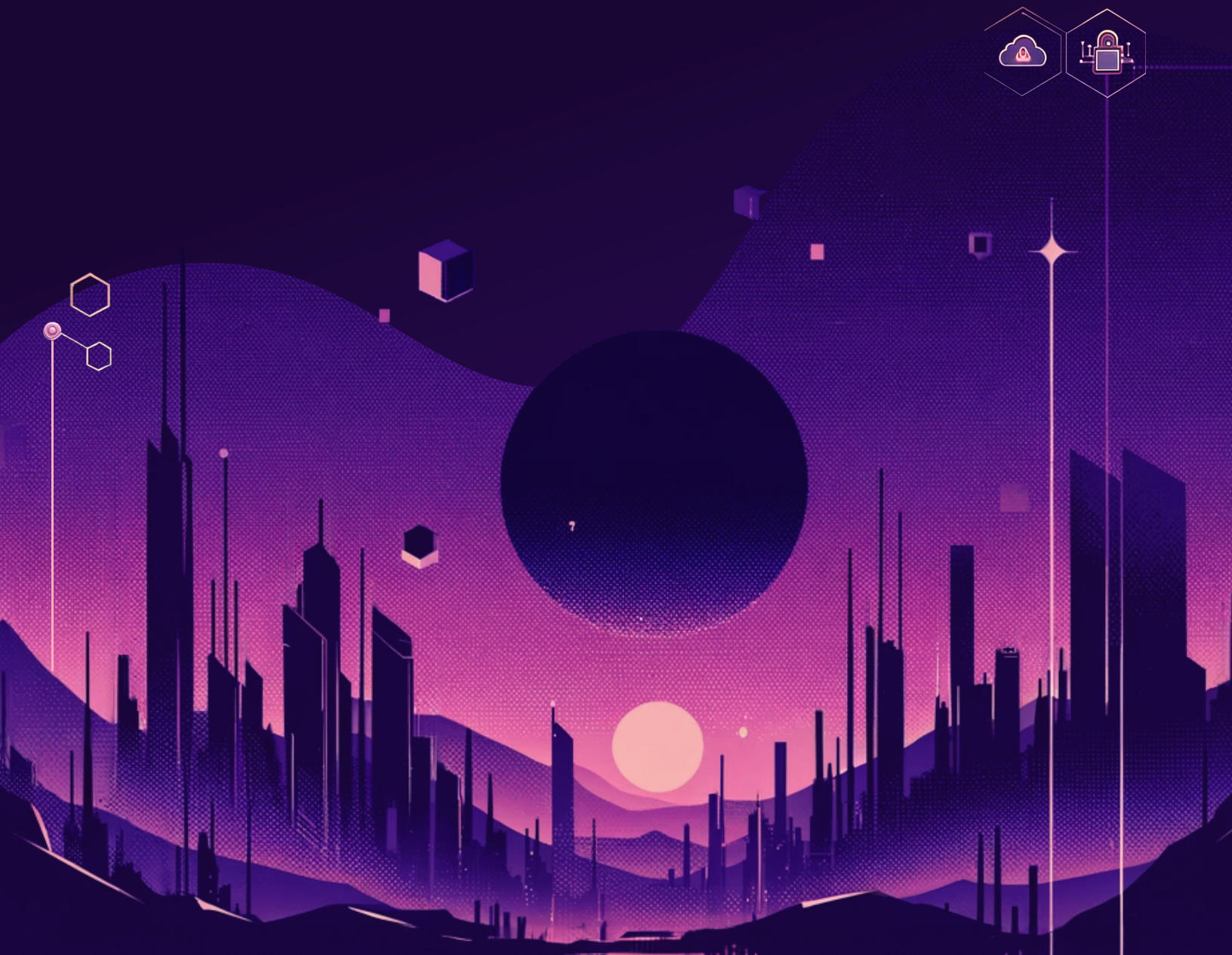
OffSec
The Path to a Secure Future™

OffSec's Insomnia Study:

What Keeps Cybersecurity Management Up at Night



Protecting organizations from cyber attacks relies on three pillars: technology, processes, and people.

Many studies have been done on the types of technology and processes that organizations should have in place to uncover and stop an attack before it causes significant damage and breaches critical systems. In this study involving **247 cybersecurity managers and leaders,** we explore the crucial role of skilled personnel – the third pillar – in enhancing cybersecurity posture and ensuring business process continuity. Without well-trained staff, processes and technology cannot function at their best to safeguard an organization.

In order for cybersecurity professionals to sleep better at night, leaders need to prioritize cybersecurity training and skills development. This focus is driven by executive and board responses to security events and the reliance on skilled teams for support.

Table of Contents

Introduction

Cybersecurity managers are accountable for the security of an organization but have limited control over executing the protection. These roles require a blend of technical acumen, strategic foresight, leadership skills, and the ability to communicate effectively with various stakeholders. With the growing importance of these roles and the increased accountability, this survey aims to understand the pressures they face in 2024.

