Delinea

Cyber Insurance – If you get it, be ready to use it

Everything you need to know

WHITEPAPER

Executive Summary

The proliferation of cyberattacks in 2020 and 2021 were a shock to the cyber insurance industry. Claims frequency and severity skyrocketed, and losses often far exceeded actuarial limits.

Demand for cyber insurance continues to increase as more companies try to offset their risk. Meanwhile, insurers are recoiling from overexposure; it's been widely reported that carriers are raising rates and requirements.

In this environment of uncertainty and change, Delinea wanted to understand the real-life experiences of companies which have obtained and used cyber insurance. We surveyed over 300 IT security professionals from across the United States to see what types of challenges they've experienced, and how they've put their cyber insurance to use.

Among the findings, three key takeaways stood out.

1. **What the Board wants, the Board gets.**
   Cyber insurance has become ubiquitous, driven by requirements from the Board of Directors. Almost 70% are currently investing in insurance, with 93% receiving it when they apply.

2. **Your policy will get a workout, but it may not cover what you need.**
   Almost 80% of respondents have used their cyber insurance policy. Half of those have used it multiple times. But the devil is in the details. Over 50% of survey respondents say their policies don't cover costs related to data recovery, ransomware, and more.

3. **Policy requirements try but fail to prevent attacks.**
   To contain risk, insurers are mandating that policy holders have core security tools and practices in place. So, why are nearly 80% of companies still experiencing cyber events that require insurance? Clearly, checking the policy requirements boxes isn't enough to keep organizations safe.

How to use this report

The results of the survey and expert analysis can help you prepare for applying, obtaining, and renewing cyber insurance, with coverage and rates that accurately reflect your risk profile.

See how you stack up and where to go from there.

Introduction

No matter how many security controls and technology solutions you have in place, you can never eliminate risk. The question isn't whether a cyberattack is going to happen. The real question is: Can you mitigate the effects and get back to normal operations as quickly as possible when it does?

The average cost of a data breach increased 2.6% from $4.24 million in 2021 to $4.35 million in 2022. This was on top of a 12.7% rise from $3.86 million in 2020.[i]

The role of cyber insurance is to offset those costs, so that even if your best efforts to safeguard your organization fail, you can maintain business continuity. Cyber insurance policies cover costs related to damages and recovery after a data breach, ransomware attack, or other cybersecurity incident. They can also shield you from the costs of investigations, forensics, compliance fines, lawsuits, and even extortion payments.

However, after several tumultuous years, that safety net is in question.

Despite increasing demand, the insurance sector is making it more difficult for companies to get coverage. Underwriting questions have become more detailed and strategic to try and reflect more accurate cyber exposure.

Carriers are raising premiums – some by 300% at renewal – and lowering coverage, particularly for sectors often targets for ransomware, such as education, public entity/government, healthcare, construction, and manufacturing, according to the *U.S. Cyber Insurance Market Outlook* report from RPS. Insurers that were willing to issue $5 million cyber liabilities policies in 2020 now set limits of $1-3 million, even on renewals, RPS reports.[ii]

Cyber insurers struggle to fit a round peg in a square hole

For many years the insurance industry has been looking to get into new markets. Focusing on cyber seemed like a great opportunity to expand their services. Little did they know, cyber risk was a lot more complicated than their models were prepared for.

Early cyber insurance policies only protected against physical asset damage such as hardware and network infrastructure, not the data and loss of revenue for the business resulting from service downtime. The tangible cost to the business resulting from a cyber incident was somewhat easy to measure when tied to physical assets. Trying to determine the value of data is much more complicated, especially as the value and volume of data which organizations collect and process has significantly increased.

Today, many insurance companies have evolved and matured their cyber insurance policies to cover many of the risks to the business from cyberattacks such as ransomware, data theft, business downtime, and even revenue loss. But not all.

Beyond the cost involved, adding more insurance doesn't solve the root problem of securing your organization.

The data in this report shows that companies need to go beyond the check-the-box exercise of obtaining insurance. For some, insurance requirements may not be enough to cover their greatest risks and offer a false sense of security.

