EBOOK

Cyber insurance runs on security.

But is what you have enough?

imprivata®

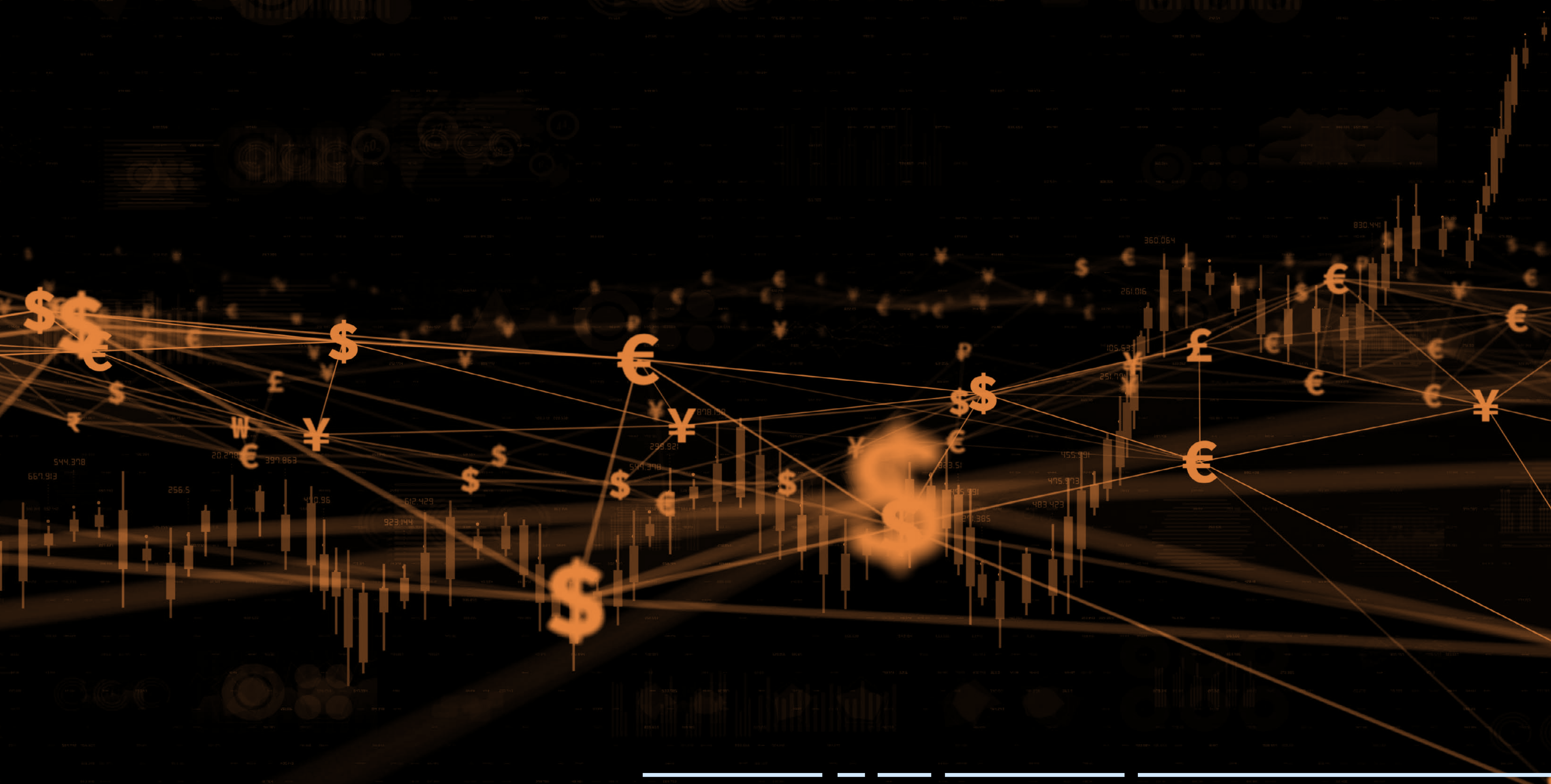
Why you're right to worry about your cyber insurance needs

It's time to talk about the elephant in the room: your cyber insurance needs. With ransomware, phishing, and other cyberattacks continuing to increase in volume, sophistication, and financial impact, you can't afford to ignore them – figuratively and literally. In fact, the average cost of a data breach was more than $4 million in 2022[1]. But damages aren't just financial, either, as your reputation is also on the line.

Cyber insurance exists to help with the costs of data breaches, but cyber insurance providers are responding to the growing threat environment by making some changes. For them, it's about lowering risk. For you? It's getting evermore difficult to qualify for coverage (or even renew your existing coverage). And even when you have it, claims might not be paid in full – or worse, outright denied.

Cyber insurance providers are requiring more comprehensive security controls. Hopefully you have some of the tools in place already, but even then, this is easier said than done. With changing requirements, you can still be left with an entire due diligence process for new technology in months (or weeks!) to guarantee coverage. And competing priorities and an already overburdened IT staff don't make it any easier.

1. Cost of a Data Breach Report 2022 (IBM)



The average cost of a data breach was more than $4 million in 2022.

The evolving – and, frankly, worsening – threat landscape means you need to lower your risk profile.