Our extensive survey reveals a spectrum of concerns ranging from obvious cybersecurity threat prevention to the well-being of our respondents' teams. Moreover, it touches upon crucial organizational aspects like talent acquisition and retention, which are pivotal in sustaining a robust cybersecurity posture. The survey highlights the role of continuous learning and skill enhancement, which are key to not only strengthening individual competencies but also the overall resilience and adaptability of organizations within the changing cybersecurity landscapes.

This report is based on a comprehensive survey conducted by ViB, an independent research firm. The survey engaged 247 security professionals, providing a vendor-neutral perspective on cybersecurity leadership's top concerns. The research offers valuable insights with an estimated Effective Margin of Error of +/- 3.7%, ensuring the reliability and relevance of the findings.

01

Profile of Respondents

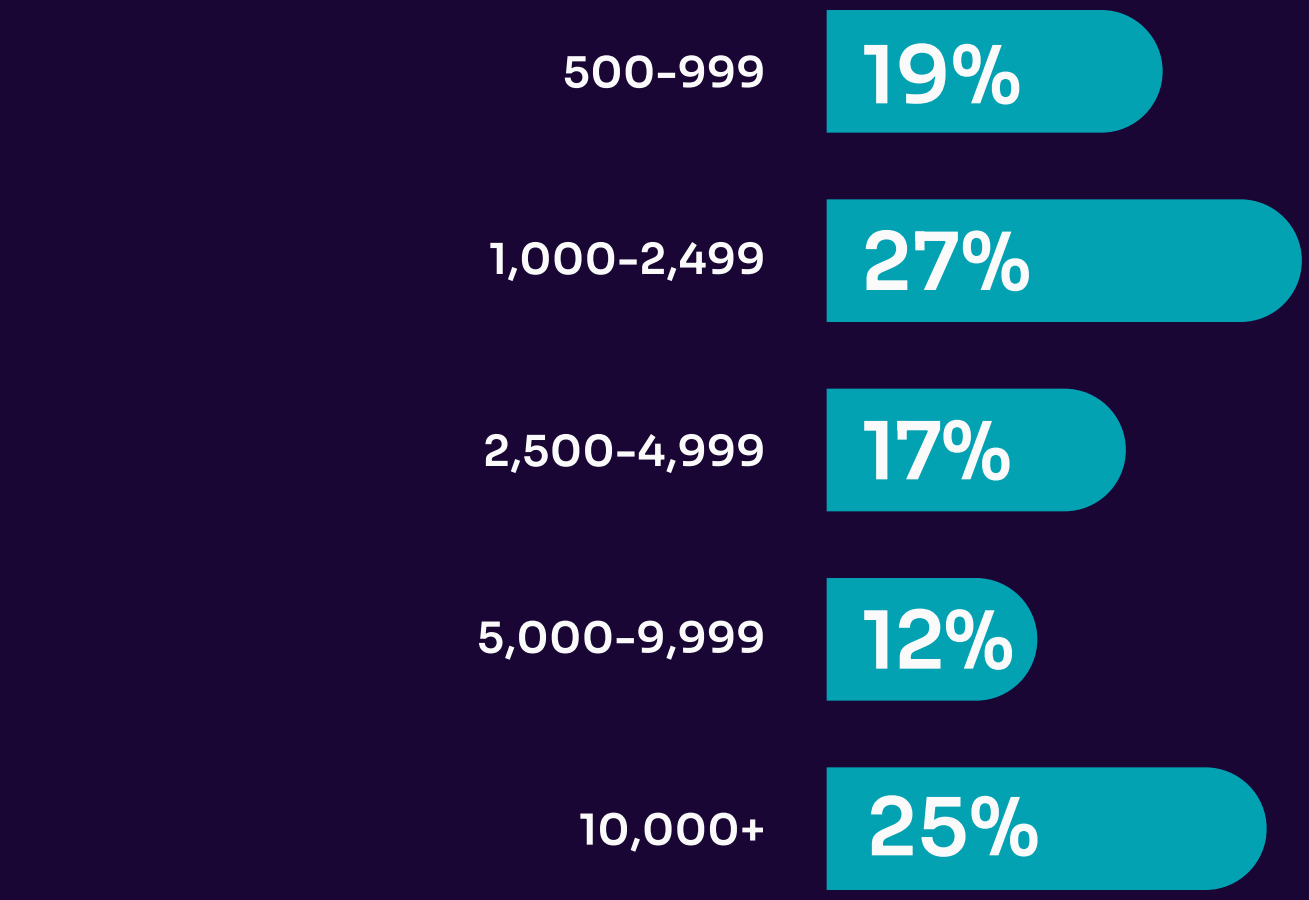
Our survey engaged cybersecurity professionals from an array of industries, roles, and organizational scales. This survey paints a detailed portrait of the current cybersecurity landscape, providing a nuanced understanding of the issues at play and the strategies employed to address them.