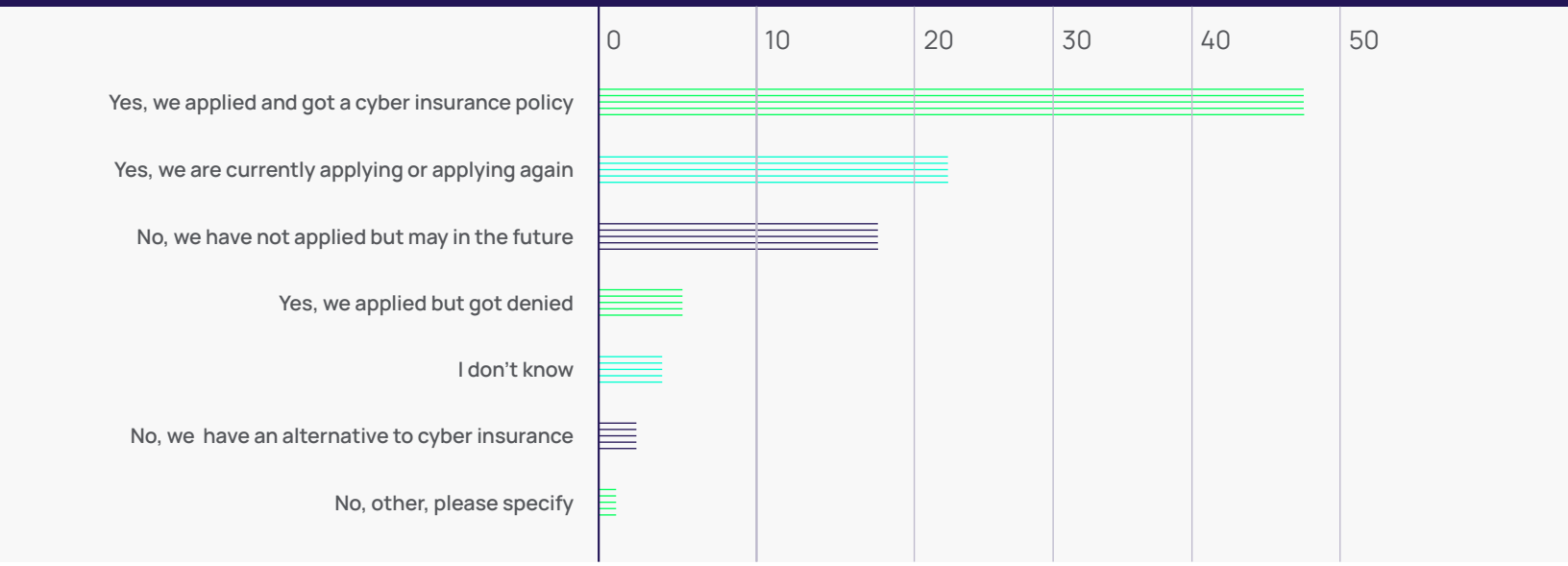
Dig into the details to make sure you have everything you need to safeguard your organization.

TAKEAWAY 1:
What the Board wants, the Board gets

Cyber insurance is on the mind of almost all survey respondents.

Almost 70% of companies already have cyber insurance or are in the process of obtaining it. Just under 20% are considering cyber insurance for the future.

Q1 Has your company applied for or are you considering applying for cyber insurance?

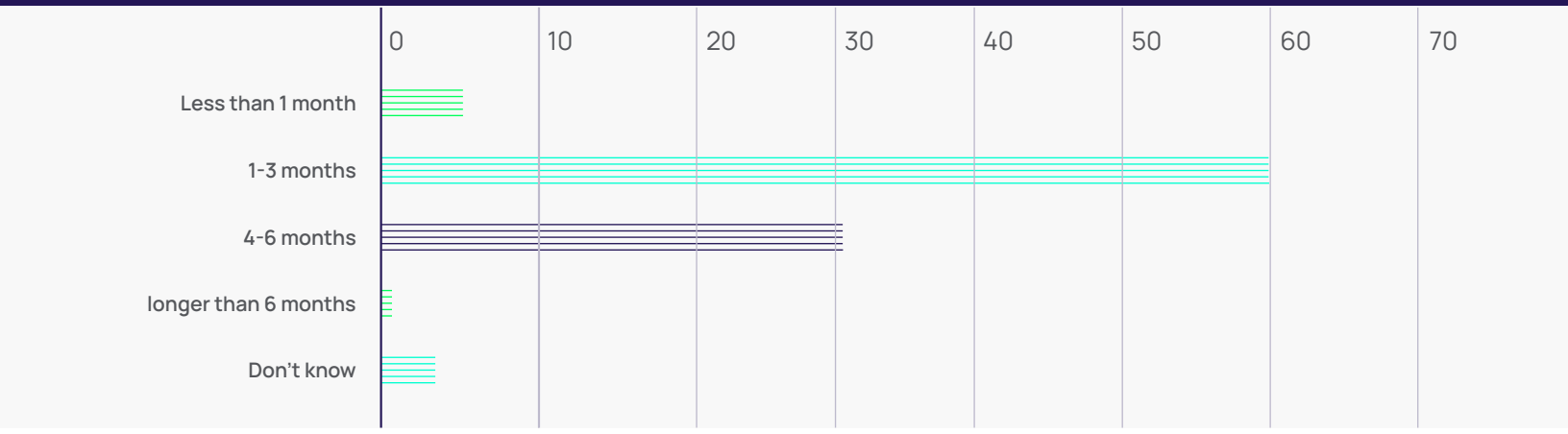


The good news for companies is that our research indicates that those who seek to obtain cyber insurance will receive it. Only 7% of survey respondents who applied for insurance were denied.

