft users have MFA

TRAVELERS PROPERTY CASUALTY COMPANY VS. INTERNATIONAL CONTROL SERVICES (ICS)

ICS held a cyber insurance policy with Travelers and made a claim for a ransomware attack

ICS told Travelers that it had enterprise-wide MFA during underwriting

Travelers denied coverage when it found that the attacked server lacked MFA

Travelers asked the court to rescind its policy for ICS

The court sided with Travelers

100% MFA Adoption is the only option for cyber insurance optimization

The case of Travelers Property Casualty company against a firm called International Control Services (ICS) offers a striking example of how poorly deployed authentication can threaten security and cyber insurance investments.

ICS bought a policy from Travelers with an application signed by its CEO and its tech people that said it used MFA for administrative and privileged access. Then a ransomware attack hit against an ICS server that had no MFA controls. It turns out the only MFA it used was on its firewall. Travelers successfully appealed to the courts to not only get the claim for that ransomware attack denied but to rescind the whole policy based on “misrepresentations” of the use of MFA.

“It spotlighted the importance of MFA and the reliance on its use by insurance carriers,” National Law Review explained in a recent run-down of the case.[15]

Insurers Now Demand Passwordless Authentication

Nine of the Top 10 cyber insurance agencies have **passwordless recommendations or requirements** so they can provide their customers with:

- The strongest coverage,
- The lowest premiums, and
- No insurance coverage exclusions written into contracts

TOP 10 CYBER INSURANCE COMPANIES IN THE UNITED STATES

RANK	INSURER	DWP	MARKET SHARE
1	CHUBB	$473.1 MILLION	9.8%
2	FAIRFAX FINANCIAL	$436.4 MILLION	9.0%
3	AXA XL	$421.0 MILLION	8.7%
4	TOKIO MARINE HCC	$249.8 MILLION	5.2%
5	AIG	$240.6 MILLION	5.0%
6	TRAVELERS	$232.3 MILLION	4.8%
7	BEAZLEY	$200.9 MILLION	4.2%
8	CNA	$181.4 MILLION	3.8%
9	ARCH INSURANCE	$171.9 MILLION	3.6%
10	AXIS CAPITAL	$159.0 MILLION	3.3%

57%

These 10 agencies make up 57% of the cyber insurance market share

Cyber Insurance Protection Package Example

No matter the protection level, SecureAuth can get you compliant. Whether it's MFA, passwordless, or integration to 3rd party threat services, we've got you covered.

MINIMUM PROTECTION

EMAIL SECURITY

- Email tagging
- Email content and delivery
  - Sender policy framework (SPF) checks
  - Office365 add-ons and configuration

BACKUP AND RECOVERY POLICIES

- Backup key systems and databases

INTERNAL SECURITY

- Deploy and maintain a well-configured and centrally managed antivirus solution
- Limit use of macros
- Patching cadence
- Well-defined and rehearsed incident response process
- Educate your users (phishing training, etc.)
- **Manage access effectively** (i.e. MFA, privileged access)

BASELINE PROTECTION

BACKUP AND RECOVERY POLICIES

- Regular testing of backups
- Disconnect backups from organization's network
- Separately stored, unique backup credentials

INTERNAL SECURITY

- Establish a secure baseline configuration
- Filter web browsing traffic
- Use of protective DNS
- End-point detection and response (EDR) tools
- **Passwordless authentication**

BEST PROTECTION

BACKUP AND RECOVERY POLICIES

- Encrypted Backups

INTERNAL SECURITY

- Comprehensive centralized log monitoring
- **Subscription to external threat intelligence services**
- Network segregation (i.e. via access control or well-configured firewall

How Passwordless Authentication and Invisible MFA Can Optimize Coverage

A healthcare organization reports their investment in invisible MFA as well as passwordless technology helped them reduce premiums and eliminate exclusions.

> We deployed passwordless authentication technology to get a $100 million coverage package with no exclusionary policies. This was a huge for us as most plans include some sort of exclusionary clause.”
>
> **– Chief Compliance Officer**
> **Healthcare Organization**

Before

$100M

COVERAGE PROTECTION

Exclusionary policies included for password-related breaches

After

20% decrease in yearly costs

$100M

COVERAGE PROTECTION

No exclusionary policies included

Dispelling the Magic-Wand Fantasy of Cyber Insurance

A lot of early momentum of cyber insurance has been driven by executives looking for the easy button for reducing cyber risks. For too long now, cyber insurance has been conflated as a replacement for a sound security program that leans on best practice technologies like MFA.

