CISO

WORK/LIFE BALANCE

REPORT 2022

WHY SECURITY LEADERS QUIT THEIR JOBS

BLACKFOG™
Privacy. Security. Prevention.

BLACKFOG™

Privacy. Security. Prevention.

CISO JOB SECURITY

Work/Life Balance Report 2022

www.blackfog.com

CONTENTS

Cybersecurity leaders want to be more confident and proactive about their positions.

CYBERSECURITY: A CHALLENGING CAREER PATH

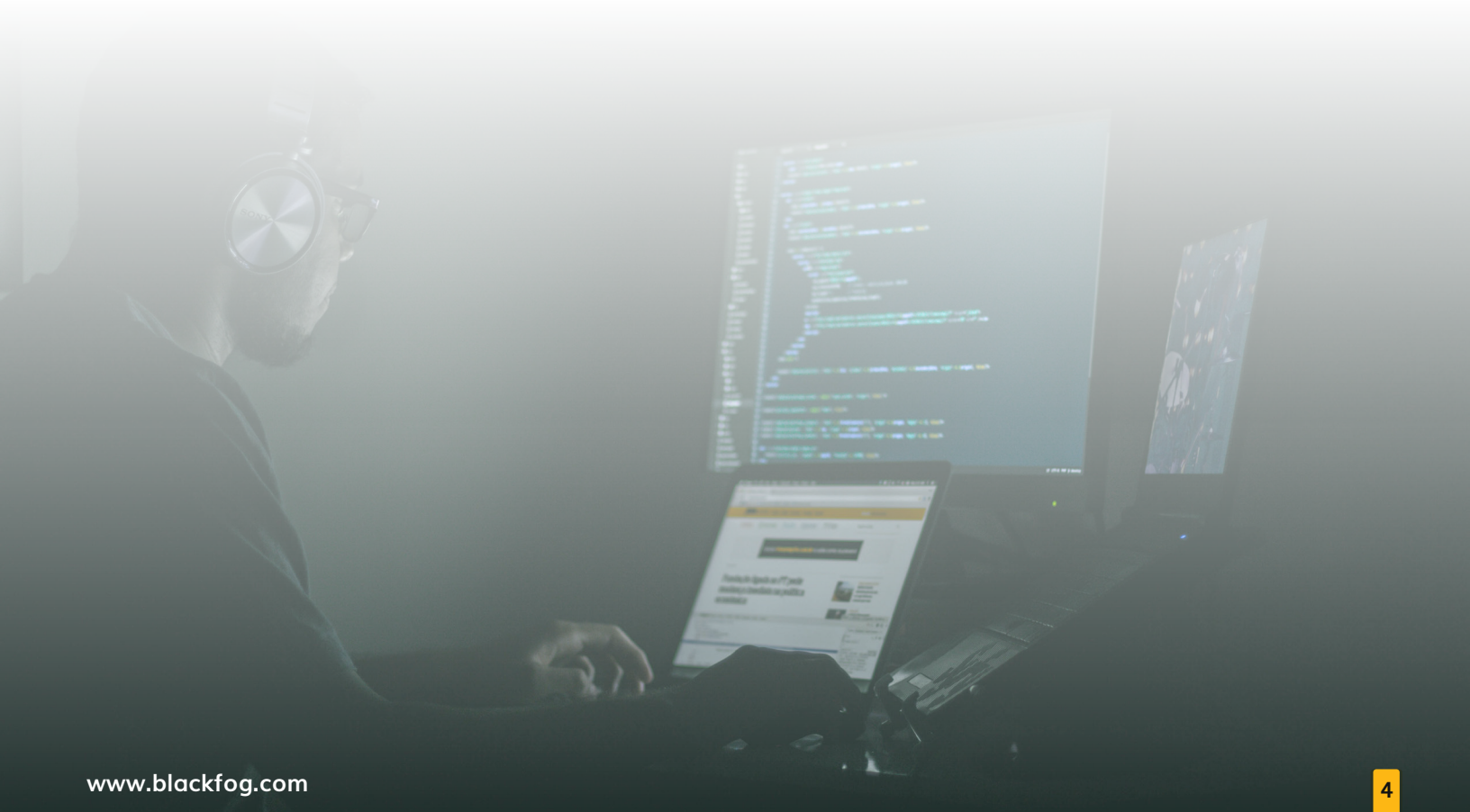
The Chief Information Security Officer (CISO) is one of the most vital roles in any organization. As an executive-level decision maker responsible for securing an organization's data, the CISO role is typically considered the final rung of the cybersecurity career ladder.