Clearly, insurers still want the business, even if the increased risk might not be sustainable long term.

In fact, the process to obtain insurance is relatively fast. Most companies were able to get a policy in place in under three months.

Q2 How long did the process take you, or do you anticipate it will take you to obtain your cyber insurance?



Boards of Directors are a key driver of insurance demand

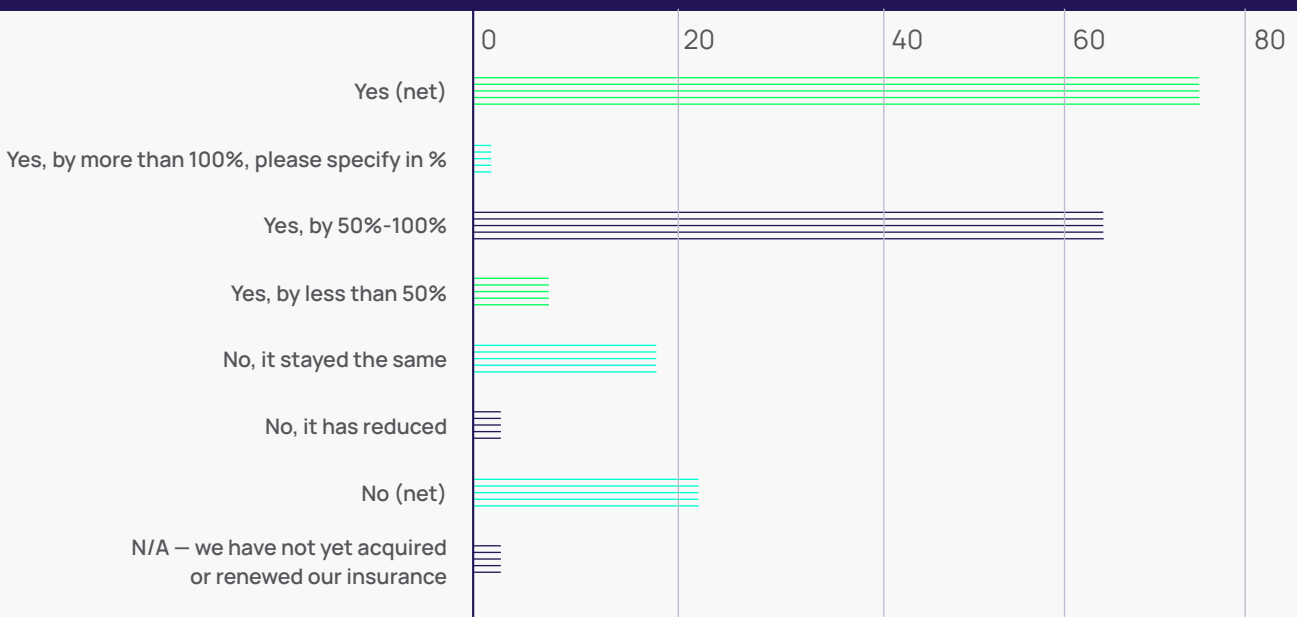
The research indicates that Executive Management and Boards of Directors are a main driver of the increase in demand for cyber insurance. 33% of respondents said the main reason they applied for cyber insurance is due to an Executive Management/Board requirement. If you aren't already in the process of getting cyber insurance, you should expect a call from the Board soon, asking you to get going.

Q3 What is your main reason for applying for cyber insurance?

