THE ESSENTIAL CISO PRIMER

Industry leaders open up about the threats and challenges they face at work.

CybelAngel

INTRODUCTION

The buzz and bustle in the cybersecurity profession means that each day, week, quarter, and so forth, brings new challenges.

The role of the CISO is emerging from the shadows to claim a central role in the boardroom, and it comes as a general feeling of instability grips executives. Rising cyber insurance premiums, ransomware threats, and, of course, the recent world-wide July outage-partly caused by a cybersecurity update by CrowdStrike-mean cyber executives are feeling the heat.

We've entered a period of **cyber crisis**.

Cyber warfare is in full swing, and cyber experts have had to speedily adjust to this unstable cyber climate. Yet, exceptional leaders strive for more, to overcome challenges and inspire other leaders and cybersecurity titans.

Over time, these experts have meticulously mapped a process that is laser-focused, highly efficient, and remarkably effective.

These leaders have influenced a new generation and have expanded the possibilities of cyber success and capabilities. Their voices and areas of focus are contained in this Ebook. 5 profiles have shared their routines, tips, and reasons to be optimistic amid the tension and stress of cyber crisis management.

There are many reasons to dive in and soak up their wisdom.

Happy Reading.

Gregory Faitas,
Deputy CEO, CybelAngel

SUMMARY

PILLAR
N°1

OPTIMIZING YOUR DAY-TO-DAY

PILLAR N°1 | OPTIMIZING YOUR DAY-TO-DAY

Cybersecurity has changed dramatically in the past 5 years, from companies switching from a defensive strategy to an efficient proactive mindset. Macro trends like the global rise in ransomware groups, the rise of API threats and automation processes at scale have driven enormous change to processes. But one thing that remains constant is the risk involved.

CISO concerns in 2024: At a glance

- **Tech and tool stacks are ever overwhelming:** *"The speed and scale at which technology is entering the ecosystem is deepening executives' concerns and stressing the underlying technology systems in their organizations."*
- **Talent scarcity is the next big headache to anticipate:** The World Economic Forum's 2024 report reports a staggering global deficit of nearly 4 million cybersecurity workers.
- **Stress is all consuming:** 94% of CISOs suffer from work-related stress, and 65% of CISOs admitted that work-related stress issues are compromising their ability to protect their organization.

That said, many of the core principles for building, organizing and driving a SOC team are the same. The general advice recommends organizing your team, however small, around the most important risk cyber sub functions.

The focus for 2024, with the CISOs we spoke to, focused on tools, budget, bodies and much more. A large number were also wary of utilizing and using AI safely. Cyber leaders have been squeezed by dual pressure- finding the most efficient way of operating, while juggling dilemmas about talent shortages, effective reporting, ransomware spikes, and other external threats expanding.

"There are a few trends in the world of cybersecurity; number one is the proliferation of cloud computing. With that comes a high level of access, but also many misconfigurations that occur. Often, third parties are unaware this is happening."

Erik Hart
CISO, Cushman & Wakefield

PILLAR N°1 | OPTIMIZING YOUR DAY-TO-DAY

CISOs everywhere have been agile in adapting to this continued state of crisis. Here are ways leaders cope with optimizing their day-to-day grind.

I: Reactivity

Cyber professionals are not managing an extreme cyber crisis everyday. Daily routines versus extreme incidents require a different approach. Yet, being a reactive leader in all the right ways is critical in this industry.

The real question is, how can you balance constant reactivity to delegate effectively within your scope?

"Managing time and incidents is a critical aspect of our operations. We involve multiple teams based on the incident and take a closer look at the details to ensure comprehensive coverage. A specific timeline is always in place, tailored to the type of incident and the response required. For us, remediations take precedence, guided by a standard operating procedure (SOP) to thoroughly investigate the incident or affected asset. We adopt a risk-based approach and have a policy in place to assess the impact and act accordingly, ensuring efficient and effective management of each situation."

