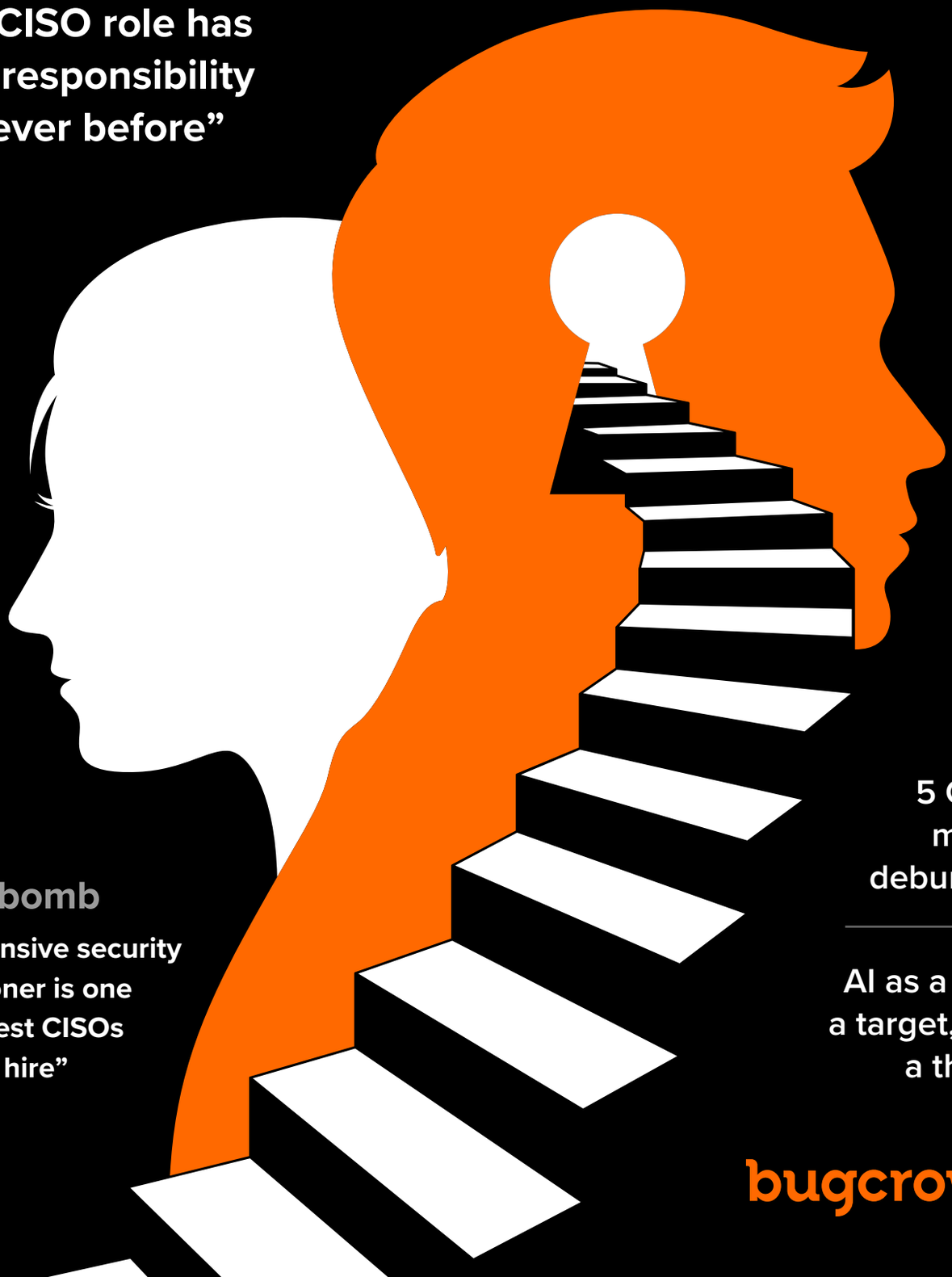
INSIDE THE MIND OF A CISO 2024

The Evolving Roles of Security Leaders

Real talk with Nick McKenzie...