With the Board behind them, companies are finding the budget for insurance

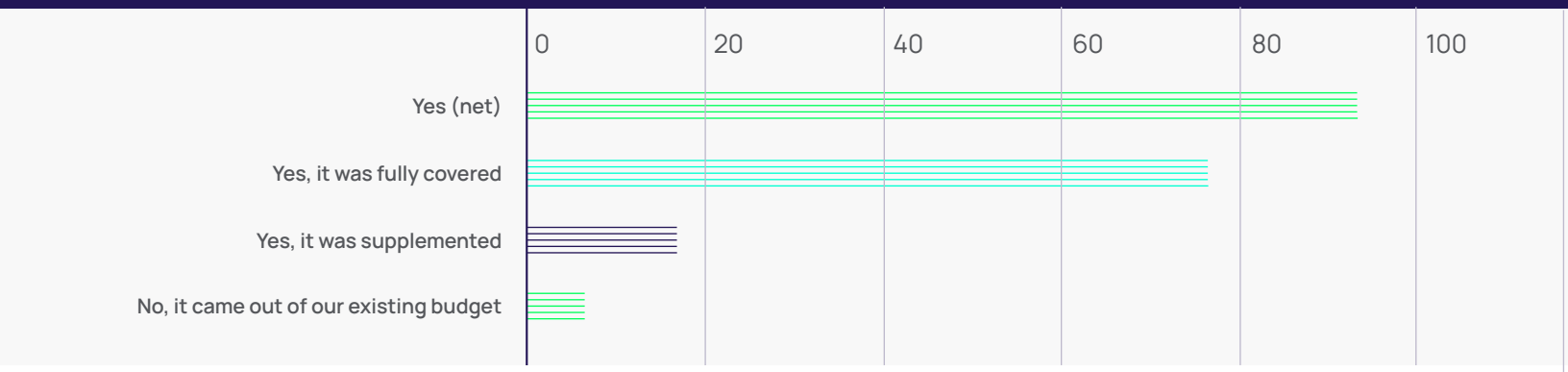
As expected, survey respondents are experiencing rising insurance costs. 75% reported that cyber insurance costs have increased since their last renewal, with 65% of those respondents indicating the increase was by 50-100%.

Q4 Have your cyber insurance costs increased in your last renewal?



Despite the increase, companies are finding the budget to pay insurers. Almost 95% of respondents got the budget needed to obtain cyber insurance and three out of four (76%) had it fully covered.

Q5 Were you allocated additional budget in order to meet insurance requirements?



This suggests IT and security leaders who struggle to get the budget for hiring experts and purchasing technology can leverage the Board's interest in cyber insurance to obtain needed resources.

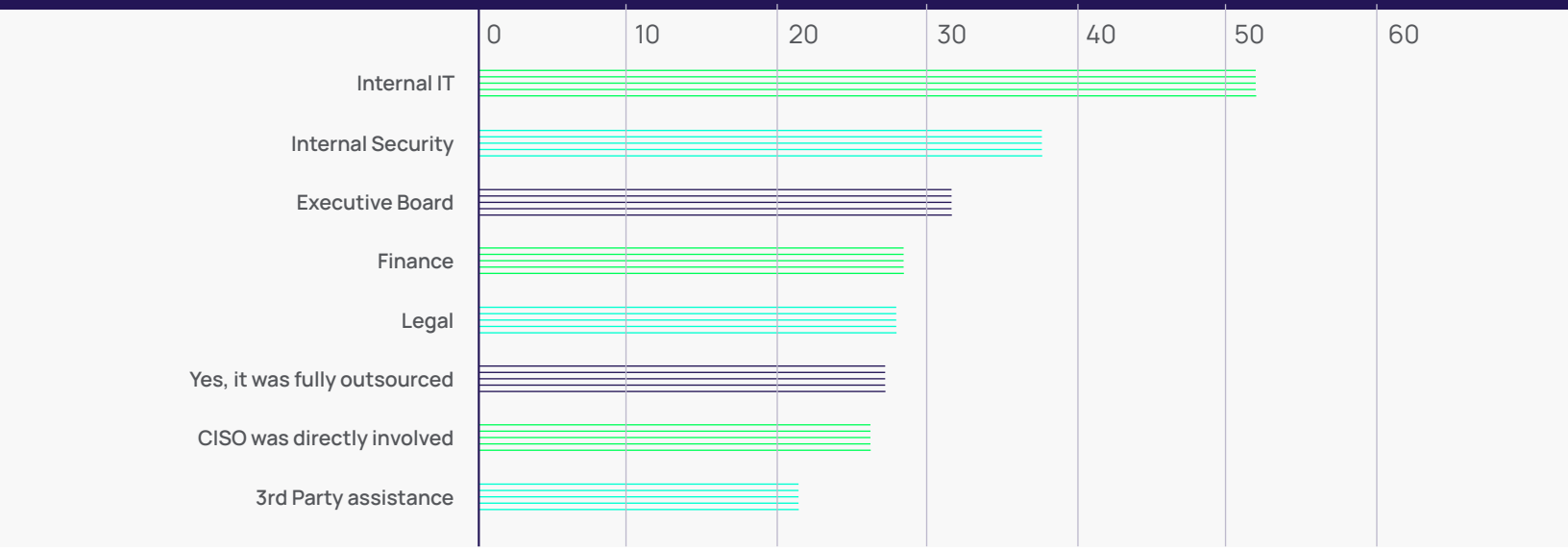
A cross-functional team supports the cyber insurance process

Let's say the mandate has come down from your Executive Management team or Board of Directors to get cyber insurance in place. Who picks up the ball and is responsible to get it done?

The research shows that multiple teams and functions will need to be involved in the process. Unlike general liability insurance, which may be handled directly by the finance or risk teams, cyber insurance also requires the skills and support from the IT and security groups. It's likely that you'll be asked to produce evidence of your security controls and share your ongoing strategies to reduce risk.

