# CISO Playbook:

## 5 Winning Strategies for Cost Optimization



CybelAngel | CYBERSECURITY DIVE

Custom content for CybelAngel by studioID

# INTRODUCTION

Over the last few years, the growing digital economy has created seemingly endless opportunities for businesses — and cyberattackers. By 2025, the annual global cost of cyber attacks is predicted to reach **$10.5 trillion**.[1]

Organizations across industries have consistently increased their cybersecurity spending by 5-10% every year in response to growing cyberthreats.[2] However, in a down turn economy, ever-increasing cybersecurity budgets aren't sustainable.

Today organizations are bracing for potential cyberattacks while also anticipating a global recession, supply chain bottlenecks and dealing with high inflation. Chief information security officers (CISOs) are stuck between a rock and a hard place, facing a growing number of dynamic cybersecurity threats, rising cybersecurity insurance premiums, increasing regulations, and a talent shortage — all the while managing costs.

There are a few things companies can do to get ahead of managing cybersecurity costs in a down turn economy. By utilising the 5 winning strategies in this playbook, organizations can begin optimizing investments in cybersecurity to see tangible results — and returns.

# SOLVING CYBERSECURITY CHALLENGES AND MANAGING COSTS FOR CISOS

Organizations are making increasingly rigorous demands on their CISOs and cybersecurity teams. The CISO position is arguably the most complicated in the C-suite, and the speed of digital transformation as well as the frequency and severity of dynamic cyberthreats often outpace its evolution.[3]

Many organizations are adding the task of managing cybersecurity costs to an ever-growing list of responsibilities. For CISOs, identifying and optimizing resources means developing a big-picture plan to help reduce costs, grow revenue, and stay ahead of emerging threats.

# ⊗ The Challenge:
## Cybersecurity is too reactive in its approach

While **proactive cybersecurity** is about anticipating future incidents and taking action to prevent them, **reactive cybersecurity** is about responding to incidents after they occur. Both approaches are critical, but many companies today simply don't have enough proactive cybersecurity measures in place. It's ironic — a CISO is continually monitoring and preventing attacks but it remains an uphill battle to convince the organization to continue investing in security. Then, shortly after a high-profile attack, the budget materializes for remediation and it's generally far more expensive than the preventive measures would have been.

In 2022, it took an average of **277 days** to identify and contain a data breach.[4] For every potential data leak or breach waiting to happen, it takes 277 days for a company to realize they're either leaking information or exposing a vulnerability. That is a lengthy and golden opportunity for a bad actor or nation-state hacker to find a weakness and attack or monetize it.

With the average data breach costing **$4.35 million**[5], a proactive cybersecurity approach to reduce the devastating costs of these incidents can save your company millions.



The average data breach costs
**$4.35M.**



The average data breach takes
**277 DAYS**
to identify and contain.

# Our Solution:
## Adopt a proactive approach

Significantly reducing the time it takes for an organization to detect and respond to a security incident can save wasted resources, but proactively identifying vulnerabilities can help stop incidents *before* they occur. This means identifying and neutralizing threats early, before they pose a real threat. Whether an employee makes a preventable mistake, a third party vendor unknowingly shares sensitive information, or a bad actor conducts reconnaissance in preparation for a cyberattack, advanced visibility into these areas will proactively prevent serious incidents. It will also protect organizations from major financial, legal and reputational repercussions.

**CybelAngel helps you to adopt a proactive response with our three key pillars:**

1. Adopt full visibility on your extended external attack surface with a 24/7 scan of the internet with over 6 billion data points processed daily.

2. Prioritize the most business-critical exposures with contextualized incident reports that confirm issues, all redacted by your dedicated cyber analyst.

3. Get set for action with streamlined and fast remediation to reduce your takedown time by 85%[6].

## ⊗ The Challenge:

# Cybersecurity is overly focused on internal security not external threats.

Most cybersecurity companies focus on defending what's inside an organization's walls, but **internal threats currently account for around 22% of security incidents.**[7] Internal threats relate to the cybersecurity risks that stem from inside an organization to exploit systems or cause damage. In most cases, insider threats result from negligence.