Job Titles

9%	C-level
11%	VP-SVP
36%	Director
44%	Manager

Company Size

Based on Number of Employees



02

Security incidents trigger extreme executive and board reactions

Over 1/2

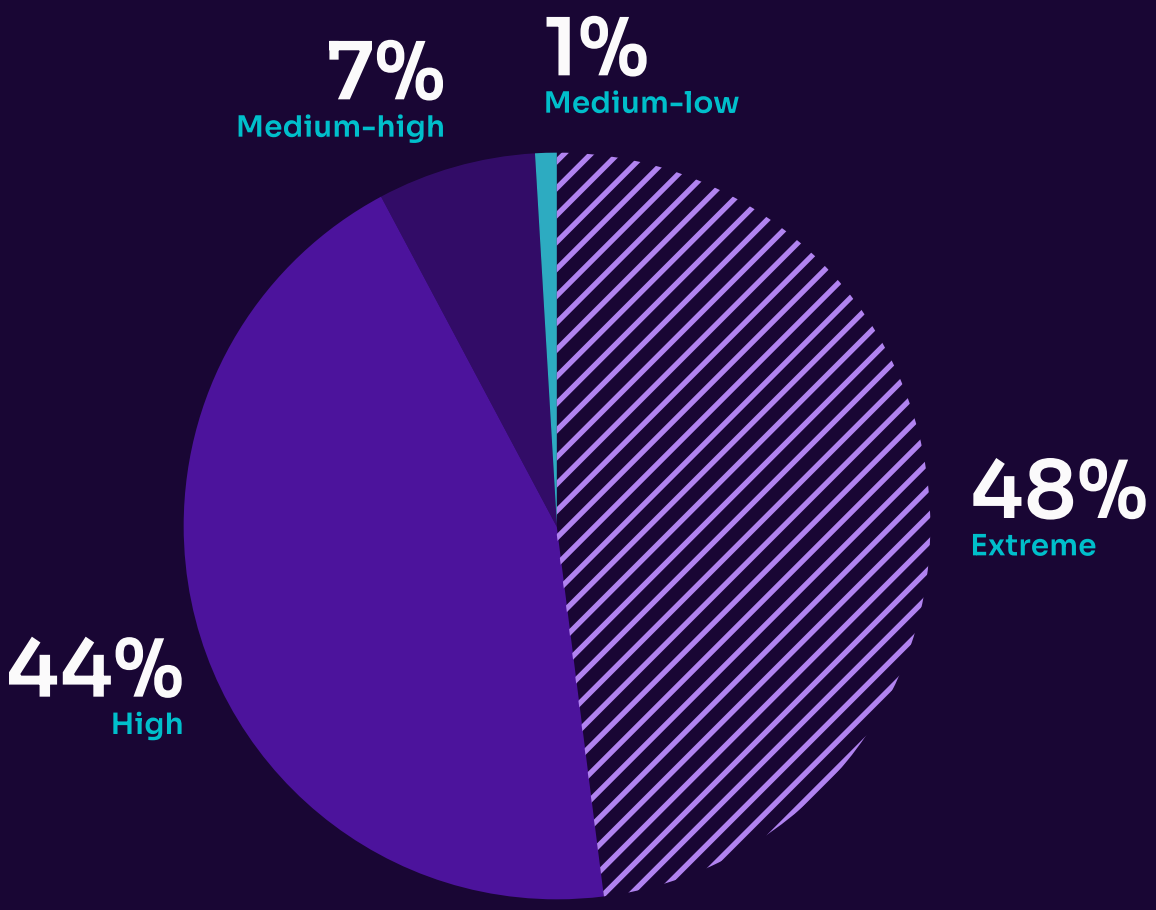
of respondents report moderate to significant impact on job security following an incident

Responses to major security incidents vary among respondents, revealing the differing levels of preparedness and strategic response across organizations. **48%** of respondents reported an extreme level of reaction by the Board / Executive leadership to a security incident indicating high urgency and seriousness.

This response level also increases internal and external scrutiny and creates a high-pressure environment for IT and cybersecurity teams. This is further confirmed by the fact that **25.7%** of respondents say that being involved in a security incident significantly impacts job security. Balancing such a reaction with thoughtful coordination is crucial to addressing the incident effectively without causing long-term negative consequences.

Yet, a high-pressure environment for cybersecurity teams, while challenging, can act as a catalyst for technological advancements and improved responses to emerging threats.