“The CISO role has more responsibility than ever before”



Truth bomb

“An offensive security practitioner is one of the best CISOs you can hire”

5 CISO myths debunked

AI as a tool, a target, and a threat

bugcrowd

Table of Contents

Report Highlights 3

SPOTLIGHT

Letter from the editor: Nick McKenzie 4

The state of security 5

The cybersecurity hiring landscape 9

INFOGRAPHIC

Five CISO myths 11

The Venn diagram of hackers & security leaders 12

SPOTLIGHT

The CISO's approach to AI as a tool, target, and threat 16

Meet Ross McKerchar CISO at Sophos 20

Advice for aspiring CISOs 22

Conclusion 25

Report Highlights

This edition of *Inside the Mind of a CISO* analyzed **209 survey responses** from security leaders across the globe. It defines **"security leaders"** as anyone with one of the following titles—CISO, CIO, CTO, Head of Security, or VP of Security. The survey was commissioned by Bugcrowd and conducted by Quest Mindshare. Respondents represent security leaders from North America, South America, Europe, Asia, Australia, and Africa; all were fully employed at organizations of varying sizes.

89%
believe there are more threats and they are more serious.

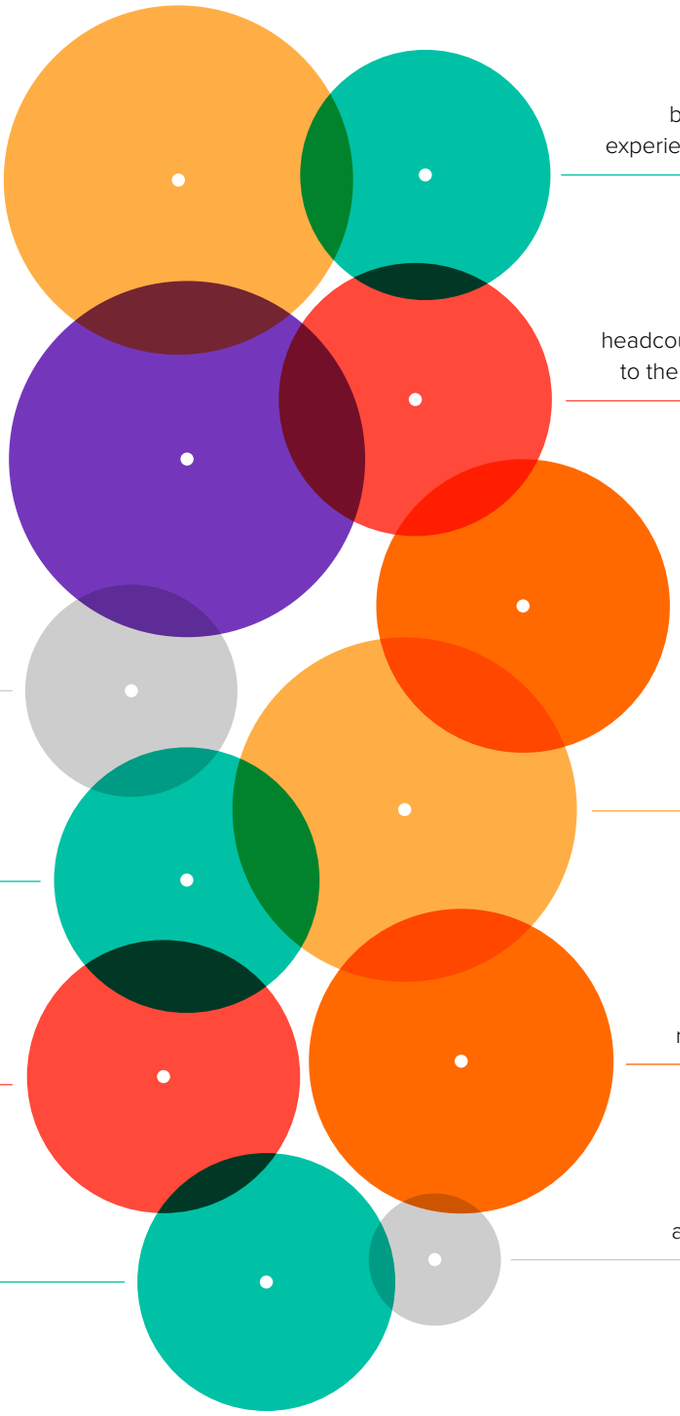
91%
believe AI already outperforms security professionals or will in the future.