External threats are harder to deal with because organizations have little-to-no control outside their perimeter. Securing companies against malicious threat actors, third parties, software vulnerabilities, and personal devices is complex but equally important in preventing security incidents.



## Our Solution:

# Monitor external threats to preemptively neutralize them

Understanding the perspective of an outside threat actor primed for attack is an often underutilized best practice among organizations. The traditional approach to security is a fully defensive play. This can involve locking all the "doors" and "windows," putting up walls, and waiting for someone to attack. If an organization detects intruders, they fence them off to limit the damages.

This approach to cybersecurity is no longer effective or efficient for most organizations. Today, there are "doors" and "windows" that most organizations aren't aware exist. For example, shadow IT, employees' personal devices, or servers and databases owned by third parties in the supply chain. It's impossible for businesses to defensively secure these entry points because they are not within the traditional realm of cybersecurity. However, they are still part of the external attack surface, offering intruders a way into critical systems.

In CybelAngel's 2023 "*State of the External Attack Surface: Annual Threat Trends Analysis Report*," our findings revealed exposures outside of an organization's firewall are the greatest source of cybersecurity threats.

While compling our annual report we found more than **70 billion files**, including intellectual propery and sensitive financial documents were currently freely available, unprotected and, on unsecured web servers. CybelAngel's suite has five modules, including asset discovery and monitoring, data breach prevention, account takeover prevention, dark web monitoring, domain protection to help you cover all your external attack surface management use cases.

An outside-in cybersecurity approach can save organizations time, money, and stress by preventing attacks in the first place, rather than waiting for them to happen and mitigating the damage after the fact. As the saying goes, an ounce of prevention is worth a pound of cure and this is especially critical when budgets are tight. Often, the cost to prevent an attack is a fraction of the cost to recover precious data. Once an attacker is inside, it's already too late.

**"With CybelAngel, we established a new border of detection outside of our architecture, encompassing the world of our partners and suppliers, where we can't, by design, take control of their security."**

**Jean-Yves Poichotte,**
Global Head of IS Security, Sanofi

sanofi

## ⊗ The Challenge:

# Cybersecurity insurance premiums are steadily rising.

Data breaches, ransomware, and other cyberattacks make for pricier cybersecurity insurance premiums.[8] In the first quarter of 2022, cyber insurance premiums **increased by an average of 28%**, compared with the fourth quarter of 2021.[9]

High demand for coverage and a reduced carrier appetite for risk are among the primary drivers for the continued price increases, fueled by greater awareness among organizations of the threat of cyber-risk for businesses of all sizes.

Should rates continue to climb and insurers increasingly offer more limited coverage, cyber insurance will become even more challenging to manage and maintain. But the widespread lack of cyber insurance poses additional problems as a single cyberattack could have an enormous financial impact on multiple organizations.