James Stills
Director of Global Information Security Operations at SC Johnson

Loren Kawasaki
Global Information Security Operations Service Manager

Cyber seasons keep shifting

The secret to managing pressure for some CISOs has been to appreciate the cyber seasons that they cycle through-high pressure down to smooth cohesion. Sometimes seasons include variations of sacrifice, frustration and stress, while others are more manageable.

TIPS

- **Take frequent pulse checks**
  Before issues escalate into something major, consider encouraging your management team to check in more frequently with your wider team. Organizations that conduct regular pulse surveys see 14.9% lower turnover rates compared to those that don't.

- **Weak prioritization and remediation**
  The SANS 2023 Attack and Threat Report notes that CISOs are often strong in identifying big risks but weak in prioritizing and remediating them. Clarification is key to fast remediation.

- **Focus on better change management processes for boardroom reports**
  Yes it is a mouthful but yes it is important. Change management is crucial when integrating outsourced services into existing security operations. We'll discuss this more in detail in the last section of this Ebook.

II: Staying sharp and up to date

Much ado about nothing?

Unfortunately, CISOs today are under pressure to be all knowing. They face expectations to keep up with management details as well as technical and financial company data, while often trending topics and education take a backseat.

Great CISOs need to stay abreast of industry trends and changes when the topic at hand is so variable. Following the development of important topics and trends offers clarity at scale for the entire SOC department and is a key component of a CISO's job.
CISOs we spoke to offered ways to improve how you can stay primed:

"The advice I would give to a young CISO is to **understand your organization's risk tolerance and understand what's important to your organization**. Some organizations are more risk averse than others. You really need to understand your business, and what risk you can accept and what risk you need to mitigate or remediate."

Erik Hart
CISO, Cushman & Wakefield

"My main four daily bricks include: 1: Building partnerships across the company to be able to successfully protect the company. 2: Being present and speaking to all key people throughout the organization and throughout levels. 3: Building cybersecurity acumen especially concerning education. 4: Building a well structured cyber defense center to make sure all tools we need are available. Overall it is important to keep in mind that everyone is a sales person and **you need to make time to talk to the newest team member right up to right up to the C-suite leve**l."

James Stills
Director of Global Information Security Operations at SC Johnson

TIPS

Read widely and critically

Read a variety of sources, including relevant essays, articles, newsletters, and books, focusing on those that demonstrate compelling use cases you can enjoy and learn from.

Demand clarity

Ensure that your technical requirements and other communications from your team are crisp and clear. Make it clear that you don't want jargon but rather just the specifics about objectives, tasks, and outcomes. A recent cybersecurity report indicates that a major impediment to cybersecurity project success is a lack of clarity about processes and digital maturity levels.

Implement the right tools for better coverage

Your tool stack needs to minimize critical stress and take the heat out of painful cyber decision making. For example, implementing a suite of tools, like the CybelAngel platform, allows you to consolidate your coverage of a huge threat landscape.

Fiercely pencil in your deep work

Deep work is a major competitive advantage in the land of cyber security distractions. "Deep Work" by Cal Newport explores how critical "deep work" is. Focused, uninterrupted, and cognitively demanding work allows you to produce at an elite level. Create two blocks a week to start carving out time for productive deep work and increase it if you have capacity.

These tips should help you to deliver business impact by marshaling the resources of your team (both humans and machines) as you identify and solve the most impactful cyber issues together.

III: Team communication 101

Remote employees. Stressed team members. Pushy board colleagues. Management gripes. Communicating well can feel like a superpower amid the pull and push of day-to-day management.

Seasoned CISOs have a lot to say about communicating with a giant web of stakeholders who need different information. Before we find out more, here are some helpful tips:

TIPS

- **Pivot meeting requests to email or chat**
  Close constant requests for a 60 minute window of your time and instead power through the “ask” in 10 minutes. Tell your team you want to start async over email before diving into a call so everyone is aware that meetings are not a default option.