58%
believe that the risks associated with AI outweigh its potential.

69%
believe most organizations are not proactive about security.

70%
use crowdsourced security testing for AI defense.

68%
believe the cybersecurity skills gap is getting smaller.



66%
believe security professionals experience a higher rate of burnout.

70%
plan to reduce security team headcount in the next five years due to the adoption of AI technologies.

75%
have personal experience with ethical hacking.

88%
believe security roles are becoming more difficult.

76%
believe the AI threat landscape is evolving too rapidly to adequately secure.

31%
prioritize building a "security brand" for competitive advantage over other factors.

An introduction from our CI&SO Nick McKenzie

The CISO title may be one of the biggest, flashiest security titles out there, but it's also one of the most nuanced roles in the C-suite.

The CISO role is evolving. The path to becoming a CISO, expectations of the role, and the path after the role is earned are varied.

Cybersecurity has so many different disciplines and potential roles, from risk and compliance to identity access management, engineering and architecture, training and awareness, and of course a variety of operational roles to testing/offensive security roles. Depending on the size of the organization, there are also the roles embedded in the business lines themselves or in other areas that are supporting cyber as a function or contributing to its mandate.

The CISO role is so nuanced because security leaders often have to move horizontally earlier in their careers to learn as many of these **unique disciplines** as possible. They have to grow into the role with experience. Personally, I worked in excess of 10 different security verticals over 20 years before stepping into a CISO role. Every time I moved, I obtained **invaluable experience** from seeing the nooks and crannies of different security processes in isolation or being entwined with and supporting the business processes.

This report found that security leaders have a **wide range of experience**. Some have master's degrees, others have worked in many different roles; some have many years of job experience, others were once ethical hackers

> **The point is: the modern CISO can't be defined by one quality or achievement. The backgrounds of security leaders are just as varied and nuanced as the position itself.**

This report explores the CISO position from several different perspectives. It looks at beliefs and priorities, hiring challenges, and of course, AI adoption. It dives into data and interviews, outlining trends, best practices, and actionable advice for security leaders.

This research is especially timely because the actual CISO role is seeing more discussion. Traditionally, CISOs report to the CIO. However, given the current risk landscape and the increasing need to **prioritize security first over operational resilience,** we're seeing a shift where many CISOs are stepping into CIO roles, either in a full-time capacity or under a new title (CI&SO or some varying derivative). Another trend is CISOs branching up into a CSO-type role, which encapsulates cyber plus physical security, fraud, and other horizontal areas. By combining these processes and neighboring risk vertices under a CSO, synergies can be harvested by having an expanded reach across interconnected business areas.

> **With these shifts and the common joining of the CISO title with other types of roles, the CISO has both more opportunity and responsibility than ever before.**

More CISOs are also **joining boards** to provide teams with better oversight with security strategy and ongoing matters. Given the number of new directives across the globe, boards need more cyber experience among their members in response and/or peering with the CIO's and reporting directly into the CEO. There are now more direct appointments to boards of CISOs who have been in the field or have a strong cybersecurity background. This isn't just a box-ticking exercise—there is a growing desire to empower a board with better security insights into current threats impacting them whilst enabling the business in turn with strategic direction.