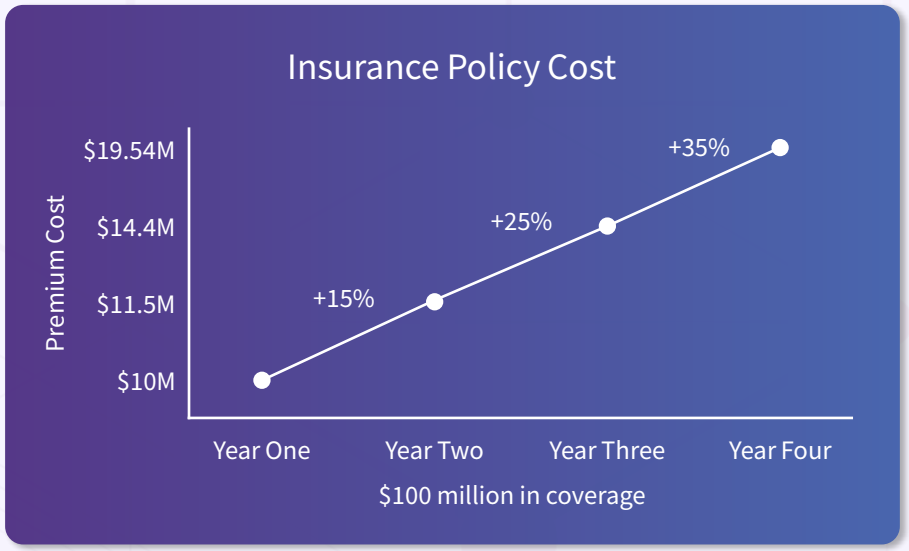

In the first quarter of 2022, cyber insurance premiums increased by an average of 28%, compared with the fourth quarter of 2021.

## Our Solution:

# Lower cybersecurity insurance premiums by improving security posture

Cyber insurance is a necessary expense for organizations, but there are ways to lower increasingly expensive premiums. While the costs of business policies tend to vary, most insurance companies will tailor a policy to an organization's particular needs. Companies should adjust their coverage strategically to cover truly catastrophic or "black swan" events, rather than relying on insurance payouts to act as a band-aid for common and avoidable incidents caused by poor cybersecurity practices.

One way companies can cut insurance costs is by improving their cybersecurity posture. A hypothetical insurance policy with premiums costing $10 million for $100 million in coverage is likely to increase by 15%, 25%, and 35% each year over a period of three years. However, with the right security solutions in place, an organization can improve its cybersecurity practices and avoid making any claims, limiting the increase rate to 10%, **saving $437,000**.[10]



# ⊗ The Challenge:
## Redundant cybersecurity tools are driving costs skyhigh

Many companies opt to invest in multiple cybersecurity tools to protect themselves from increasingly common and catastrophic cyberattacks. On average, organizations utilize **25 to 49 security tools** from 1 to 10 vendors.[11]

An overdependence on many tools can potentially expand a company's attack surface and actually prevent developers from addressing critical threats.

It's no surprise that the more tools a business turns to for solutions increases spending. Organizations should look for solutions that can accomplish more instead of choosing ones narrowly focused on niche areas. This will reduce the number of redundant tools and overlapping capabilities.

Additionally, too many technology investments can give organizations a false sense of confidence in their security posture.

> **While there is a prevailing perception that the more security tools an organization uses, the more secure it is, the opposite can be true.**

Too many tools could expand a company's attack surface and prevent developers from addressing critical threats.[12]

# Our Solution:
## Streamline security tool stacks

It's no surprise that the more tools a business turns to for solutions increases spending. Organizations should look for solutions that can accomplish more instead of choosing ones narrowly focused on niche areas to reduce the number of redundant tools and overlapping capabilities.

CybelAngel was recognized by Forrester in the External Threat Intelligence Service Providers Landscape, Q1 2023, as the only provider able to cover all external attack surface use cases:

- compromised asset detection
- vulnerability management enhancement
- general threat landscape monitoring
- targeted threat monitoring
- enabled threat hunting and modeling

Opting for a security tool that offers a modular approach can enable organizations to pick and choose which areas to focus on first. Addressing the most significant threats first can help reduce risk in those areas without over-investing in unnecessary capabilities.

Choosing vendors with a comprehensive platform allows organizations to reduce the total cost of ownership, by simplifying administrative overhead, facilitating integration and setup and reducing SOC team fatigue. Learn more here.

# The Challenge:
## A global cybersecurity talent shortage

A global cybersecurity **workforce gap of 3.4 million people** means there are simply not enough security professionals to fill open positions.[13] In the US alone, there are more than 700,000 unfilled cybersecurity positions.[14]

Despite offering superior pay, benefits and perks, many organizations still struggle to fill empty seats. Running a tight ship puts pressure on understaffed teams to deliver the same results with fewer employees at the helm.