Like other C-suite leadership positions, the CISO role comes with an extraordinary degree of responsibility. The challenge of effectively managing risk while being accountable for the outcomes of uncertain decisions significantly impacts overall CISO job satisfaction and work/life balance.

The well-documented cybersecurity talent gap – projected to remain at 3.4 million open positions through 2023 – puts additional obstacles between organizations and robust security leadership staffing. The cybersecurity industry has an extremely high turnover rate, and that rate extends to cybersecurity leaders as well as analysts and managers.

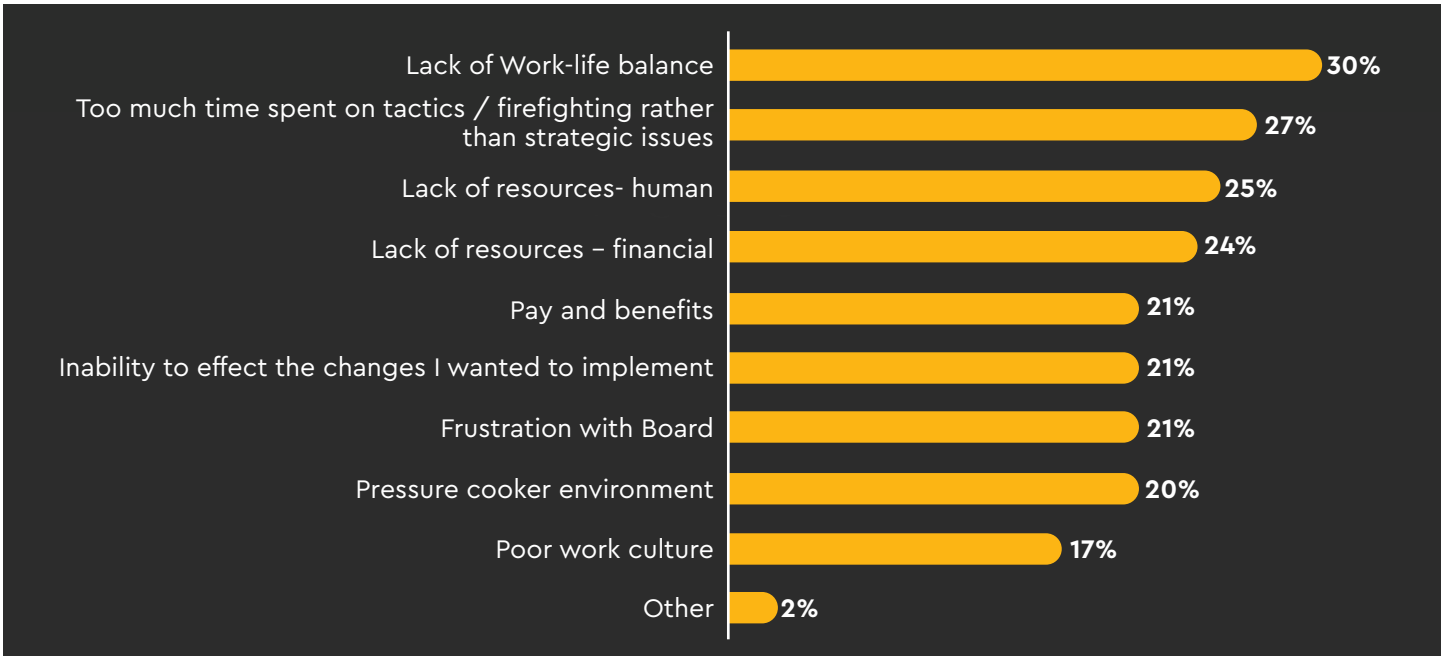
For organizations dealing with rapid changes in the threat landscape, cybersecurity leadership turnover is a significant risk. Organizations can't afford to replace cybersecurity leaders before they've had a chance to accomplish valuable strategic objectives.