More than 50% of companies used internal IT resources when getting cyber insurance, and just under 40% involved the security team.

Q6 What assistance, if any, was/is required in obtaining your cyber insurance policy?



Why Boards of Directors care about cyber insurance

The Board's responsibility is to make sure that the Executive Management team has a plan, is prepared, and is hardening the whole organization for the eventuality of an attack.

Most Board members aren't cyber experts, but they are expected to understand a company's financial exposure to cyber risk.

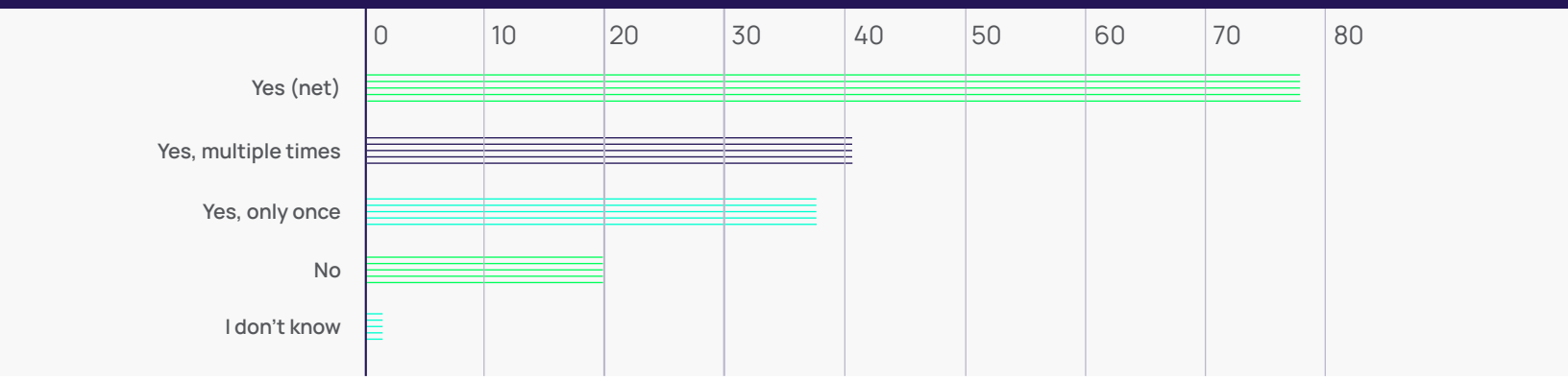
The Securities and Exchange Commission (SEC) advises companies to disclose in their proxy statement the Board's role and engagement in cyber risk oversight. If a data breach or cyberattack occurs, directors will be under scrutiny. They can be held personally liable if their actions are found to breach their fiduciary duty to the company and shareholders.

TAKEAWAY 2:
Your policy will get a workout, but it may not cover what you need

If you're successful in obtaining a cyber insurance policy, it's very likely that you will need to use it.

Almost 80% of respondents have used their cyber insurance policy. Furthermore, over half of those have used it multiple times.

Q7 Has your organization ever used cyber insurance due to a security breach or incident?



Unfortunately, you have less than a 50% chance that your costs will be covered.

One of the reasons insurance companies are so willing to grant policies – and so quickly – may be that they are pulling back on their coverage, finding more reasons to limit coverage or eligibility.

Less than 50% of respondents say their current cyber insurance policies cover data recovery. What's more, 60% or more don't cover common costs such as victim identity and credit monitoring, costs, incident response, hardware and software replacement, regulatory fines, and third-party damage

Ransomware payment coverage is far from a guarantee; 70% say their policies won't cover it.

There's a slim chance that future profit loss will be covered; only 27% are willing to cover that.

Q8 What does/would your cyber insurance policy cover?

With these scenarios in mind, check your policy carefully. See if it will cover losses due to ransomware, lost equipment, third-party actions, and human error.

Requirements for ransomware response

Control over ransomware payouts is a hot topic. Many companies worry that insurance companies have too much influence over ransomware response. Based on the data in this survey, some carriers want to be involved in the decision whether to pay the ransom.