Why you’re right to want to act *now*

Candidly, the odds of getting hit by a cyberattack aren’t in your favor. In fact, 54% of all organizations experienced a cyberattack in the last 12 months[2]. And there are no real signs that point to that improving any time soon.

That evolving – and, frankly, worsening – threat landscape means you need to lower your risk profile. And starting to do so today – because yesterday isn’t an option – is the only right choice. Because the fact is, without the proper security measures in place, your organization is more at risk. This is true from a pure security perspective and from the perspective of getting, and keeping, cyber insurance.

Cyber insurers are asking to see more comprehensive security solutions because you’re a better risk for them when they can see that you’re doing all you can to prevent needing them at all.

So, if you need to pause here to go re-read your cyber insurance policy – do it. Know what they’ll expect for renewal, and start planning for it now. Otherwise, you might be left scrambling. And at risk.

2. 2022 Ponemon Institute State of Cybersecurity and Third-Party Remote Access Security Report (Ponemon and SecureLink)

No really, don't wait to implement comprehensive security measures

The security of your organization is – and needs to remain – priority number one. And cyber insurers want to see proof that you embody that, because they're seeing the same statistics you are:

- More than 80% of organizations experienced at least one successful phishing attack in 2021[3]
- Ransomware attacks increased 80% from 2021 to 2022[4]
- The use of stolen credentials was the top attack method in more than 40% of breached in 2022[5]

All of that on top of the knowledge that the average cost of a data breach is more than $4 million, and that more than 50% of organizations experienced a cyberattack in the last year.

And as a result, cyber insurance providers have significantly raised their premiums – even just from Q1 of 2022 to Q2 of the same year, premiums went up 79%[6].

The final nail? 27% of data breach insurance claims were not paid due to a policy exclusion[7]. (Really, go re-read that policy!)

3. 2022 State of Phish report (Ponemon and Proofpoint)
4. 2022 ThreatLabz Report (Zscaler)
5. 2022 Data Breach Investigations Report (Verizon)
6. Marsh's Global Insurance Market Index
7. Cyber claim analysis report (Willis Towers Watson)

27%

of data breach insurance claims were not paid due to a policy exclusion.

Cyber insurance isn't a nice-to-have. It's a need-to-have. Which means stringent security requirements are need-to-have, too.

Why security, not just cyber insurance, is a need-to-have

No matter the size of your organization, if you handle personally identifiable information (PII), protected health information (PHI), financial information, or data of any kind, you can be a target. And if you find your organization being targeted, your financial health and reputation is on the line.

So cyber insurance isn’t a nice-to-have. It’s a need-to-have. Which means stringent security requirements are need-to-have, too. And the bonus? With more comprehensive security tools in place, you’re at less risk, anyway. Win-win.

And for those organizations with lean security and IT teams? We can tell you it’s easier to be prepared now than to deal with a cyberattack if it occurs. Tightening budgets and staffing issues make it even more critical to do something now.

But amidst changing requirements for getting – and keeping – cyber insurance, competing security and IT priorities, and the prospect of a potentially rushed timeline to get an implement new technology, the road ahead can still appear daunting.

But it doesn’t have to be. And you don’t have to go it alone – or with dozens of individual solutions, each from a different vendor.

A comprehensive platform to make cyber insurance easy(er)

Single vendor support affords you more time and assurance, as you're not strategizing and collaborating with multiple vendors – there's no passing the buck when you have one trusted, strategic partner, after all! Having a single platform that helps your organization maintain cyber insurance coverage, keep premiums down, and increase the likelihood of a claim payment in the event of a breach really should be your goal. And what you should be looking for is a platform that can deliver:

- Fast, flexible multifactor authentication
- Comprehensive privileged access management, for internal and third-party users
- More secure, stringent password policies and access management
- End-to-end identity governance, complete with provisioning and de-provisioning

The cyber insurance process can be difficult, that's no secret. But finding a single suite of solutions and services that meets stringent requirements doesn't have to be. With the Imprivata digital identity platform, you get more than just a new tool that meets cyber insurers' requirements. You'll also get:

- Support for shared workstations
- Efficient workflows, with badge-tap access to endpoints
- Fast, flexible, and user-friendly multifactor authentication
- An easy-to-implement, cost-effective, and comprehensive suite, from a single vendor
- A full complement of implementation and managed services

Having a single platform that helps your organization maintain cyber insurance coverage, keep premiums down, and increase the likelihood of a claim payment in the event of a breach really should be your goal.

Cyber insurance is increasingly difficult to come by, but you can help keep your organization safe and qualify for cyber insurance by putting security best practices into place.

Start to prepare, now

Cyber insurance is increasingly difficult to come by, but you can help keep your organization safe and qualify for cyber insurance by putting security best practices into place. And, critically, starting to do so now.

You know that the path to cyber insurance starts with security, which is getting harder to maintain. But with the right technology – and the right technology partner – you can be better prepared.

Get started

Now that you know there's a way forward, how do you gain an advantage? Dive into the detailed requirements you'll need for cyber insurance with this checklist.

PREPARE TO MEET CYBER INSURANCE REQUIREMENTS >

imprivata®

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com

CI-EBOOK-cyberinsurace-runs-on-security-0423