BlackFog has conducted research into cybersecurity leader turnover rates and the factors that contribute to security leaders quitting their positions. These findings will help organizations go beyond compensation and consider valuable quality-of-life improvements that attract and retain top talent.



WORK/LIFE BALANCE:
THE MOST DISLIKED PART OF THE JOB

Almost one-third of CISOs and IT security leaders surveyed reported considering leaving their position in the next six months. Survey respondents cited nine different reasons behind their lack of job satisfaction:



Lack of work/life balance is the most disliked aspect of working as a cybersecurity leader. It is followed by a lack of balance between reactive and proactive security initiatives and a lack of resources, both human and financial.

Combined with board frustration and a high-pressure environment, these issues paint a compelling picture of a leadership role that assigns accountability to leaders without giving them the empowerment necessary to achieve long-term objectives.

Cybersecurity leaders are under intense pressure to protect the organization against increasingly sophisticated threats, yet they don't always have the resources necessary to adequately address structural vulnerabilities within the organization itself. As a result, they put in extra time and effort reacting to threats instead of proactively preventing them.

It's a well-known fact that cybercriminals routinely exploit work holidays to compromise systems when staff are distracted and offices are closed. Without the tools or technologies necessary to automate threat prevention, security leaders must be ready to drop everything and respond to emergencies at a moment's notice, and it many cases it's simply too late to prevent the attack.

PROTECTION AND INNOVATION: CORE DRIVERS FOR SECURITY PERFORMANCE

44% of respondents say their favorite aspect of cybersecurity leadership is taking on the role of a protector, keeping systems working optimally and securely. A close second (43%) report working alongside a team of like-minded individuals as the aspect of their work they most enjoy. The ability to innovate and stay ahead of the latest technological developments is an important driver of job satisfaction as well.

These findings point to a role whose value is driven both by internal motivations and external validation. Security leaders and IT decision makers want to feel like they are making a difference for the organization and be rewarded for their successes. At the same time, they want to know their organization supports them and is willing to invest in innovative technologies that make their job possible.

Organizations can improve their retention of capable cybersecurity leaders by emphasizing the importance of their roles and equipping them with the tools they need to achieve results. A company culture that prioritizes individual attribution and team performance, alongside technical innovation is likely to face fewer challenges when it comes to retaining top security talent.

CYBERSECURITY LEADERS KNOW THEIR REPUTATION IS ON THE LINE

Information security leadership drives its value from effective risk management. CISOs must develop strategies for mitigating the risks associated with cybercrime. Many of these risks are unknown, which puts a great deal of pressure on cybersecurity leaders to perform in uncertain environments.

41%

of newly hired cybersecurity leaders left a previous leadership role due to a cyberattack or data breach. Cybersecurity leaders are deeply aware of how their organization's cyber resilience reflects on their performance and reputation.

44%

say they enjoy being a protector in their role the most. Being looked upon as a credible authority is important for cybersecurity leaders.

27%

enjoy that the role is risk focused. Most cybersecurity leaders see risk as a threat to their reputation, and by extension their careers.

50%

have been prevented from adopting a new cybersecurity solution due to integration challenges. Executive buy-in is of critical importance to IT decision-makers who want to improve security performance at their organizations.

From here, it stands to reason that cybersecurity leaders who feel overworked (due to a work/life imbalance), or under-equipped (due to over-emphasis on reactive security tasks) are the ones least likely to put their reputation on the line for their employers.

Cybersecurity leaders who aren't given the resources they need to accomplish their goals are more likely to feel trapped into assuming responsibility for cyberattacks and breaches they feel they could have prevented. For them, finding a new position could be a career saving move.