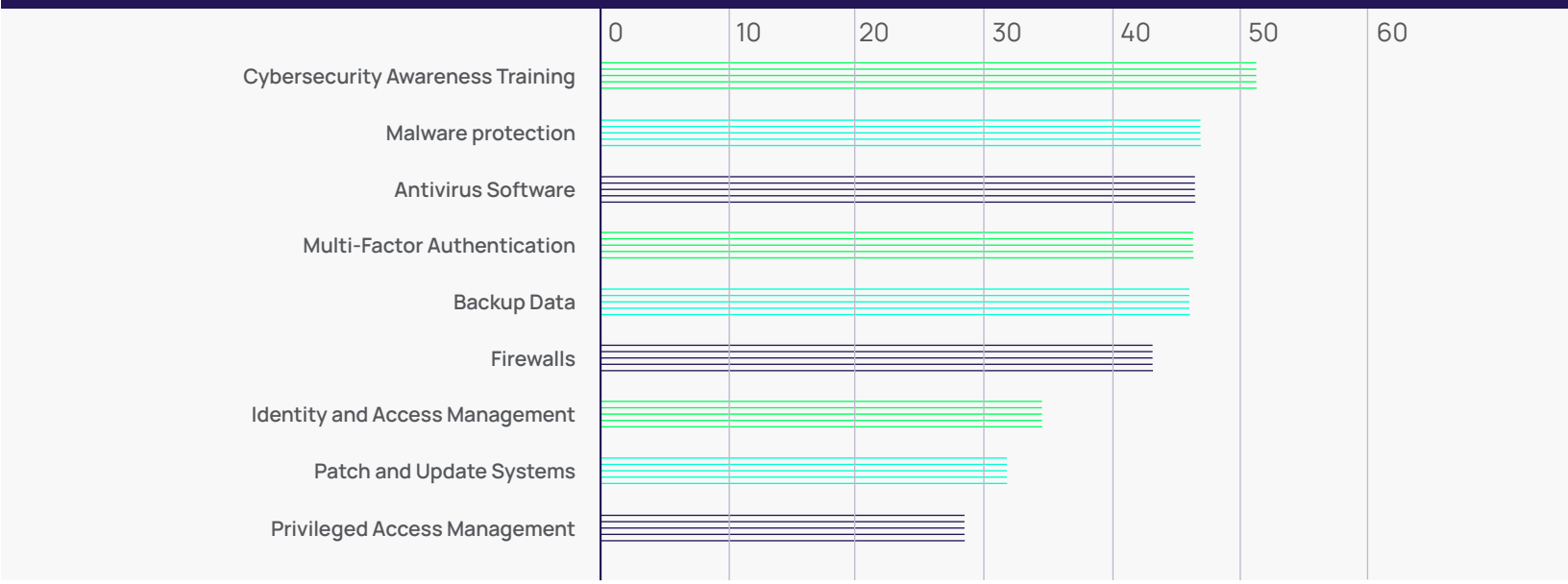
Some organizations are also discovering that their policy requires them to inform the insurance company of a ransomware attack prior to anyone else, including incident response teams and law enforcement.

TAKEAWAY 3:
Policy requirements try but fail to prevent attacks

Many insurance companies are trying to get a clearer picture of risk and insert policy requirements to reduce it.

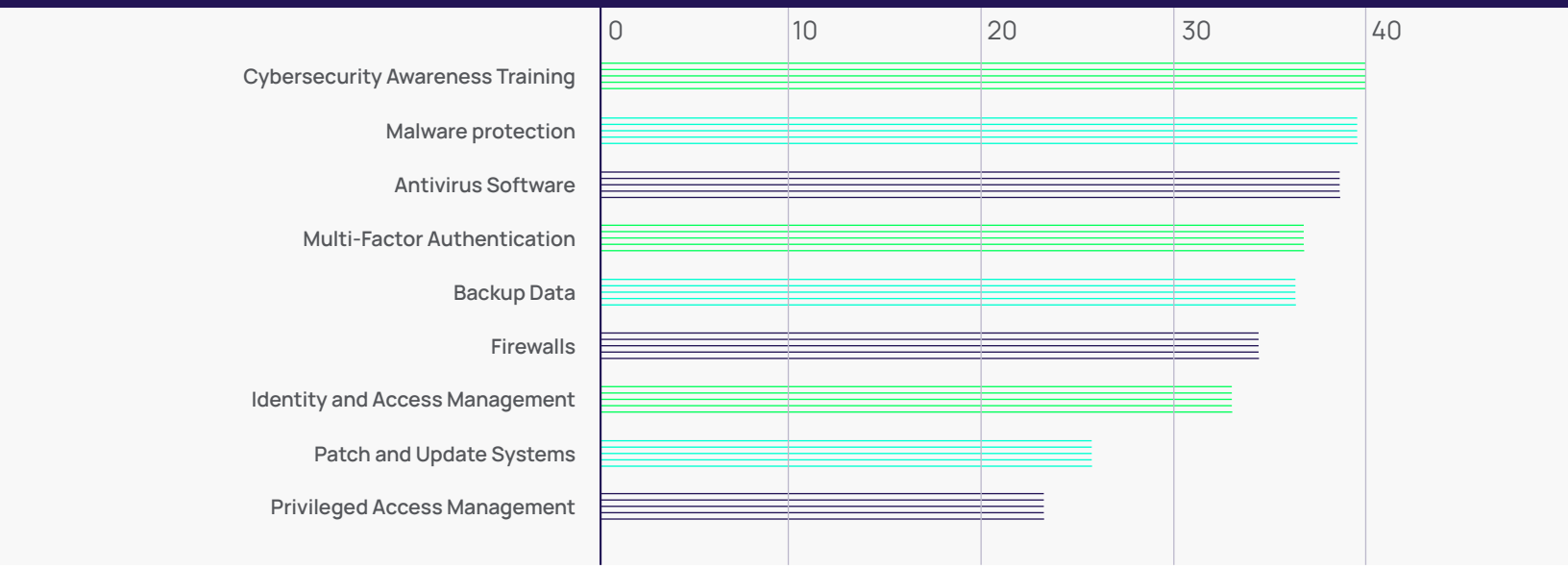
Cybersecurity awareness training tops the list of cyber insurance demands, with over 50% of policies requiring employees to be trained. Just under 50% of policies require malware protection, antivirus software, Multi-Factor Authentication (MFA) and a backup strategy.