- **Flex your “NO”**
  Burnout is affecting a reported 70% of surveyed CISOs in the U.K. It is just a given that cyber professionals cannot have productive conversations and handle today’s workload without deprioritizing more critical items on that ever growing to-do list.

- **Respond quickly to issues**
  Act swiftly when your team raises concerns that will escalate and turn detractors into promoters. Crisis management issues largely need your on-the-spot decision making as indecisiveness can undermine your authority.

- **Humanize interactions**
  Did you know that just 32% of employees trust their senior leaders to do what is right? Focus on building genuine connections to enable talent retention within your SOC team.

"You need to be able to put security issues firmly into a business context or you cannot secure the support of other business units. **As a CISO you cannot be in a vacuum**."

Todd Carroll
SVP of Cyber Operations and CISO, CybelAngel

"My day can be broken down into monitoring ongoing daily security threats, both in-house and outsourced, gathering data to report to the board, managing all alerts and services, ensuring that operations are functioning smoothly, and addressing stakeholders' needs, with training also being a significant part of my responsibilities."

Loren Kawasaki
Global Information Security Operations Service Manager, SC Johnson

PILLAR
N°2

TRANSFORMING PROCESSES, VISIONS AND STRATEGIES

I: Vision, strategy and operations

In 2024 what are some key strategic and operational insights you need to be more agile? How can you mold your cybersecurity strategy to be more optima ? What are some approaches recommended by cybersecurity frameworks?

Find out why responses that are agile, risk-informed, and continuously improving set an overall tone for managing your organization's risks.

The power of an agile cybersecurity strategy

The NIST Cybersecurity Framework 2.0, released in February 2024, outlines six core components for a comprehensive cyber strategy: Govern, Identify, Protect, Detect, Respond, and Recover. This updated framework emphasizes a more proactive and holistic approach to cybersecurity risk management.

TIPS

- **Secure executive buy-in**
  Obtain support from key stakeholders including the CEO, CFO, CPO, and COO by presenting compelling data demonstrating the need for organization-wide changes in cyber hygiene, training, and engineering policies. You should emphasize the framework's applicability across various sectors and its role in regulatory compliance.

- **Scale Cybersecurity through Engineering and IT**
  Transitioning from isolated cyber operations to an integrated approach involving your central data team is the goal here. Try to focus on creating and scaling proper security and governance practices across the entire organization. You can also leverage the framework's implementation examples and informative references to guide you.

- **Embrace agility over perfection**
  Ultimately you'll need to recognize that there's no one-size-fits-all solution; instead, focus on an optimal structure that aligns with your specific cyber lifecycles, vision, and strategies. Leading CISOs should consider their organization's inherent strengths in technology and team approaches. You should also regularly review how your organizational structure impacts internal decision-making and talent retention.

- **Leverage NIST CSF 2.0 resources**
  Make use of the framework's expanded guidance, including Quick Start Guides (QSGs) for smaller organizations. You should also regularly consult the online resources provided by NIST, such as updated implementation examples and informative references.

- **Focus on proactive risk management**
  By using this framework you'll be able to identify and address potential vulnerabilities before they can be exploited. You can also outsource your external threat monitoring

"**Lean on your vendors when resources are lean**. Challenge them to improve and address today's threats. Demand more from them. Let them know you need more data to communicate the value and ROI of your spend to your board."

Todd Carroll
SVP of Cyber Operations and CISO, CybelAngel

II: Talent retention and structuring your team

Is talent retention truly a headache? What are the key drivers of talent mobility in the industry? What are the pivotal policies and benefits needed to stay competitive amidst global competition for cyber skills? What business strategies are needed to link everything together and harness potential?

Needless to say, cyber talent retention is a hot topic.