Clearly, the insurance market is rapidly maturing its stance on how and to whom it extends cyber policies. The big picture lesson here is that organizations can no longer afford to engage in the fantasy that their cyber insurance policy is a magic wand for inadequate security controls.

Cyber insurance doesn't wash any policy holder's hands of security responsibility. Insurance is just another layer of risk mitigation.

The faster organizations can come to terms with this lesson, the more rapidly they'll start to reduce cyber risk—not just through an insurance backstop but through sound preventative measures.

Sure, investments in technologies like next-generation MFA and passwordless technologies will serve to provide organizations with more favorable insurance terms. But at the end of the day, the reason insurance companies want their clients to deploy sound authentication is the same reason why executives should want it also: because controls like next-generation MFA and passwordless technologies drastically reduce the chances of a breach!

> "Cybersecurity insurance is not a substitute for effective cybersecurity measures. Rather, it is meant to provide additional protection in case a data breach does occur."
>
> **— Dan Burke, Woodruff Sawyer**[16]

New SEC Ruling: Public Companies Can Be Sued for Lack of Timely Breach Disclosure

A new SEC ruling opens the door to class action lawsuits against any public company if they fail to disclose breaches within 4 days.

Board members and company executives are not immune from such class action lawsuits. Neither the usual D&O liability insurance nor cyber insurance will cover such legal issues. For example, **MGM Resorts is facing a class-action lawsuit** due to their most recent Okta breach (Sep 2023). And their cyber insurance policy has now paid out over $100M. It's assumed their premiums for future coverage will also skyrocket.

This is a huge step forward for consumer rights and will force corporations to properly budget (money and resources) for basic cyber security best practices. These include invisible MFA and passwordless technology powered by a risk-based continuous authentication platform.

Cyber Insurance isn't a panacea for saving companies from financial impact of getting hacked

Why Cyber Insurance is Worth the Effort

So, the last logical question some organizations — especially larger ones — might ask themselves is:

> If I've got invisible MFA and passwordless technology and I've got all of my other security controls deployed, why do I need cyber insurance at all?

While self-insurance might seem like a good option at first, there are a number of considerations that weigh heavily in favor of cyber insurance →

Why Cyber Insurance is Worth the Effort

HIDDEN COSTS OF BREACHES

The indirect costs of breaches—including regulatory fines, reporting requirements, and loss of business—often sneaks up on self-insured companies, causing them to incur huge losses they never estimated on the front end.

DISCOUNTS ON INCIDENT RESPONSE

Most cyber insurance companies have preferred incident response vendors with whom they've negotiated highly discounted rates for policyholders. Self-insured companies pay a much higher rate for these response services.

INSURANCE-SPONSORED CYBER RISK SERVICES

Many insurance companies offer programs that provide services and products, such as risk monitoring, to help their policyholders boost their cybersecurity capabilities and practices.

CUSTOMER AND PARTNER REQUIREMENTS

Third-party risk management departments at a growing number of companies are requiring their vendors and partners to carry cyber insurance in order to get in the door.

SHAREHOLDER DEMANDS

Shareholders and boards of directors are increasingly pressuring their firms to carry cyber insurance as a standard best practice.

Bulletproofing Your Cyber Insurance Investments with Invisible MFA and Passwordless Technologies

Organizations need to plan carefully to ensure their cybersecurity practices are bulletproof in today's maturing cyber insurance market.

We hope this eBook has explained the importance of deploying Invisible MFA and passwordless technologies to help you attain cyber compliance.

SECUREAUTH

About SecureAuth
More security shouldn't equal more obstacles. And, with Identity Management solutions from SecureAuth, leading companies worldwide find it easier than ever to create experiences that are as welcoming as they are secure.

Our AI-driven Risk Engine helps you deliver dynamic – and often invisible – authentication and authorization for your users, combined with a data privacy framework that protects their information and ensures their consent.

It all adds up to a virtual handshake at the digital door to your company. Making you more effective than ever at eliminating bad actors or incorrect authorizations. And giving your employees and customers the seamless and safe access they deserve.

Learn more at www.secureauth.com

SecureAuth. Welcome to Better Identity.