EBOOK

Trust in zero trust: Your cybersecurity insurer does

imprivata®

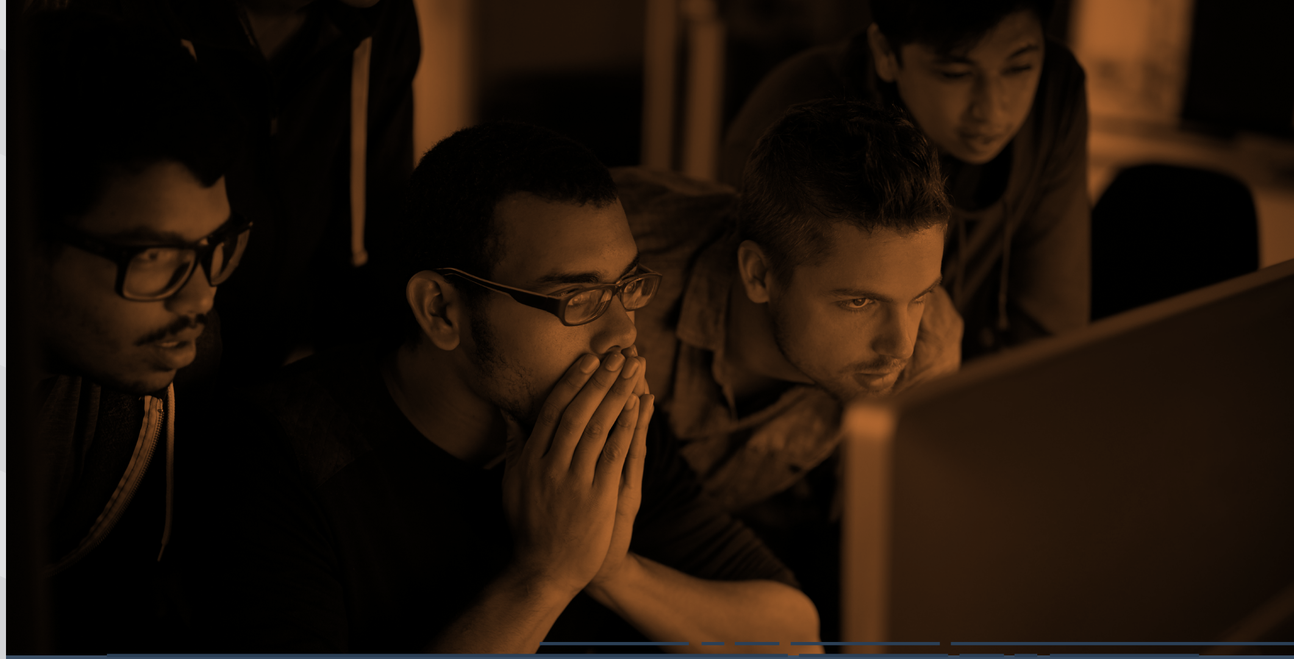
The evolving threat landscape

To tell you something you know already: cyber attacks are on the rise. Over the past five years, the U.S. has experienced over **4,000 ransomware attacks per day**, and in 2020, these attacks cost organizations an estimated $20 billion. That's a **75% increase** over the previous year.

More worrying? There's nothing to suggest any of that will slow down.

Take the emergence of huge numbers of remote workers as a result of the COVID-19 pandemic, for example. The impact of that has been huge – both on the way work gets done and security implications. According to IBM's Data Breach Report 2021, "the average cost was $1.07 million higher in breaches where remote work was a factor in causing the breach, compared to those where remote work was not a factor." What's more, it can actually take longer to identify threats – making containment more difficult.

There are still plenty of stragglers when it comes to adopting cybersecurity precautions, strategies, and solutions, but organizations can't ignore it any longer. Especially because it's a requirement for something that modern enterprises are increasingly having to rely on: cybersecurity insurance.



In 2020, ransomware attacks cost organizations an estimated

$20 billion

Make sure you have security strategies, systems, and protocols in place that limit the possibility you'll need to be covered for anything.

Cybersecurity insurance: The *real* new normal

There's no doubt that cyber insurance plays a critical role in organizations' security strategies. It can help pay for:

- Data recovery
- Fines and judgment
- Identity theft protection and credit monitoring services for customers
- Repairs to hardware and/or software systems
- Lost income as a result of interruption of service
- Ransom payment and extortion costs

More than that: cybersecurity insurance actually promotes security best practices. Want coverage? Make sure you have security strategies, systems, and protocols in place that limit the possibility you'll need to be covered for anything.

But all of that comes at a cost – and we mean that literally.

Rising insurance premiums, reduced coverage, stringent requirements, oh my!