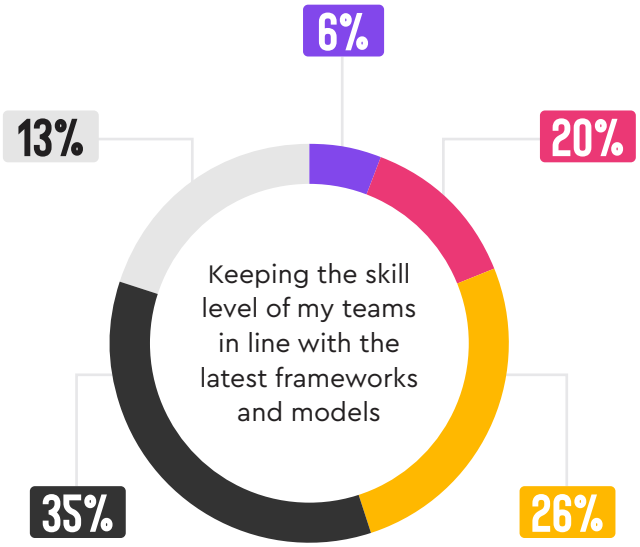
THE FIRST SIX MONTHS ARE CRITICAL

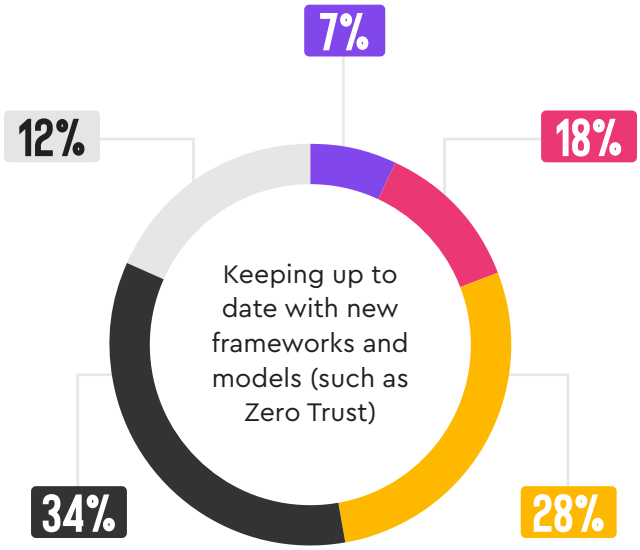
Over a third of survey respondents had been employed at their current organization as IT decision makers for more than four years. More than 40% have occupied their current role for between one and three years.

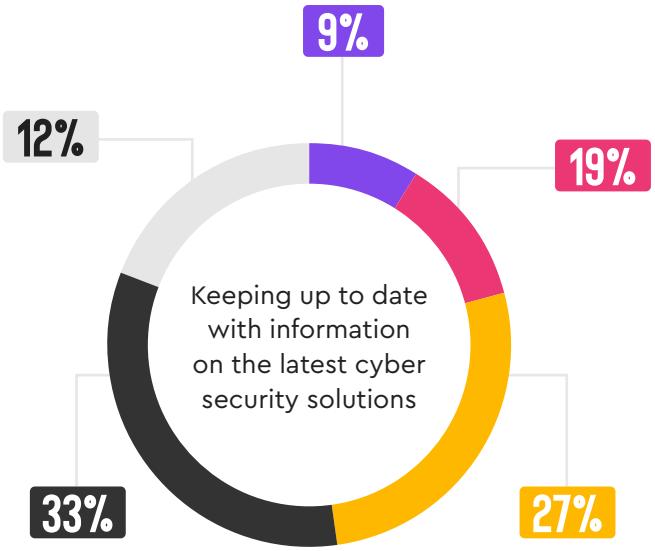
64% of survey respondents reported completely accomplishing their personal job priority within the first six months of starting their cybersecurity leadership role.