I believe that by understanding the ways CISOs across the globe are approaching common security pain points, we can collectively **build stronger programs** that outpace threat actors. *Inside the Mind of a CISO* really spotlights these initiatives, and I hope you find it as insightful as I did.

The state of security

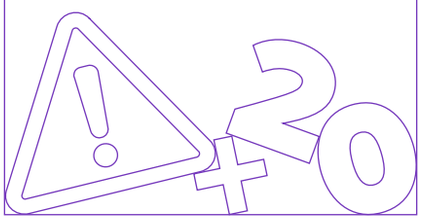
Dissecting the top priorities of CISOs

CISOs and security leaders work tirelessly to keep our data safe and our assets and infrastructure secure. These peers make up a diverse and dedicated group of individuals who bring a wealth of experience, knowledge, and skills to the table.

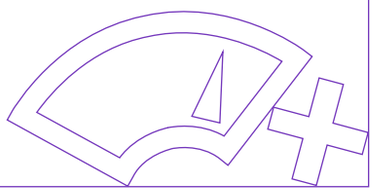
In the face of growing risks and heightened organizational demands, security leaders are feeling the heat. Cybersecurity is quickly becoming a **key competitive advantage** for firms, making security leaders' challenge clear: stay ahead of threat actors. This chapter delves into the insights, hurdles, and top priorities for security leaders in 2024.

Security leaders' perceptions of the threat landscape

88% believe there are more threats now than before 2020.



89% think that the threats are more serious now than before.



88% believe that security roles have become more difficult in the past four years.

Security leaders overwhelmingly agree that cyber threats are now more prevalent and serious than just four years ago! According to Accenture, an astonishing 97% of organizations have seen an increase in cyber threats since the beginning of 2022.

The world has changed a lot since the start of the decade. AI and other technological advancements have enabled threat actors to develop new and creative ways to carry out their digital attacks.

Remote work has become the new norm. While people were learning to navigate this new digital landscape, threat actors were working hard to spot opportunities.

Remote environments are inherently less secure. Their **larger attack** surfaces require the average person to understand the basics of security more than ever before. Threat actors target collaboration tools like Slack, Teams, OneDrive, and Google Drive, looking for any chance to sneak in and steal valuable data. Schools and universities have had a particularly tough time, with many of them diving into the digital world without proper safety nets, making the education sector one of the most attacked markets globally.

To stay one step ahead of the dangers, organizations must prioritize cybersecurity and work closely with security leaders to create strong defenses. Organizations must adopt measures like regularly updating software and systems, providing top-notch security training for employees, and establishing clear protocols for responding to incidents quickly and effectively.

Security leaders' top priorities

Building a "security brand" for competitive advantage — 30.5%

Building resilience to attacks — 20%

Avoiding breaches at all costs — 18%

Balancing risk against achieving business objectives — 17%

Developing a security culture — 14.5%

Gone are the days when security was just a checkbox for organizations. Security is no longer just a compliance requirement—it's a powerful competitive advantage.

Almost a third of these peers are prioritizing building a security brand to differentiate their organizations from their competition. That's right—they think it's even more important than avoiding breaches and creating an internal security culture.

This is a growing trend. CISOs and security leaders are accountable to their board of directors and are now responsible for delivering more tangible business results.

With global digitalization, security has become a hot topic among consumers and customers.

They want to know that organizations are keeping their data secure, and they're making choices based on their perceptions of brands' security consciousness. Organizations are catching on and want to send a clear message: **"We've got your back better than our competitors do!"**

Other security leaders see protecting their organization as their most important mission, with 20% prioritizing boosting resilience to attacks and another 18% focusing on avoiding breaches at all costs. These proactive security leaders know that cyberattacks are not a matter of **"if" but "when."** They believe they can create brands that speak for themselves by keeping their organizations safe and staying out of the headlines. No news can be good news when it comes to security!