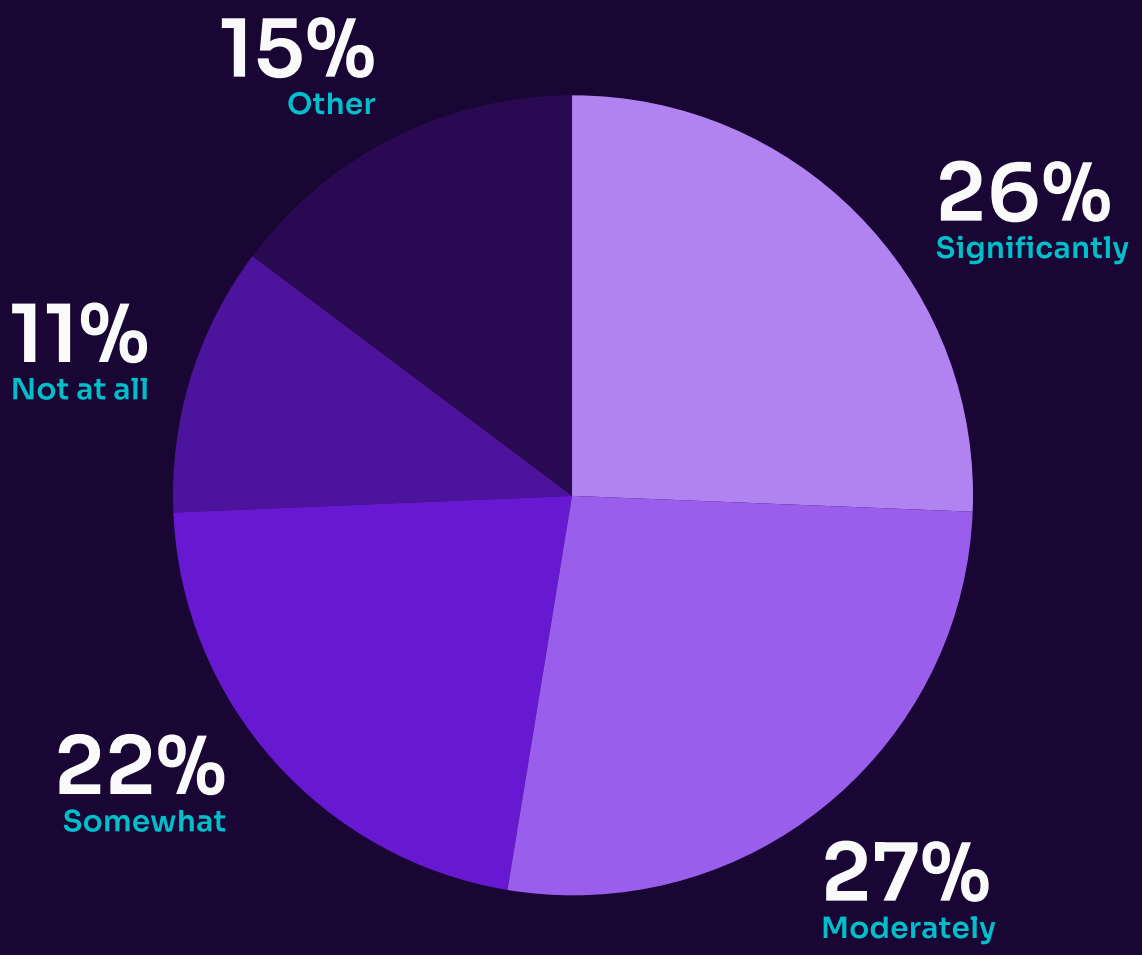
Board Reaction to an Incident



Nearly ½

report an extreme level of reaction by the Board / Executive leadership to a security incident.

Incident Impact on Job Security



03

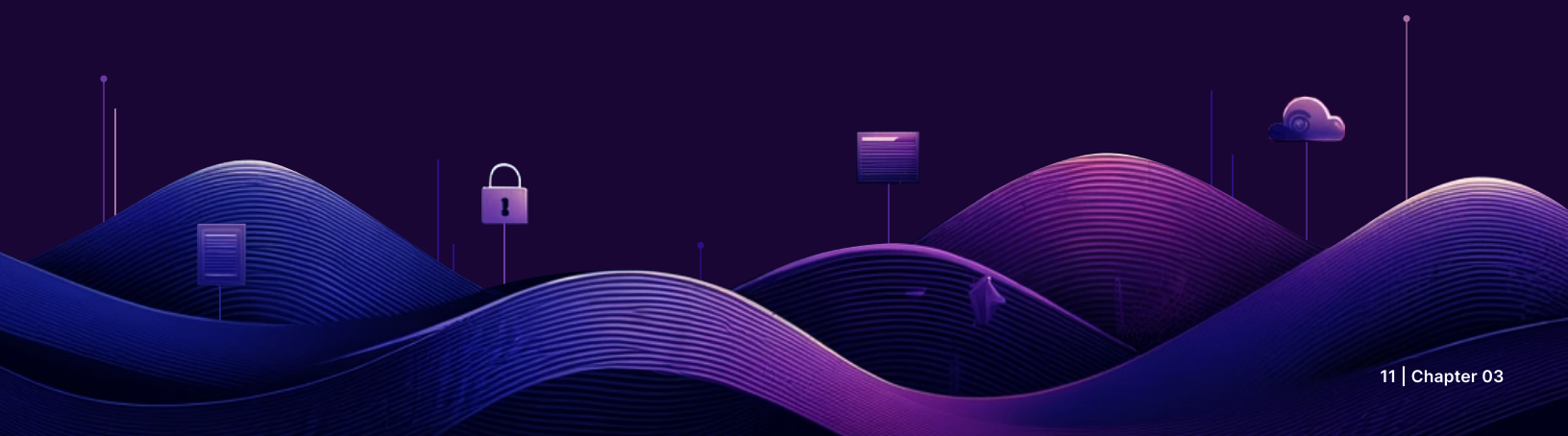
Respondents would rest easier knowing their team had the right depth and breadth of skill