Q9 What security requirements did/does your insurance policy require?



Survey respondents say they had to invest in a variety of technology purchases and security practices to meet the demands of their insurance providers.

Q10 Did you have to purchase any of these to fulfill your requirements?



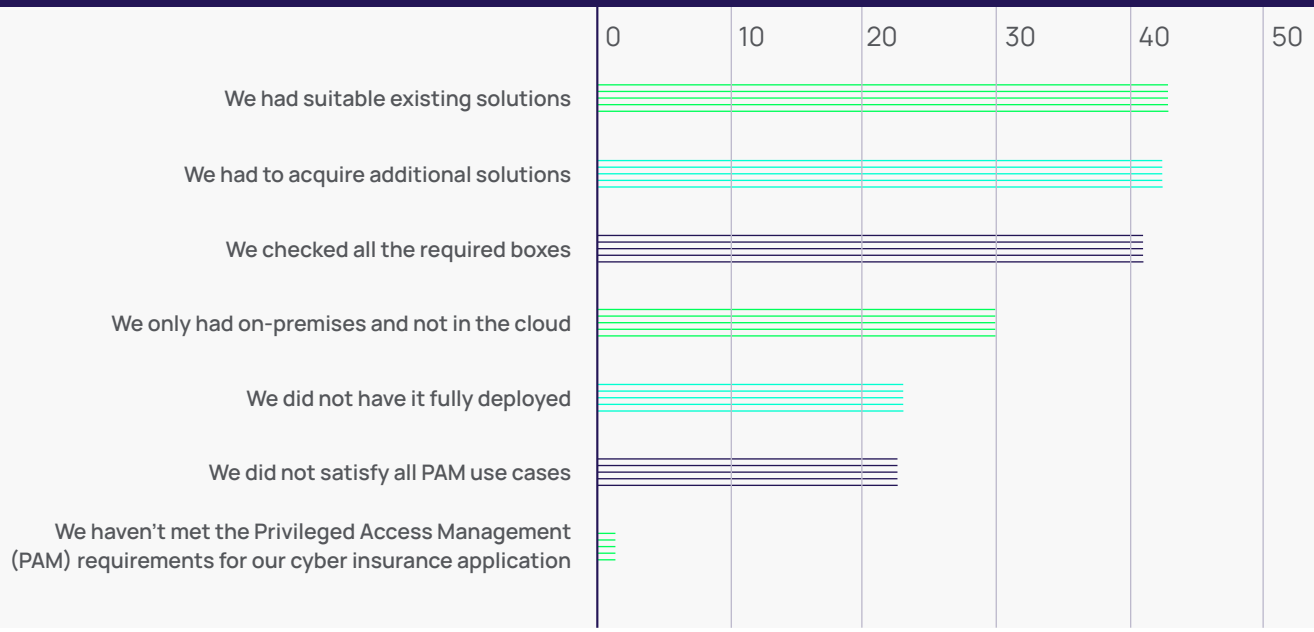
With these requirements in place, why are nearly 80% of companies still experiencing cyber events that require insurance?

It's clear that having a cyber insurance policy in place may not be sufficient to meet your need for cyber resilience and business continuity.

Not all cyber insurance practices are equal. Some require a simple self-assessment approach. Others require an in-depth assessment to confirm that security tools and practices are indeed in place and functioning as intended. It's possible that companies aren't maintaining the security controls they claim to have, or aren't using them to their fullest potential.

For example, it appears that only 29% of cyber insurance policies require Privileged Access Management (PAM), a critical strategy to prevent and contain one of the most common techniques used by cybercriminals. While policies more frequently require Multi-Factor Authentication, which attempts to confirm user identities, without PAM companies still run the risk that a criminal with a stolen credential could masquerade as a verified user. PAM policies that limit access are needed to contain the damage.