"**Retaining talent is a top priority for us**, as we are always looking for long-term hires who are focused on development. **We're less concerned about technical aptitude and more about culture fit, dedication, and the drive to learn and grow**. We believe in teaching them the hard skills, provided they come equipped with soft skills. Our very formal process outlines what we outsource versus what is kept in-house; we outsource most operational actions and center our internal team on driving strategy. **Staying lean and scaling our managed services as needed allows us to create a stable environment without disrupting business operations**."

James Stills
Director of Global Information Security Operations at SC Johnson

Loren Kawasaki
Global Information Security Operations Service Manager

TIPS

Steps to reduce high-performer burnout

If high talent density is your aim within your team, aim to double down on data and feedback from star performers about burnout and workload related issues. Research from Ivanti noted that of IT professionals who report high levels of burnout, 42% are considering quitting their company within the next six months.

Handling talent volatility and hiring bets

In 2021 data showed it took 50 days to fill cybersecurity positions, compared to 41 days for general IT jobs. The European Cyber Security Organisation noted that, *"The expectations and attitudes of the employers sometimes exceed the real qualification and proficiency levels of the graduates and there are very limited options for HR professionals to assess this."* This extended timeframe reflects the complexities and specific skill requirements associated with cybersecurity roles. In volatile industries, hiring takes place quarter by quarter.

Ongoing feedback and open conversations are key

IMaintaining excellence isn't a one-off task; it's a continuous conversation. Avoid rigid performance reviews and instead opt for regular, open dialogues combined with an annual 360 feedback process—aimed purely at fostering growth and improvement, not doling out ratings.

Review the meaningful work quota (yes really!)

Deloitte emphasizes that the number one tip for talent retention is to provide meaningful work, which includes offering employees autonomy, opportunities to collaborate in small teams, and ensuring they are well-suited for their roles. This approach not only enhances employee engagement but also fosters a sense of purpose within the organization. Notably, the cost of replacing employees can range from 1.5 to 2 times their annual salary, highlighting the financial importance of effective retention strategies.

III: Designing, deploying and maintaining the perfect tool stack

Does the perfect toolstack balance exist? Can CISOs reduce internal friction and waste with tools? How close is AI to replacing SOC tasks? Plus, why are 85% of cloud security professionals struggling to prioritize security events and manage multiple tools despite having enough resources?

The cybersecurity industry moves fast, which leads to lots of confusion about what tools are performant and worth it. To make matters more challenging, advice can be contradictory.