No matter how your peers approach their security strategies, more organizations are realizing that strong security is the name of the game and a big competitive advantage. Going forward, we can expect to see security play a bigger role in **shaping business strategy.**

As security leaders continue to lead this charge, they're not just protecting data—they're redefining what it means to be a resilient, trustworthy, and successful organization in the digital age.

CISOs' perceptions of overall attitudes toward security

How many organizations do you believe understand their true risk of being breached?

Fewer than 10%	**10%**
10–25%	**30%**
20–50%	**31%**
50–75%	**26%**
75–100%	**4%**

How many organizations do you believe are truly proactive about security?

Fewer than 10%	**7%**
10–25%	**29%**
20–50%	**33%**
50–75%	**25%**
75–100%	**6%**

How many organizations are willing to sacrifice their customers' privacy or security to save money?

Fewer than 10%	**11%**
10–25%	**20%**
20–50%	**36%**
50–75%	**26%**
75–100%	**7%**

Are organizations ready for real threats? Security leaders aren't so sure.

When you ask security peers about the state of security among organizations, they'll tell you that many organizations need to up their game. A whopping 68% of security leaders believe that only half of the organizations or fewer have their acts together when it comes to **breach preparedness.**

So, what's behind this lack of preparedness? Many organizations are **reactive rather than proactive** when it comes to security. They deal with threats as they come instead of planning and implementing solid security measures ahead of time. Only 31% of security leaders believe that at least half of all organizations are proactive about their security. This lack of foresight can be likened to building a dam only after the floodwaters have begun to rise—not exactly the best timing!

The reasons why so many organizations struggle to be proactive and prepared are as varied as the threats themselves.

The rapid pace of change and the complexity of the cybersecurity landscape can be overwhelming.

Trouble hiring the right folks and navigating the ever-changing regulatory maze only adds to the headache.

Human error is another significant factor. Despite the advanced technology at our disposal, humans remain the weak link in the security chain.

Mistakes, oversights, and lack of proper training can all lead to vulnerabilities. According to Verizon, almost three-quarters of data breaches are the result of human error.

Leaders are also concerned that organizations will take **shortcuts** in their security. 89% of security leaders suspect that at least one in ten organizations is willing to sacrifice its customers' long-term privacy or security to save money in the short term, and about a third believe that over half of the organizations would throw their customers' trust out the window to save a few bucks. Not really the news we want to hear!

Ultimately, security leaders are not entirely convinced that organizations are doing enough to **proactively protect themselves** or adequately prepare for the inevitable security breaches. To bridge this gap, organizations must prioritize cybersecurity as a critical business function, invest in ongoing training and awareness programs, and incorporate security at every level of the organization. Only then can we hope to build a more resilient and secure digital future.

Cyber insurance premiums

CISOs want to demonstrate a proactive approach to security risk management to reduce insurance premiums.

Regulatory obligations

With regulatory obligations and government oversight of cybersecurity on the rise, CISOs need vendors who can provide solutions to these challenges.

Legal exposure

Gartner predicts that by 2027, two-thirds of Global 100 organizations will extend D&O insurance to CISOs due to personal legal exposure.

Security leaders' top concerns

What topics are coming up in conversations with CISOs and their peers?

We've analyzed conversations with our customers and market research partners to highlight some of the main trends and topics.

Burnout

50% of current CISOs will have changed jobs in the next year as a result of burnout.

Professional development

69% of top-third CISOs prioritize recurring professional development time.

Closing the skills gap with AI

Gartner predicts that by 2028, the adoption of Gen AI will close the hiring gap for entry-level skills.

Risk vs. compliance

CISOs are taking a risk-driven approach to security in addition to ticking compliance boxes.