91%

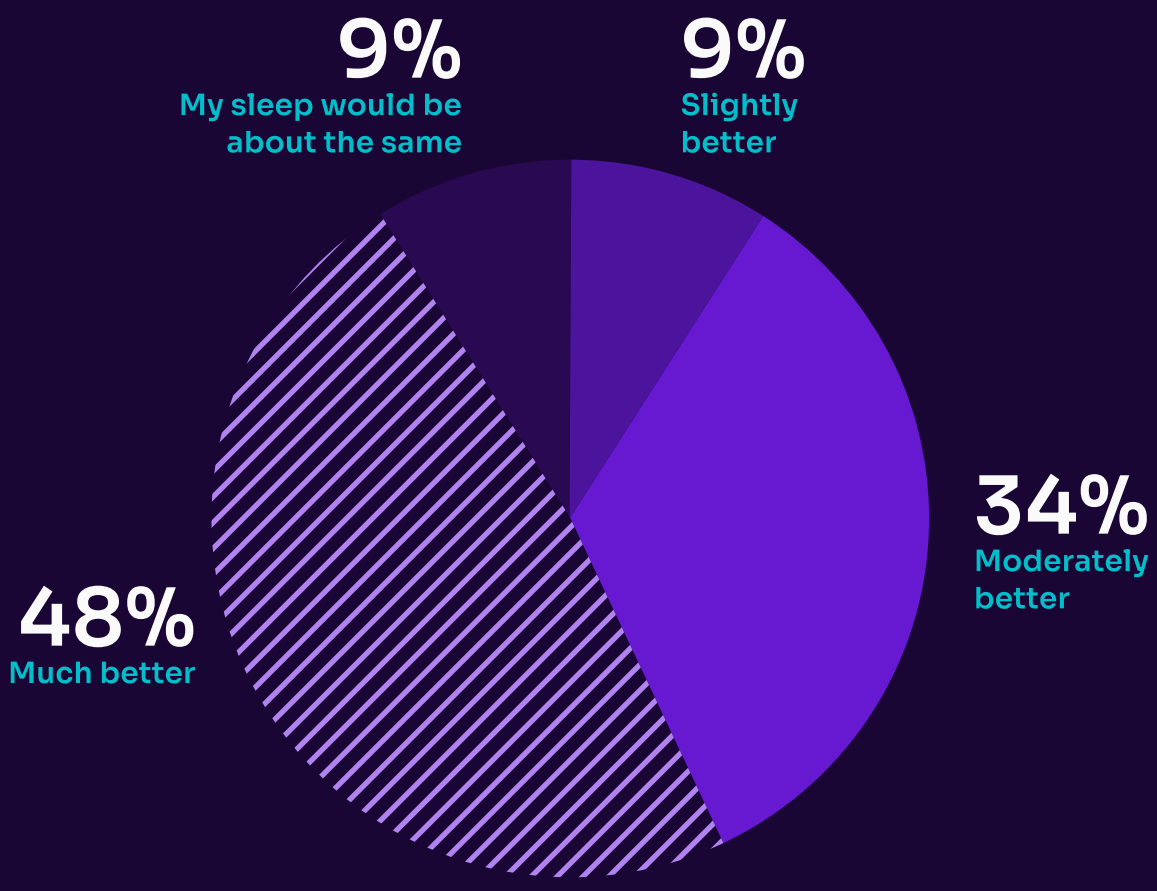
of respondents would sleep better at night knowing their team had the right skills

Our findings indicate that **91%** of respondents would feel more at ease if they were assured of their team's comprehensive skill set in handling cyberattacks. Additionally, **21.1%** emphasized the high importance of improving the retention rates of skilled cybersecurity professionals. This data points to a significant link between the proficiency of cybersecurity teams and the mental and emotional well-being of executive leaders. When leaders are confident in their team's abilities, it not only enhances the security of data and assets but also contributes to a more stable and less stressful leadership environment.