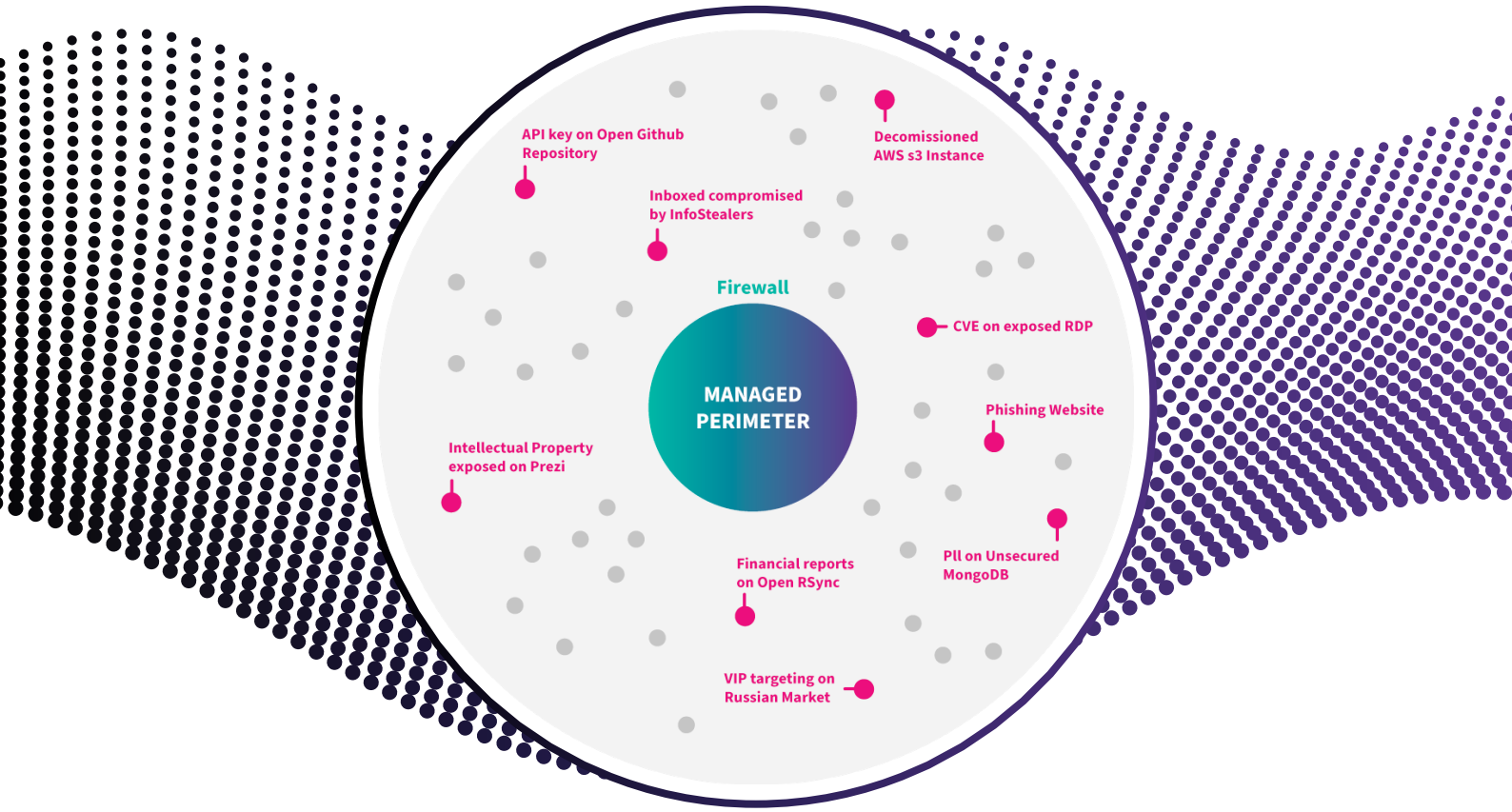


Figure: *A visual representation of your External Attack Surface*

"For the next year, our challenge is to monitor more and more cloud computing."

Thierry Auger
CISO, Lagardère

TIPS

Evolve your toolstack

The average security team manages upwards of 75 different security tools, leading to operational inefficiencies and a fragmented security posture. Sit down and put pen to paper about the benefits of switching from multiple vendors. Cost savings and increased efficiency make sure your toolstack is working hard for you. Tool consolidation is a term du jour but consider this guide for all of the arguments why it matters.

Team management tools matter too

Here is our pick of the most secure team tools for seamless collaboration:

Kroolo

Manage projects, tasks, goals, and documents with easy collaboration thanks to secure AI-powered features that maintain data integrity.

Assembla

Looking for a secure code repository integration that is compatible with Perforce, Subversion and Git? Test Assembla's agile documentation.

Microsoft Teams

As part of the Microsoft ecosystem, Teams benefits from advanced security features, including multi-factor authentication and compliance with various industry standards, making it a secure option for team collaboration.

G suite

The G-suite is an industry titan for a reason, with Google Meet reporting 99.9% accuracy in blocking spam and compromising emails .Google claims zero detected or hijacked accounts after deploying security keys. It is an excellent collaboration suite.

ClickUp

Increase visibility across your IT and SOC departments with a tool committed to user data protection, improving your workflows, processes and visibility.

Don't dismiss regulatory compliance

Data shows that 44% of cybersecurity professionals struggle with regulatory compliance. With increasing scrutiny on data protection and privacy regulations, ensure that the tools selected comply with relevant laws and standards.