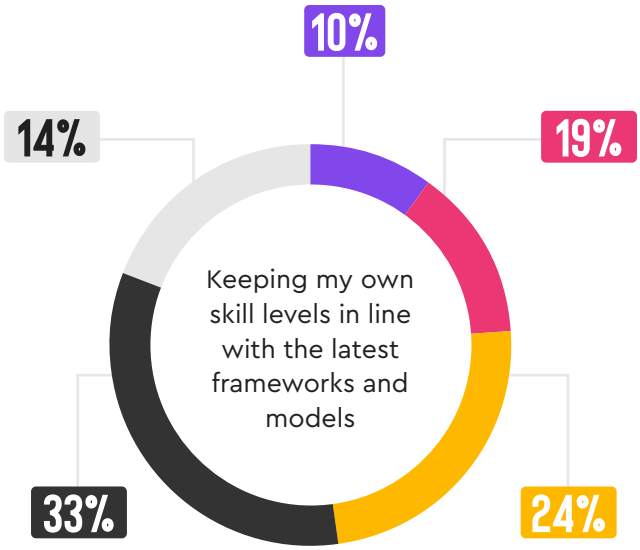
The three most common objectives include developing successful relationships with stakeholders, building out a security team, and securing additional budget for implementing security technology.

At the same time, more than half of respondents said that keeping the skill level of their team in line with the latest frameworks and models is their biggest long-term challenge.