This predicament often produces a vicious cycle of stress, low morale, and burnout. All of which leads to poor productivity and more mistakes, while creating more work and more pressure to improve performance. A stressful work environment causes high turnover, which puts even more pressure on those who are left to pick up the slack.



The global cybersecurity workforce gap is

**3.4M PEOPLE.**



In the US alone, unfilled cybersecurity positions are upwards of

**700,000.**

## Our Solution:

# Invest in technology that enables higher team productivity and prevents burnout

The right security solution should help cybersecurity teams do more in less time, rather than be a source of frustration. Companies should be wary of tools that simply generate huge volumes of alerts and reports without context. Some of these tools may actually create *more* work for cybersecurity teams, as teams can spend hours manually sifting through graphs and charts trying to find actionable insight.

If technology can compensate for the workload of at least two security analysts, organizations can theoretically **save about $860,000** over three years.[15] It might be tempting to develop an in-house solution with the money saved, but commercial off-the-shelf cybersecurity solutions are often faster to deploy and more robust.

In a tight economy, demonstrating fast time to value for tech and tool investments is critical, so kicking off a multi-year development project without immediate results is often a losing proposition.

CISOs should give the same consideration to selecting a new solution. Is the technology proven and field-tested or is your team going to waste time and money acting as guinea pigs while bugs are worked out? At CybelAngel we have dedicated analysts for all our clients. It saves our CISOs' teams a lot of time to focus on added value tasks.

## ⊗ The Challenge:

# Teams are wasting time on unimportant threats and false positives

A security tool sprawl combined with a lack of cybersecurity talent leads to many teams being  so overwhelmed by security alerts that they miss critical threats. As many as 40% of organizations admit that their teams can't respond to at least 25% of security alerts.[16] Today, many security analysts are experiencing what's called "alert fatigue," which can cause burnout, high turnover, and internal friction.

Additionally, **more than 40% of security alerts are false positives** or alerts that incorrectly indicate that a vulnerability is present.[17] In 2021, 75% of organizations spent as much or more time chasing false positives as they did dealing with actual security incidents.[18]



## Our Solution:

# Adopt tools to help teams prioritize important threats

Effective cybersecurity solutions will not advertise the raw number of alerts as their sole selling point without also mentioning their false positive rates, or the methods they use to help process and prioritize these alerts. Rather than overwhelming cybersecurity teams with too much information, solutions should have advanced filtering and severity ranking capabilities to ensure that only the most important or critical issues are surfaced for human intervention. The ideal solution — and by extension, the support staff behind it — should add value to your team on a daily basis, not introduce more noise into workflows or send your team on a wild goose chase.

At CybelAngel our unrivalled machine learning allows for filtering 1 billion data points everyday to provide zero false positives. This is key for CISOs who stop wasting time investigating fake incidents. On top of AI, all accounts at CybelAngel have a dedicated analyst who is your go-to expert for analyzing and contextualizing every alert targeting your brand and business.

# THE RIGHT SOLUTION EXISTS

You may wonder is it possible to make your job as a CISO easier while keeping your threat landscape more secure? It doesn't require magic but rather, the right technology.

Managing cybersecurity costs in a downturn economy requires more attuned focus and time. Your technology should help your people be more efficient and effective. It should also help you determine where to focus your efforts so that no one is burned out working on the wrong things. This solution should quickly highlight where you're most at risk so you aren't blindsided by a cyberattack that could have been prevented. By shifting to a proactive and preventative strategy, it is possible to maintain the same level of security with a reduced budget.

**REQUEST A CUSTOM DEMO HERE**

# A REAL TIME SOLUTION

Cushman & Wakefield is the world's third-largest global commercial real estate firm, with over 50,000 employees and approximately 400 offices in 60 countries.[17] When Cushman & Wakefield came to CybelAngel for help, they were primarily interested in increasing threat visibility and optimizing response capabilities.