Outcomes

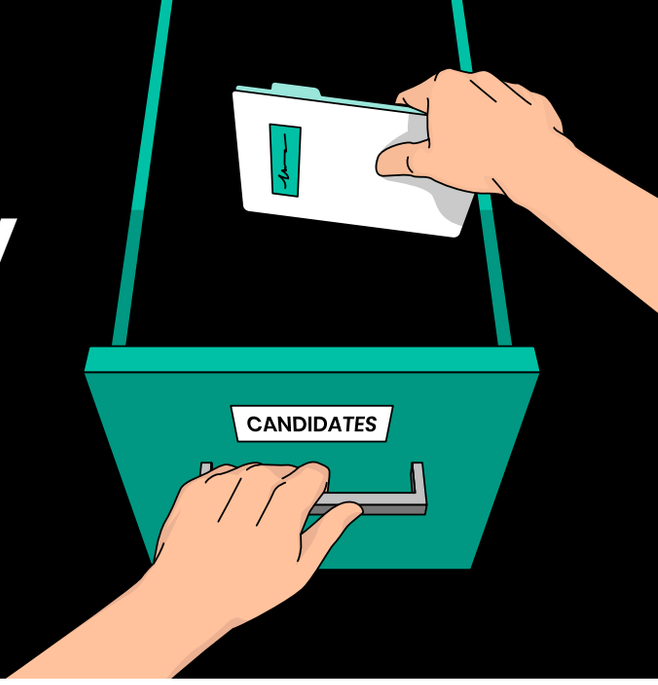
Instead of approaching solutions through the lens of security silos and products, CISOs are focusing on outcomes.

SOURCES

– Gartner, The Key Drivers of CISO Effectiveness in 2024
– Gartner, The Top Predictions of Cybersecurity for 2024
– https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends
– https://ww1.bugcrowd.com/forrester-tei/

The cybersecurity hiring landscape

Is the cybersecurity skills gap evolving with the times?



For many CISOs and security leaders, hiring is the bane of their existence. Many teams struggle to find suitable candidates to fill cybersecurity roles, often citing the famous **"cybersecurity skills gap."**

An open position will receive hundreds of applications, but few applicants will be truly qualified. This article looks at how the current job market is evolving.

Cybersecurity Skills Gap

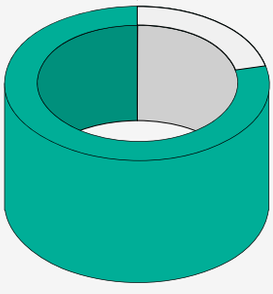
[Cy•ber•se•cu•ri•ty • skills • gap]
Noun

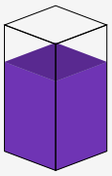
The mismatch between the skills employers require in cybersecurity professions and the qualifications possessed by potential candidates.

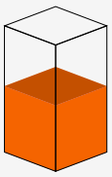
Hiring potential of cybersecurity teams

The hiring landscape remains highly competitive, with the majority of organizations currently recruiting for open roles. This phenomenon is prevalent across organizations of all sizes.

Most organizations see the skills gap as hindering their hiring efforts. Compounding this, over half of teams consider themselves understaffed, which puts **strain on existing employees** and amplifies the urgency to onboard qualified new hires.



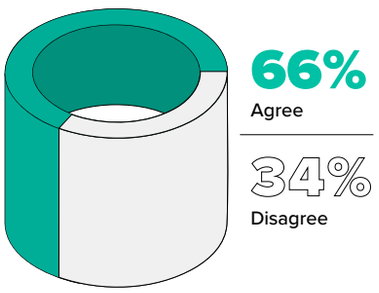




Cybersecurity is a relatively new field and has evolved quickly over the past five years. Looking for candidates with many years of relevant experience can therefore be difficult, both at the junior and senior levels. The primary problems stem from **skills matching and the pipeline,** not the demand.

Do cybersecurity professionals experience burnout at a higher rate?

Another compounding factor is the burnout rate, which is high: 66% of those we surveyed agree that the burnout rate for cybersecurity professionals is higher than for other professionals across different organizational sizes and regions.