PILLAR
N°3

DEMONSTRATING EXTERNAL VALUE TO STAKEHOLDERS

PILLAR N°3 | DEMONSTRATING EXTERNAL VALUE TO STAKEHOLDERS

How can you get back on the right track when it comes to reporting metrics and KPIs? What mistakes are CISOs invoking when it comes to presenting strategy and everything in between to the board? What driver metrics are you ignoring? And, finally, can anything be done to make budget wrangling easier (or is this the impossible dream?).

If the idea of self-promotion as a CISO makes you feel uncomfortable, consider the expert perspectives below on what value this process achieves. We know that advocating for your team's needs and resources, and sharing important metrics you've all achieved helps everyone.

Here are some insights we've rounded up.

"Overall we look at attack surfaces and then look at what critical controls there are. Then from an asset standpoint we look at coverage and efficacy to define how effective a control is. When it comes to compliance and assurance, we ask ourselves why does each control matter and how does it give us assurance in our cyber security program. When it comes to evaluating tools we consider the specific goal of each tool to understand how it bolsters our assurance in the cybersecurity measures we have in place."

James Stills
Director of Global Information Security Operations at SC Johnson

"What are my tips for sharing KPIs with stakeholders? For starters, a good briefing to any audience is well prepared and adapted to their experience and backgrounds. Review resumes, talk to your peers and use resources like LinkedIn profiles to get more context on board members. Ask yourself if you know what your audience anticipates, don't be afraid to ask them questions to make sure your briefing is tailored to their needs, level of expertise and expectations. Also, you always need to share big issues before board meetings so no one is caught unaware. Most importantly, don't waste anyone's time with irrelevant KPIs."

Todd Carroll
SVP of Cyber Operations and CISO, CybelAngel

TIPS

Set up a regular metric review NOW

If you want to get on the right track, faster, switch to a more frequent review. This ritual will help you to transform how you approach reporting when you focus on the driver metrics that are essential for distilling complex data down. A regular cycle meeting makes clarification faster, keeps everyone aware and accountable.

Take the right route with KPIs

CISOs should focus on reporting on key control indicators (KCIs) that directly measure the effectiveness of security controls and their impact on business risk. Examples of KCIs include the percentage of assets within policy, the percentage of privileged accounts managed within policy, indicators of incident volume, cyber incident categorization etc. Mostly you need to make sure that every KPI or KCI is an understandable metric for your audience. A complex or KPI which has to be explained will likely be ignored or misunderstood.

Outcome-Driven Metrics (ODMs)

Gartner emphasizes the importance of using ODMs that link security and risk operational metrics to business outcomes they support. These provide a more accurate picture of cybersecurity capabilities and can include:

- Time to patch
- Third-party risk engagement
- Endpoint protection
- Ransomware recovery

Make sure you have leadership buy-in for your CISO strategy

We've previously touched on this, but everything from resource allocation to a crisis management incident plan means nothing unless you have leadership support. The culture of fear around cybersecurity failure creates acute pressure on you and your team. Offset these nerves by setting the tone with your board before issues arise.

BUDGET TIPS

Budget should be a top focus for any CISO. Why? Well, a 2023 study by Stott and May found that 51% of CISOs see budget constraints as their biggest barrier to executing their security strategy, up 16% year-over-year.

1

Start totting up risks and their costs
Quantify, quantify, quantify. You'll need to articulate the potential financial impact of cyber threats (our annual report makes great reading on threat landscape trends and costs). Make your case for the right amount of investment. Flat or declining security budgets year-over-year spell future issues and you'll need to use key metrics to fight this.

2

Keep the focus on KPIs and ROI
The right metrics move the discussion on further. KPIs related to cybersecurity initiatives that demonstrate expected ROI should be your driver metrics here. By highlighting how specific investments will reduce risk or improve compliance, you'll reduce friction for decision-makers to see the value in funding these initiatives.