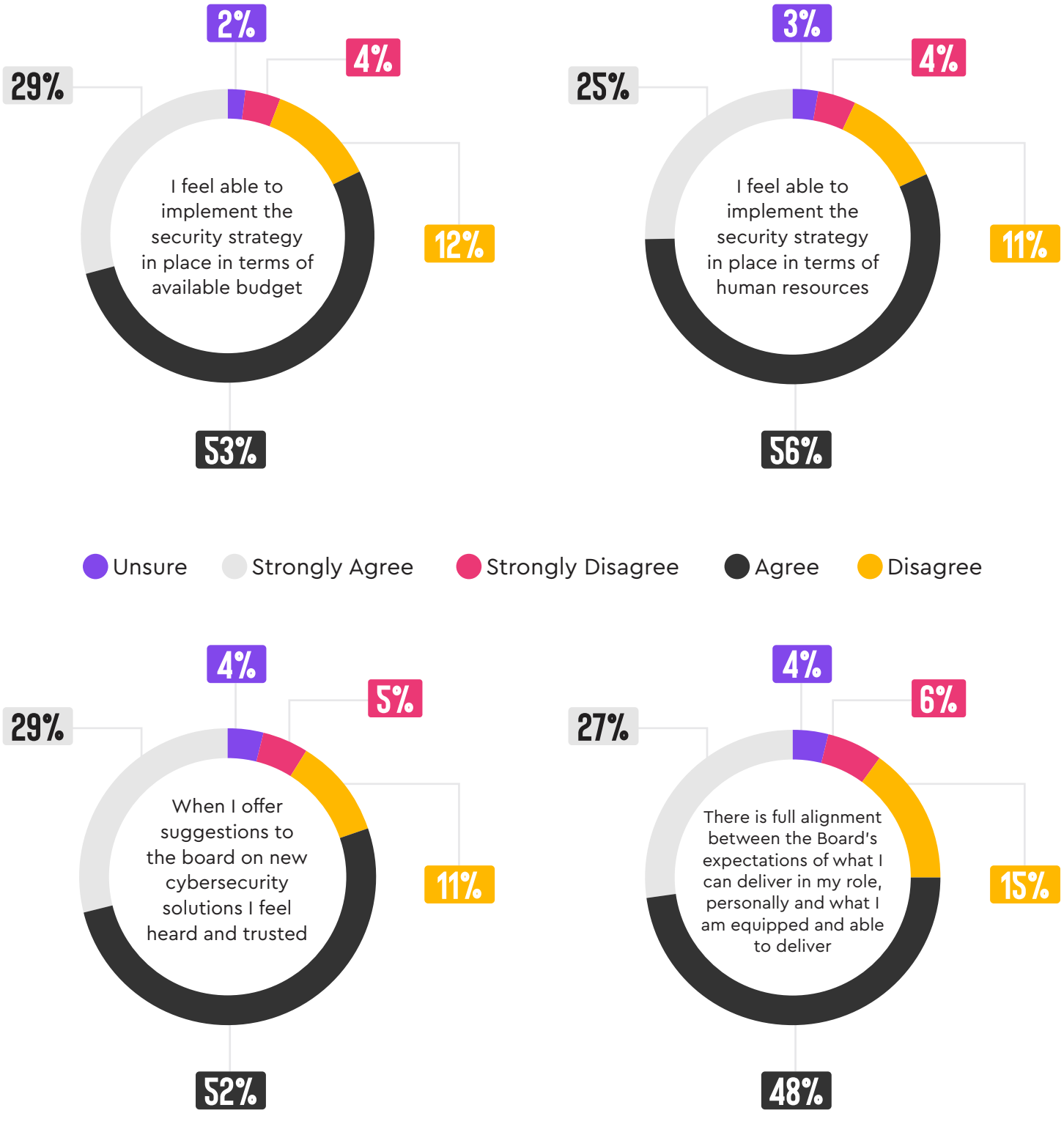








25% of respondents report not achieving full alignment between the board's expectations of what they can deliver and the resources they were equipped with.



These findings suggest that long-term leadership performance depends crucially on the success of the first six months leaders spend in that role.

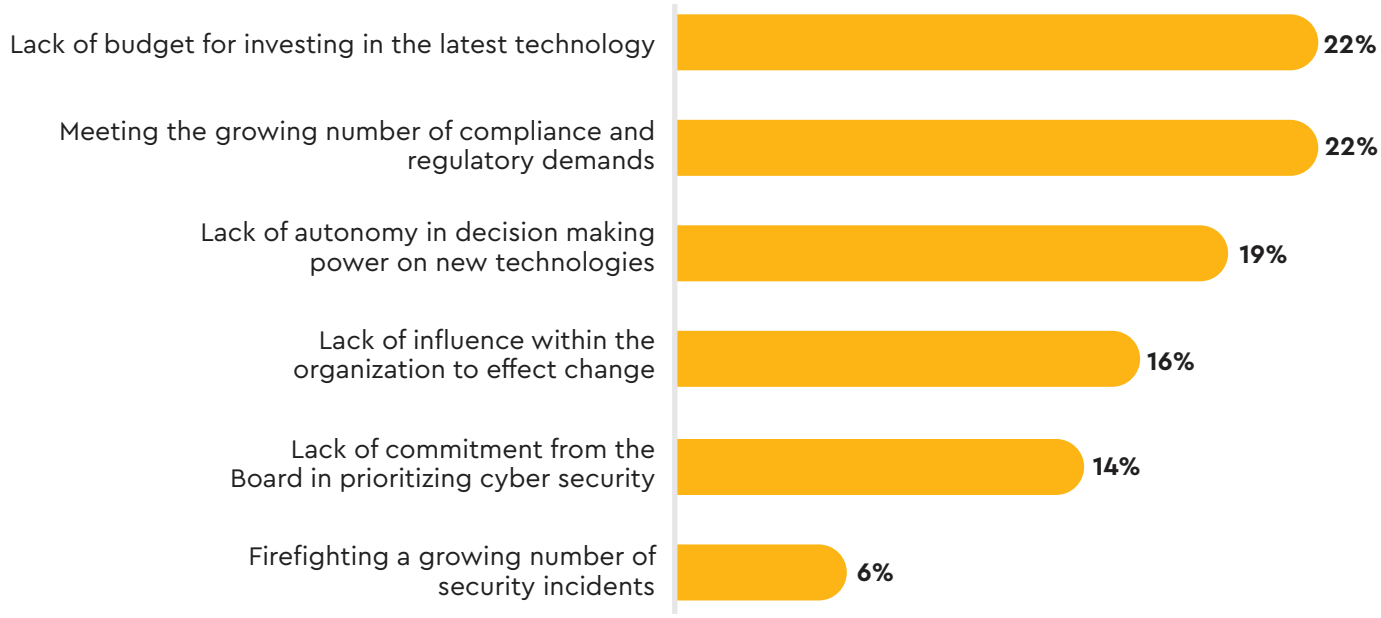
Cybersecurity leaders who obtain stakeholder buy-in for technology investments, build successful security operations teams, and secure the capital necessary to fund these investments within six months, appear far better-equipped to handle the stress of managing cybercrime risks in a complex IT environment.