Effective training programs are essential in developing these necessary skills and competencies within cybersecurity teams. Training should be continuous, adaptive, and aligned with the evolving nature of cyber threats. It should encompass not only technical skills but also strategic thinking, crisis management, and effective communication, ensuring that teams are well-rounded and prepared for any scenario. Teams that are continually trained are able to keep up with the ever-changing threat landscape that often wreaks havoc on organizations.



Improved Sleep Based on Team Skills



91%

of respondents would sleep better at night if they knew their team had the right depth and breadth of skills to fight cyberattacks.

Which would have the biggest impact on sleep?

Knowing my team had the right depth and breadth of skills to fight cyberthreats

37%

A bigger security budget

28%

Improving our retention rates of skilled team members

21%

Having access to evergreen training resources like a cyber range

12%

Other

2%

04

Ability to keep pace with technological advancements is critical

50%

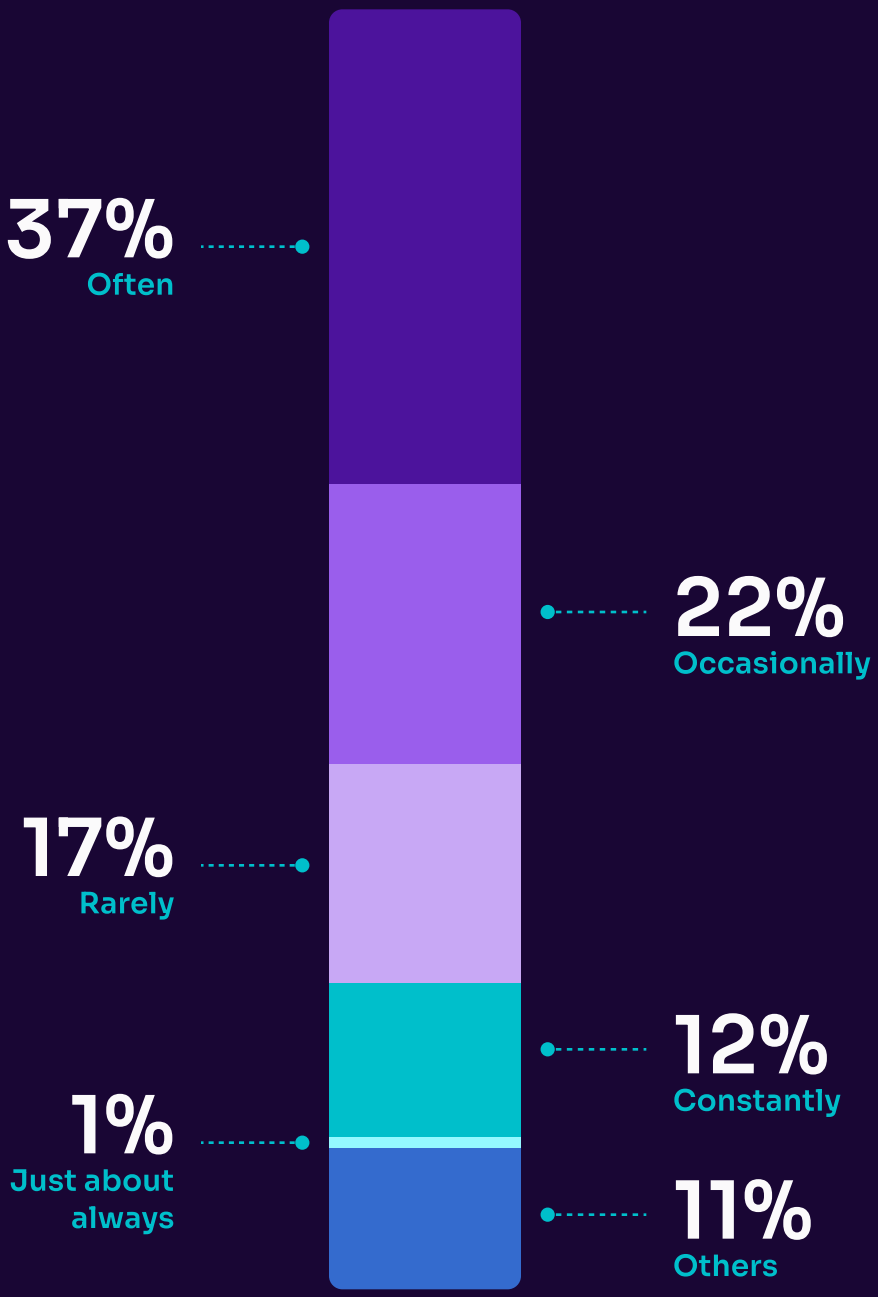
of respondents are frequently concerned about their team's ability to keep pace with threats

The challenge of keeping pace with the rapidly evolving threat landscape is a constant pressure for cybersecurity teams. The study reveals widespread concern among professionals about staying updated with technological advancements, a necessity for preventing serious organizational repercussions.