**"With a smaller team, it was important we get actionable recommendations filtered through automation and human intelligence levels. To date, there hasn't been a single alert CybelAngel has raised to us that isn't linked to us."**

**Erik Hart,**
CISO, Cushman & Wakefield

**With CybelAngel, Cushman & Wakefield was able to:**



**Reduce false positives on alerts to zero**



**Gain visibility into previously untapped areas including the dark web**



**Outsource analyst talent and reduce internal expenses**



**Remediate external threats with actionable information and accurate risk ratings**



**Proactively prevent internal threats from causing security incidents**

# Sources


1. "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And ...." 19 Jan. 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/.
2. "2023 Global Digital Trust Insights Survey: PwC." https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html.
3. "Evolving the CISO Role to Make Cybersecurity a Competitive ...." 4 Oct. 2019, https://hbr.org/sponsored/2019/10/evolving-the-ciso-role-to-make-cybersecurity-a-competitive-advantage.
4. "Cost of a data breach 2022 - IBM." https://www.ibm.com/reports/data-breach.
5. "Cost of a data breach 2022 - IBM." https://www.ibm.com/reports/data-breach.
6. "Data Breach Prevention - CybelAngel." https://cybelangel.com/solutions/data-breach-prevention/
7. "2022 Data Breach Investigations Report - Verizon." https://www.verizon.com/business/resources/reports/dbir/.
8. "Companies are finding it harder to get cyber insurance - CNBC." 11 Oct. 2022, https://www.cnbc.com/2022/10/11/companies-are-finding-it-harder-to-get-cyber-insurance-.html.
9. "Q1 P/C Market Survey 2022." https://www.ciab.com/resources/q1-p-c-market-survey-2022/.
10. "The Total Economic Impact™ Of CybelAngel." https://cybelangel.com/wp-content/uploads/2022/05/Forrester-Total-Economic-Impact-Report-CybelAngel-May-2022.pdf.
11. "Security Point Tools Problems - Enterprise Strategy Group." 30 Jan. 2019, https://www.esg-global.com/blog/security-point-tools-problems.
12. "Is Your Organization Suffering from Security Tool Sprawl?." 27 Sep. 2019, https://www.darkreading.com/cloud/is-your-organization-suffering-from-security-tool-sprawl-.
13. "(ISC)$^2$ 2022 Cybersecurity Workforce Study." https://www.isc2.org/Research/Workforce-Study.
14. "Companies are desperate for cybersecurity workers—more than ...." 30 Jun. 2022, https://fortune.com/education/articles/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/.
15. "The Total Economic Impact™ Of CybelAngel." https://cybelangel.com/wp-content/uploads/2022/05/Forrester-Total-Economic-Impact-Report-CybelAngel-May-2022.pdf.
16. "Study Reveals Major Security Challenges Companies Face." https://cisomag.com/study-reveals-major-security-challenges-companies-face/.
17. "2022 Cloud Security Alert Fatigue Report." https://orca.security/lp/2022-cloud-security-alert-fatigue-report/.
18. "Reaching the Tipping Point of Web Application and API Security." https://www.fastly.com/web-application-and-api-security-tipping-point.
19. "Cushman & Wakefield | Commercial Real Estate Brokers & Services ...." https://www.cushmanwakefield.com/en/united-states.



# CybelAngel

CybelAngel is a leader in External Attack Surface Management (EASM) solutions. We protect our customers with an extensive and continuous 'outside-in' search of an organization's internet-facing attack surface to discover exposed and unknown assets, produce a living map of online infrastructure, and uncover hidden vulnerabilities and threats. CybelAngel analysts then contextualize the most critical findings based upon business severity and perceived risk. This unique combination of machine and human intelligence leads to the highest signal-to-noise ratio on the market, leaving IT and security teams free to focus on core business operations.

For a complimentary assessment of your external attack surface, contact us today for a free External Exposure Scan.

LEARN MORE

# studio/ID

## BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

**LEARN MORE**