3

A seamless CFO X CISO collaboration needs you both
Make it your business to have a regular catch up with your CFO to share relevant granular insights that keep you both abreast of department needs and spend. Alleviate pain and shame by aligning with Finance to understand security needs and buy in that reflect the company's financial realities. The keyword here is responsible. Both departments need to buy into budget realities.

4

Get the support with other departments
Enlist the support of other departments, such as IT, legal, and compliance, to strengthen the case for increased funding. Use cases like robust data loss prevention (DLP) compliance measures can be used to boost your argument. Highlighting shared economic interests can push for and uncover additional resources.

5

Prepare for the worst case scenario
Just like with incident planning, plan a worse case scenario for the budget, with the broader economic environment in mind. A well-researched budget that accounts for budget setbacks demonstrates foresight and responsibility, making it more likely to gain approval.

6

Tool consolidation is a good thing

Leaner budgets require more flexible vendors that have tool stacks that work harder for your money. 75% of companies pursue security vendor consolidation, according to a recent Gartner survey. We detail more of this strategy in this Ebook.

7

Showcase previous wins

Highlight your previous successes in managing cybersecurity risks and the ROI of your improved security posture. Don't be shy when it comes to your track record. Use your vendor dashboards to collate your data neatly.

8

Keep the board up to date

It sounds simple but do maintain ongoing communication with the board regarding cybersecurity issues and your budget needs.

"When negotiating the budget, I start by asking for additional funds with full transparency to the board; I self-assess all metrics and, if a gap is identified, I develop a thorough business case that considers the cost-versus-time ratio to address the issue, all while building upon and maintaining the trust that the board places in our security team."

James Stills
Director of Global Information Security Operations at SC Johnson

---

"Here are my two cents when it comes to Finance. One, it is all relationship driven so talk to the Finance team about risk and impact on a larger scale. Don't isolate them from the bigger security picture. Two, there is always something that will come up so be prepared to navigate those difficult asks, by listening to their concerns and building trust."

Todd Carroll
SVP of Cyber Operations and CISO, CybelAngel

WRAPPING UP

WRAPPING UP

We interviewed many brilliant cybersecurity professionals as part of this report. We found that the topics that criss-crossed each interview were enlightening and affirmed a lot of shared solutions to old problems.

Here's a summary of the key conversation topics as we wrap up:

1. **Managing daily challenges**
   Employee retention is so critical, but organizations need to remember that offering meaningful work can significantly decrease turnover rates. Deloitte research highlights giving employees autonomy and well-suited roles can reduce the cost of employee replacements, which ranges from 1.5 to 2 times their annual salary. With high levels of burnout on the rise, strategies aimed at reducing work-related stress to retain your top talent are critical.