The risk of falling behind is significant: a major breach can harm a company's reputation, customer trust, and financial stability. This reality pressures teams to develop proactive strategies that address both current and future threats. Cybersecurity's role extends beyond information protection to securing the foundations of business operations, as organizations increasingly rely on these teams for uninterrupted, secure functioning.

Respondents also highlighted the need to invest in advanced technologies and develop and maintain skilled personnel. A balanced approach, merging technology with human expertise and continuous training, is essential for equipping teams with up-to-date skills and knowledge.

Frequency of concern of team's ability to stay up-to-date on threats



What worries you the most about emerging threats?

Keeping pace with technological advancements and their security implications

30%

Ensuring our organization's cybersecurity strategy remains aligned with evolving threats

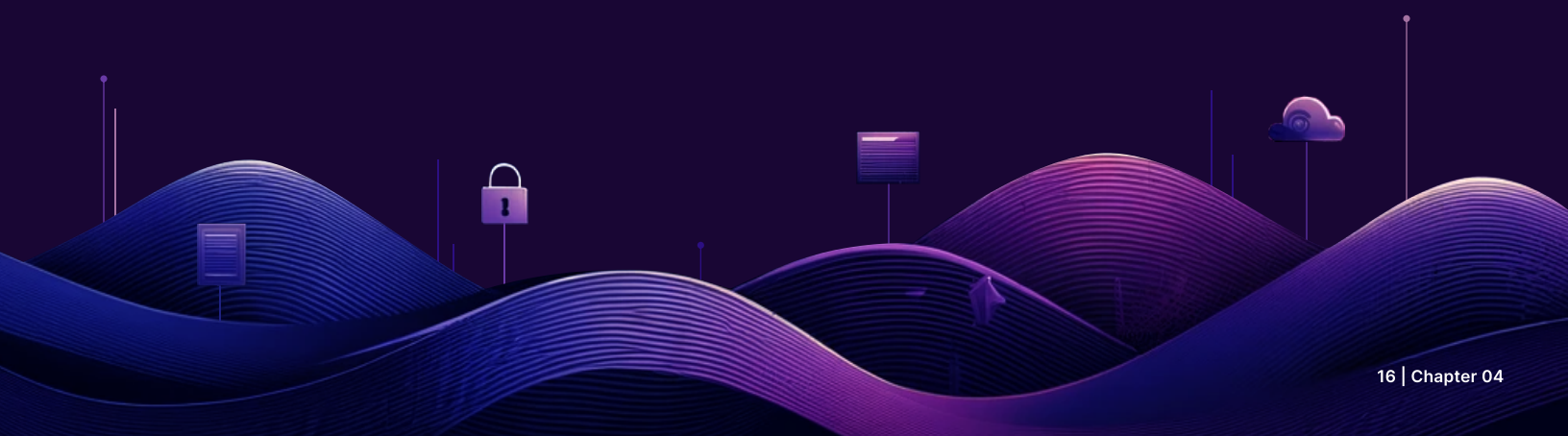
28%

Identifying and mitigating sophisticated cyberattacks

22%

Not knowing if our organization's cybersecurity skills are sufficient to prevent attackers from exploiting vulnerabilities

20%



05

Strength of a security team's skills is a concern

46%

of respondents are concerned about their ability to develop a strong security team

When **45.5%** of cybersecurity experts report that developing and maintaining a strong security team and **28.3%** report retaining top talent in a highly competitive market is a prominent concern, it highlights the importance of having skilled and competent professionals to manage and secure against increasingly sophisticated cyber threats. The emphasis on team development and talent retention reflects the recognition that the human element is as crucial as technological advancements and solutions in infosec.

This concern also signifies the challenges in finding and keeping individuals who possess the necessary skills and expertise in a market where demand for such talent far exceeds supply. The competition for qualified cybersecurity professionals suggests that organizations must train and develop their existing workforce while creating attractive career paths and work environments to retain these valuable employees.

Moreover, the focus on team strength and talent retention highlights the dynamic and evolving nature of cybersecurity threats. As these threats become more complex, the need for experienced and knowledgeable professionals who can adapt and respond effectively becomes more pressing. But, this doesn't mean that talent development and retention come without it's own set of challenges.

By investing in the development of their cybersecurity personnel, organizations can improve job satisfaction and retention rates. Skilled professionals are more likely to stay in an environment where they feel valued and where there are opportunities for growth and learning. This investment in training not only builds a more competent and confident team but also creates a positive cycle of attracting and retaining top talent in the field.