To address the skills mismatch and increasingly under-resourced and over-burdened teams, there is a need to invest in targeted education and foster an early interest in cybersecurity. Generating a **consistent pipeline for hiring** is a common goal. While many individuals often pursue **certifications,** their real-world value is a topic of debate.

Employers are increasingly prioritizing **practical experience** and demonstrable skills over certifications alone. Aspiring cybersecurity professionals should therefore focus on acquiring hands-on experience to develop the skills that employers seek.

Burnout

[Burn • out] *Noun*

Mental collapse caused by overwork or stress. Burnout is linked to higher rates of errors and safety issues and interferes with innovation, leadership development, and effective teaming.

For those experiencing burnout, check out the Stress and Resilience Institute's Burnout Resource Center.

The cybersecurity skills gap in the age of AI

To be frank, the numerous articles on the cybersecurity skills gap have not offered new insights in a long time. The subgenre needs a refresh, and the changes brought about by AI are the perfect opportunity to give the topic a second look.

Despite economic uncertainties and fluctuations in the job market, the cybersecurity job market appears largely insulated. The threat landscape is constantly evolving, as are the types of assets requiring protection. Positive hiring trends suggest that the talent pool is varied and increasing in quality. However, the persistent shortage of qualified candidates underscores the need for investment in workforce development.

AI is poised to play a significant role in the future of cybersecurity employment.

On the one hand, AI tools may aid in threat detection and **improve employee productivity** by streamlining information access to multiple systems. On the other hand, AI can be used to create more effective cyber scams. AI has already had a drastic effect on the workforce: 23% of respondents (19% of small teams, 33% of medium teams, and 18% of large teams) have reduced their security headcounts with the adoption of AI technologies. The rest are not far behind, with 28% planning to follow suit in the next 1–2 years and 20% in the next 3–5 years.

The remaining 29% of organizations don't currently think they will change their headcounts in the near future. Security leaders must adapt to these AI-driven changes and ensure that their teams have the **necessary skills.**

The cybersecurity job market is **complex and evolving,** as the field itself is changing rapidly. While there is a perennial demand for cybersecurity professionals, candidates must be up to date with the **latest trends.**

An overall focus on targeted education, practical experience, and adaptability to emerging technologies like AI is crucial. As the cybersecurity landscape continues to evolve, professionals and organizations must remain ready to adapt.

5 CISO MYTHS

MYTH #1

CISOs are opposed to ethical hacking

73% of security leaders view ethical hacking in a favorable light, and 75% of them have actually engaged in it themselves.

MYTH #2

CISOs are mainly management professionals

76% of CISOs have worked in 3 to 10 cybersecurity roles, and 82% of CISOs have either a bachelor's or master's degree in cybersecurity.

MYTH #3

Only large companies need CISOs

20% of CISOs lead teams with fewer than 10 members, showing that even smaller teams benefit from the high-level strategizing of a CISO.

MYTH #4

CISOs are unprepared for AI

95% of CISOs are already implementing AI-based defensive measures, namely crowdsourced testing, pen testing, and color teaming.

MYTH #5

CISOs all believe in the value of AI

58% of CISOs believe that the risks of AI outweigh its potential benefits, while 42% believe in the potential of AI, indicating that there is no consensus on this issue.