Q11 How, if at all, did you meet the Privileged Access Management (PAM) requirements for your cyber insurance application?



Just over 40% of organizations had an existing PAM solution in place that satisfied the cyber insurance policy. A similar percentage needed to purchase additional solutions to meet the cyber insurance demands.

When purchasing solutions to meet cyber insurance requirements, it's important to differentiate between a basic password management vault and an enterprise solution like Privileged Access Management. While a vault is an excellent way to keep passwords and other secrets secure, Privileged Access Management offers additional functionality to establish access levels for privileged users and monitor privileged behavior. PAM allows you to provide just-in-time, just-enough access so you can avoid risky practices like standing access that leave the door open for cyberattacks.

Conclusion

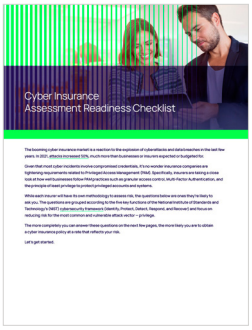
If you don't already have cyber insurance, prepare to get it. The Board is sure to ask, and probably soon. Get your ducks in a row now so you can quickly provide evidence of security strategies, controls, and technologies to complete cyber insurance questionnaires. The more prepared you are, the faster you'll obtain insurance, and the lower your rates are likely to be.

While cyber insurance will provide some level of comfort, based on the survey results it's likely not enough to offset the cost of many cyber incidents.

Filling out an insurance checklist is not the goal; it's one step toward securing the future of your organization. Also make sure you're choosing security tools wisely and using them to the fullest. Monitor and audit your security controls to be sure they're working as you expect.

In today's world, cyberattacks are inevitable. Reduce your risk as much as possible and prepare your organization to respond before an attack becomes a cyber catastrophe.

Additional resources: learn more about cyber insurance



FREE TOOL: Delinea's Cyber Insurance Readiness Checklist

This sample cybersecurity insurance checklist guides you through the top questions most insurance companies ask when you apply for cyber insurance, such as:

- ☐ **How you address cybersecurity risks, such as unmanaged privileged accounts**
- ☐ **How well you manage access to critical, sensitive assets**
- ☐ **Your ability to detect unexpected or suspicious credential use**
- ☐ **Your incident response plans in case of a cyberattack**

Get the checklist

EBOOK: Conversational Geek's Quick Guide to Cyber Insurance

Conversational Geek's quick guide to cyber insurance breaks down the choices and the process for obtaining cyber insurance. It includes expert guidance from cyber insurance brokers, using plain language helpful for folks new to the insurance process.

Inside, you'll learn:

- How to read a cyber insurance policy quote to understand coverage categories and key information such as limits and exclusions
- Questions insurers are sure to ask that influence your rates
- How to prepare before applying for cyber insurance or renewing your policy

Get the guide

BLOG: Cyber Insurance – What Is It and Why Do You Need it?

Before you seek cyber liability coverage or negotiate your next insurance policy renewal, it's important to understand the dynamics of the rapidly changing market and consider how well your security controls will stand up to an insurance company's review.

This Delinea blog answers some common questions about cybersecurity insurance and make sure you get all the facts you need.

Read more

BLOG: A Tale of Two Cyber Insurance Customers

Two companies tell their story of reducing risks related to cloud migration with cyber insurance.

Read more

PODCAST: The Intensification of Cyber Insurance

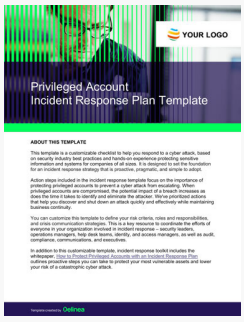
Chief Data Scientist Ann Irvine and VP, Cyber Underwriting Kevin McGowan of Resilience join Delinea's Joseph Carson to provide the latest on cyber insurance.

Listen to the podcast

PODCAST: Cyber Insurance with the Experts

Delinea's Joseph Carson talks with the folks at Resilience Insurance - Michael Phillips, Head of Claims, and Kevin McGowan, VP of Cyber Underwriting.

Listen to the podcast



FREE TOOL: Delinea Incident Response Template

Prevent a cyberattack from turning into a cyber catastrophe. With your incident response plan documented and tested, you can respond swiftly and effectively when a cyberattack occurs. This customizable toolkit helps you prepare a rapid, coordinated response.

Claim your free tool

About the report:

Censuswide, on behalf of Delinea, surveyed 301 IT decision makers in the U.S. during August and September 2022.

---

i. https://www.Ibm.Com/security/data-breach

ii. https://www.Insurancebusinessmag.com/us/news/cyber/cyber-insurers-hiking-premiums-lowering-coverage-limits-report-312738.aspx

Delinea

Defining the boundaries of access

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**