What aspect of talent causes the most worry?

06

Lack of hands-on training and skills development poses a concern

52%

Struggle to access hands-on skill development and therefore can't measure skills effectively

Limited access to hands-on practical experiences for skill development and the ability to measure skills for leadership have been reported as the most challenging elements of learning and development initiatives by our respondents. This finding suggests that while theoretical knowledge is important, there is a critical need for more practical, real-world training experiences. Cybersecurity professionals require opportunities to apply their learning in practical scenarios to effectively develop and hone their skills.

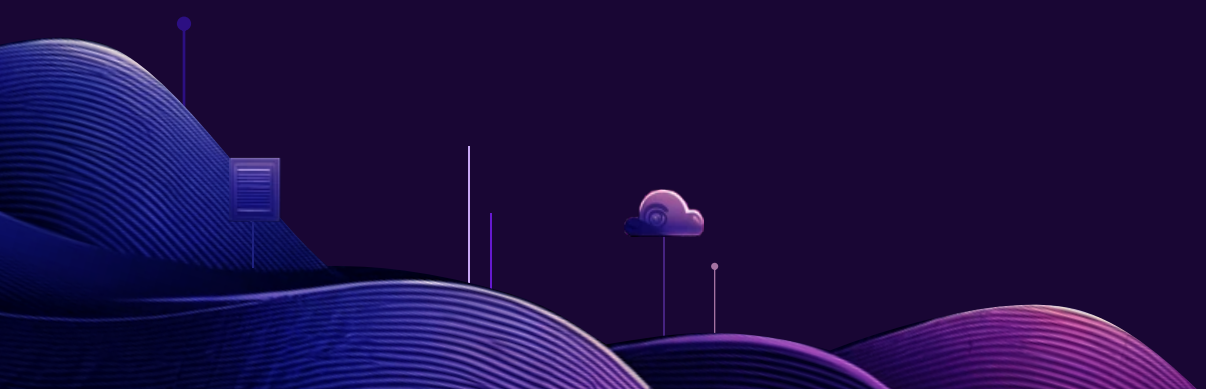
The challenge of proving these skills to leadership further highlights a disconnect between the training programs and the measurable outcomes expected by organizational leaders. It suggests that while professionals may be gaining knowledge, there is a lack of clear, quantifiable ways to demonstrate the effectiveness of this training to those in decision-making positions. This gap can lead to underestimation of the team's capabilities by leadership and may impact the allocation of resources and support for further training initiatives.

This scenario highlights the need for training programs that are not only comprehensive and practical but also include mechanisms for professionals to demonstrate their competence and the value of their skills. Incorporating hands-on exercises, simulations, and other practical components into training, along with clear metrics for evaluating skill proficiency, could address these challenges. Ensuring that training outcomes are visible and recognized by leadership is essential for the continued support and investment in these vital learning and development initiatives.

Furthermore, managers might think their teams have the right knowledge, but until something happens there is no way to test it, so having hands-on training makes sure they have the right depth and breadth of skill.

What aspect of Learning and Development is most challenging?

Limited access to hands-on practical experiences for skill development	28%
Quality of learning materials and instruction	25%
Ability to prove skills to leadership	24%
Access to cross-training	23%



Conclusion

The survey’s findings illuminate the multifaceted challenges that range from strategic operational decisions to the intricacies of managing a skilled cybersecurity workforce.

Significantly, the survey highlights the crucial role of continuous learning and skill development in addressing these challenges. In line with OffSec's commitment to ongoing training, the findings demonstrate the need for enhanced skill-building to strengthen organizational resilience and adaptability in the face of evolving cybersecurity landscapes.

Looking ahead, it is imperative for organizations to actively focus on enhancing the skill sets of their cybersecurity teams. This proactive approach, centered around regular training and upskilling, contributes significantly to the well-being of cybersecurity leaders. By ensuring that these training programs are in sync with the most recent trends and challenges in the cybersecurity field, leaders can feel more confident in their team's ability to handle emerging threats. Knowing their teams are well-prepared and adaptable eases the mental burden on leaders, allowing them to focus on strategic decision-making with greater peace of mind.

OffSec empowers individuals and organizations in the fight against cyber threats by providing essential cybersecurity skills and resources including offensive and defensive training.

As the leading provider of continuous professional and workforce development, training, and education for cybersecurity practitioners, OffSec is dedicated to closing the infosec talent gap. Employing a unique approach and practical, hands-on learning, OffSec equips organizations to train their teams on the most critical skills demanded in today's cybersecurity landscape with customized learning solutions. OffSec also funds and maintains Kali Linux, the leading operating system for penetration testing, ethical hacking, and network security assessments.

To get started with a free trial and start sleeping better, visit **learn.offsec.com/free-trial-request**

OffSec™
The Path to a Secure Future™