If cybersecurity leaders and IT decision-makers don't achieve those goals, they may not feel empowered to make meaningful changes to the organization's security posture. This puts them at greater risk of developing a work/life imbalance and spending too much of their time on reactive IT processes instead of high-impact strategy. From that point, the risk of turnover rises significantly.

UNDERINVESTMENT AND COMPLIANCE CHALLENGES: TOP REASONS IT DECISION MAKERS LEAVE SECURITY ROLES

22% of respondents reported they would consider leaving their current role due to a lack of budget for investing in new technology, or the struggle of meeting compliance and regulatory demands.

For mid-sized companies with 500–999 employees, 22% of respondents claimed they would consider leaving their current role due to lack of commitment from the board in prioritizing cybersecurity.



These issues speak to the challenges that compel cybersecurity leaders to seek employment opportunities outside their current organization. Since they are keen to improve their work/life balance and protect their professional reputation, they place great importance on organizations willing to invest in new technologies.

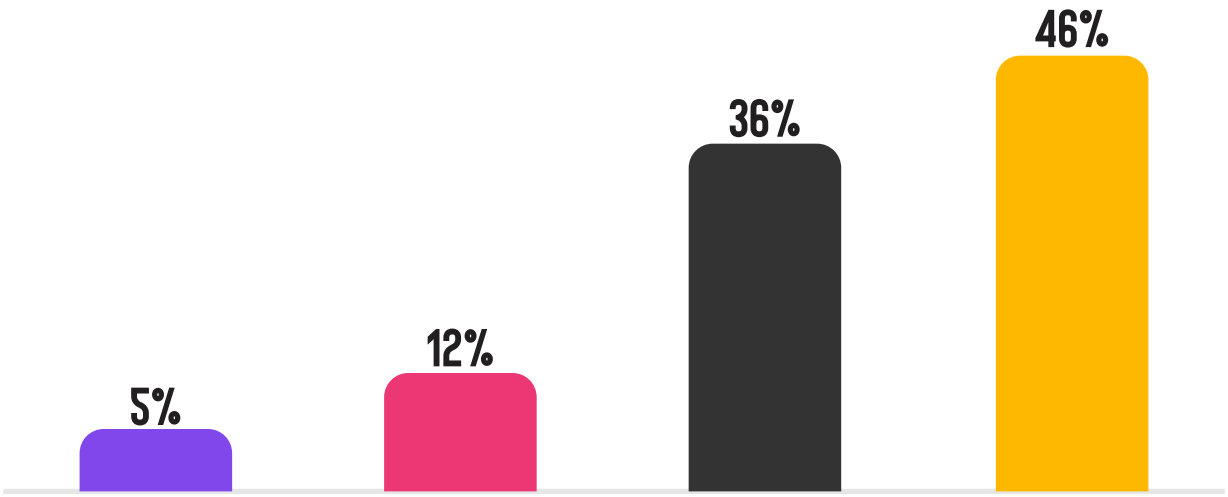
New technologies can provide visibility, scalability, and automation that streamlines compliance while reducing the organization's overall risk profile. Cybersecurity leaders and IT decision makers prefer working for organizations that are willing to deploy these technologies and may interpret the refusal to do so as a lack of commitment on the Board's behalf.

PREVENTION-BASED TECHNOLOGIES DRIVE RETENTION AND PERFORMANCE

Security leaders are well aware of the need to adopt cost-effective solutions that meet strategic security goals. Budget limitations, implementation restrictions, and talent shortages make many technologies and approaches economically unfeasible. This is especially true of advanced detection and response solutions that leverage emerging technologies like machine learning and AI.

Under increasing pressure to deliver more with less, stakeholders, executives, and security leaders are looking beyond detection-based security methodologies and towards prevention-based systems that are more robust and cost-effective.