Cybersecurity insurance is hard to come by, that's not a secret. And yet cybersecurity insurance is a must-have for modern enterprises who work in a digital world. So taken together, what does that mean? Increased premiums, increasingly stringent requirements, and, in some cases, cancelled or outright denied policies.

Cybersecurity insurance rates have **increased across all industries by about 32%** in the past year, while, over the past four years, **the average growth of claims has been about 39%**. But according to the Council of Insurance Agents and Brokers (CIAB), **poor risk management protocols and lack of employee training** are often to blame for increased premiums.

That's where the more stringent requirements come in.

Many leading cyber insurance providers now require documented evidence, as well as a formal assessment, of an organization's information access security strategy so that they can measure an organization's risk management preparedness, processes, controls, and tools.

And that's all prior to deciding whether they'll grant coverage or not. That's right, *whether* they will.

According to the Council of Insurance Agents and Brokers (CIAB), poor risk management protocols and lack of employee training are often to blame for increased premiums.

61%

of all breaches exploited credential data via brute force attacks, credential stuffing attacks, or credential data leaked and used later.

Get covered* and strengthen your security posture

Noticed that asterisk, did you? Well, if it were that simple, the coverage probably wouldn't actually offer you anything you needed. But, to get – or maintain – coverage, you need to strengthen your cybersecurity posture.

One place to start: securing those credentials.

According to Verizon's **2021 Data Breach Incident Report**, 61% of all breaches exploited credential data via brute force attacks, credential stuffing attacks, or credential data leaked and used later.

And those credentials that were exploited? Tied to individual digital identities. At their core, many breaches are attacks on identity – so securing those identities is paramount. Adopting an identity-centric zero trust approach can help you do that.

And there's more good news: a zero-trust approach can help you secure coverage *and* secure your organization.

Zero trust and identity management

Zero trust is an architectural approach where inherent trust in the network is removed: everything and everyone on the network must be authorized and authenticated in order to gain access, which helps to ensure that the right individuals are accessing the right resources at the right time and for the right reasons. An architecture like this encompasses:

- Identity management
- Authentication
- Access management
- Continuous monitoring

And there's some really good news (yes, even more than securing cybersecurity insurance coverage and keeping your organization secure!): **a zero trust approach can reduce costs** associated with breaches. In fact, breaches are 42.3% costlier without zero trust. Really.

Breaches are

42.3% costlier

without zero trust

Whether or not you're actively involved in procuring or extending your cybersecurity insurance coverage, a zero trust strategy can help keep your organization safe and secure.

A brief intermission

Before the lights start to flicker and we go back to our seats, just a reminder that an identity-centric zero trust strategy is a security best practice. The solutions that come together *to create* a robust zero trust strategy are security best practices.

We're talking about cybersecurity insurance, here. But really, what needs to be underscored is this: the security of your organization is already top of mind, and – whether or not you're actively involved in procuring or extending your cybersecurity insurance coverage – a zero trust strategy can help keep your organization safe and secure.

Zero trust in practice

So, zero trust sounds nice, but how do you get started? Rooted in identity and access management (IAM), zero trust creates checkpoints, requiring authorization and authentication, at the access point of applications containing sensitive data.

A robust IAM solution will include the following capabilities:

- Identity governance, with lifecycle provisioning and de-provisioning
- Multifactor authentication
- Single sign-on (SSO)
- Privileged access management (PAM)

With those foundational pieces in place, securing your sensitive data and systems becomes a lot simpler.

Zero trust creates checkpoints, requiring authorization and authentication, at the access point of applications containing sensitive data

The security of your organization is your number one priority. And cybersecurity insurers expect it to be.

Where to start, and how to help cybersecurity insurers help you

No matter what your other business goals are, the security of your organization is your number one priority. And cybersecurity insurers expect it to be. By implementing identity governance, multifactor authentication, SSO, and PAM solutions, you can help bolster the security of your enterprise and prove to insurers that you already have proactive security strategies and systems in place.

Obviously, setting up those solutions also costs money – and labor, and potentially tedious conversations, and more. That's also no secret. But investing in solutions that keep your organization, your data, and your customers' data safe and secure is a good investment for the future. And by partnering with the right technology providers, you'll be able to see fast time-to-value and tangible ROI.

Oh, and yes, lower those insurance premiums.

Your next step

Now that you know how difficult it is to get covered, how do you gain an advantage? Dive into the detailed requirements you'll need for cyber insurance – and solutions for them – by checking out this datasheet.

MEET CYBER INSURANCE REQUIREMENTS >

imprivata®

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

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

CI-ebook-trust-in-zero-trust-0122