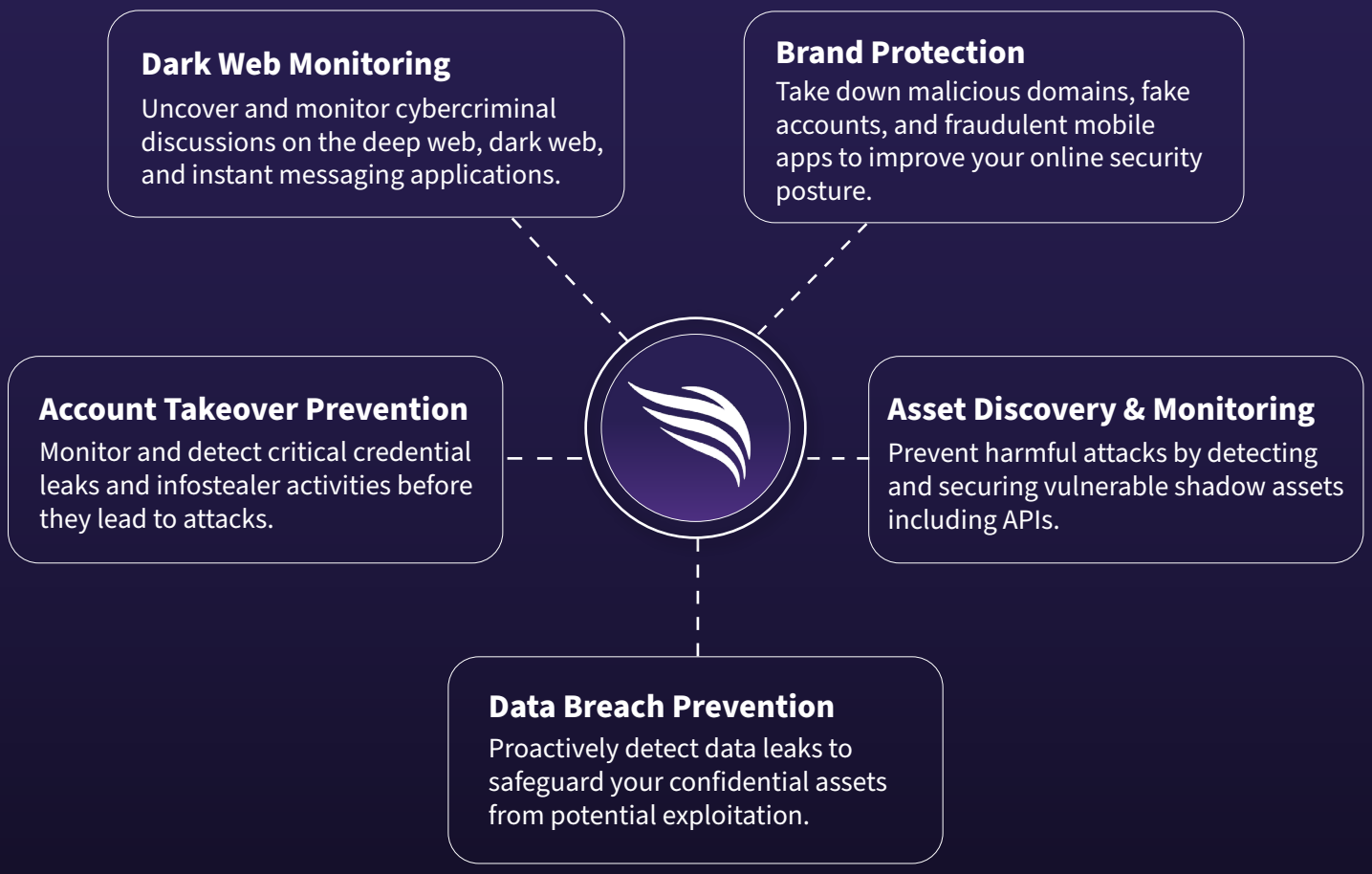
2. **Transforming processes, visions, and strategies**
   Transforming organizational approach is pivotal. With 85% of cloud security professionals struggling to prioritize security events despite adequate resources, this conversation evolves continuously. Leaders everywhere are keen to strike the perfect balance in cybersecurity tool stacks that enhance performance and value without overwhelming their budget.

3. **Demonstrating external value to stakeholders**
   Financing cybersecurity initiatives is more important than even when global cybercrime costs are projected to reach $8 trillion by 2025. Additionally, with flat or declining security budgets spelling future troubles, key metrics and aligning with departments like IT and legal can pave the way for increased funding and robust data loss prevention measures.

We hope that the insights shared within the three pillars outlined in this Ebook will help professionals navigate this challenging yet rewarding landscape, providing strategies to mitigate stress, improve talent retention, and enhance overall resilience in the cybersecurity field.

This Ebook is brought to you by

CybelAngel



Scan, Prioritize, Resolve External Threats

CybelAngel is the world's leading platform for External Attack Surface Management.

Secure your digital activities against cyberattacks and cyber breaches.

Learn more: Cybelangel.com
Dive deeper: Cybelangel.com/blog/

Stay connected