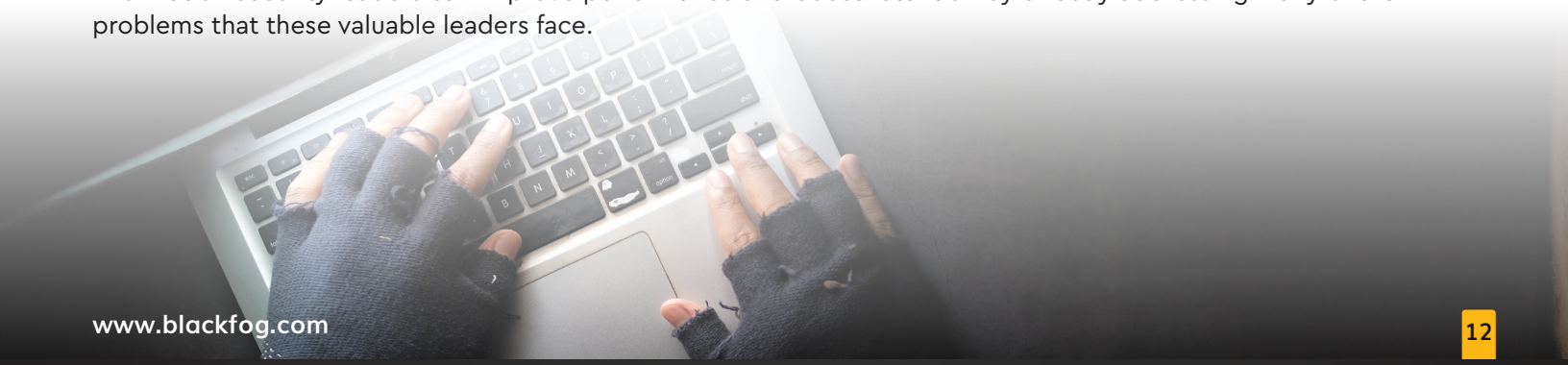
82% of cybersecurity and IT decision-makers are familiar with Data Loss Prevention and Anti Data Exfiltration (ADX) technologies, though only 46% have kept up with the latest developments in the market.



Of the 46% of security leaders who report keeping up with the latest ADX technologies, 55% are based in the United States and 38% are based in the United Kingdom. Just under 60% report working for organizations with less than 1000 employees, while 36% work for enterprises with 1000+ employees.

This data suggests that cybersecurity leaders are broadly aware of the benefits that prevention based technologies like ADX have to offer. However, a smaller number of security decision-makers know the full capabilities of the latest technologies.

Stakeholders, board members, and cybersecurity leaders can work together to deploy prevention-based security solutions that are robust, economical, and scalable. Putting powerful technologies in the hands of capable information security leaders can improve performance and boost retention by directly addressing many of the problems that these valuable leaders face.



BRING PEACE OF MIND TO THE CYBERSECURITY LEADERSHIP ROLE

The security operations center is a busy, high-stress environment. Information security personnel who feel supported and equipped by their organizations are able to drive the value of security processes with lower turnover and less burnout.

Organizations that invest in prevention-based security technologies like ADX can dramatically improve the quality of life their staff experience while tackling some of the world's most sophisticated threats.

ADX is a technique, pioneered by BlackFog that prevents the unauthorized removal of data from a device or network. As a robust prevention-based solution, it goes beyond first and second generation technologies like Antivirus and EDR/XDR and focusses on preventing data exfiltration.

Cybersecurity leaders want to know they have a robust, multi-layered security system protecting the organizations critical data. Cost-effective tools like ADX provide the peace of mind that few other security technologies can offer.

BlackFog provides ADX protection to organizations that prioritize building cyber resilience while maximizing the value of every member of the security team. Find out how BlackFog's technology can help you achieve operational security excellence.

METHODOLOGY

The results from this survey are from an online survey Sapio Research fielded on behalf of BlackFog with IT Cybersecurity Leaders and Decision Makers in companies of over 500 employees across the UK (200) and US (205). The research was conducted in August and September 2022.

www.blackfog.com