The Venn diagram between hackers and security leaders

A look at the “Offensive Security CISO”

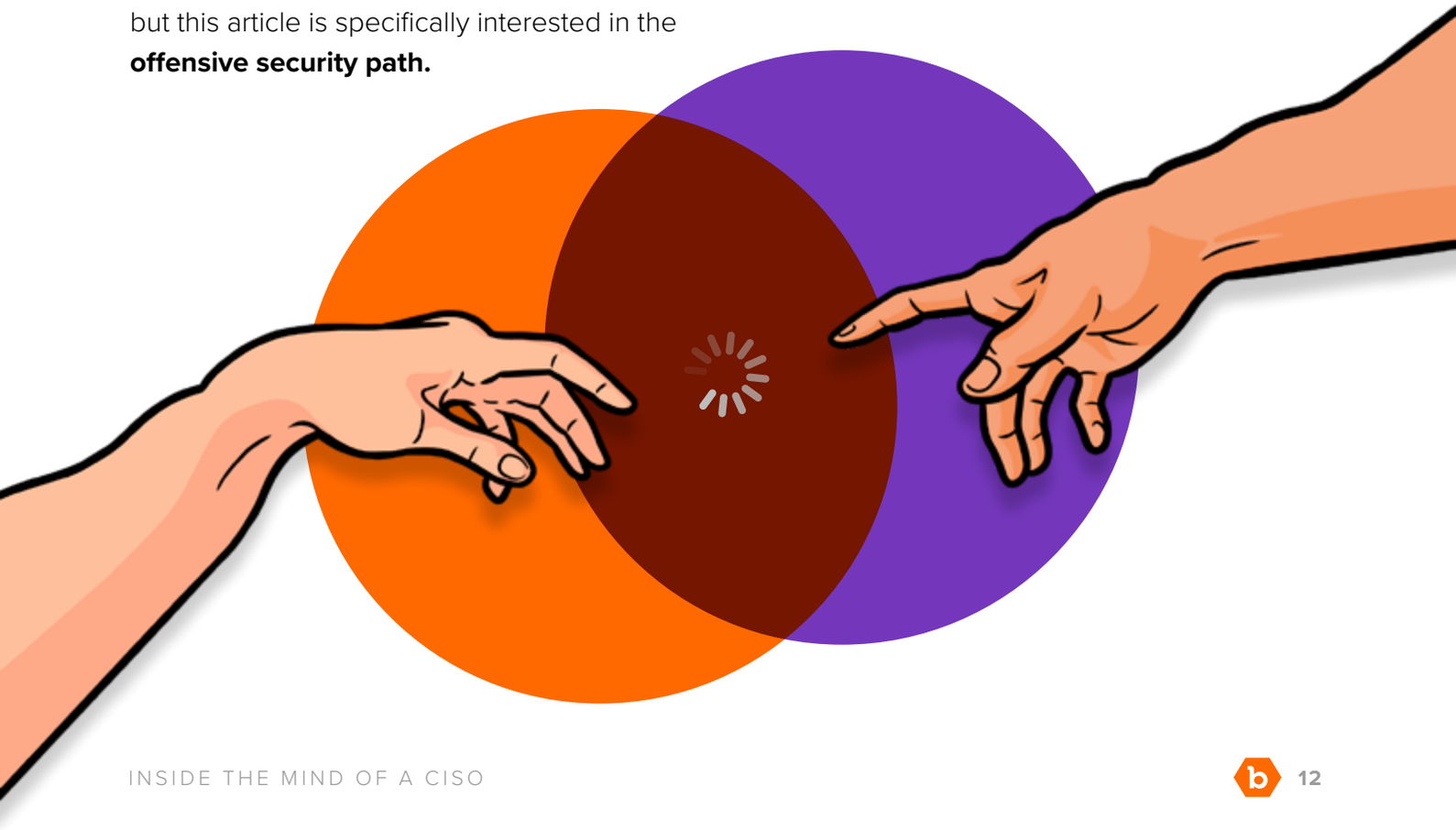
One of the most striking pieces of information revealed by the data presented in this report is the variety of ways security professionals work their way up into security roles, ultimately landing the coveted “CISO” title.

No CISO is identical to another—they have a wide range of experience, likely different educational backgrounds, and extensive technical know-how. Beyond just backgrounds, the CISO role itself can be somewhat of a moving target, as it’s constantly evolving.

There are many different paths a security professional can take to become a CISO, but this article is specifically interested in the **offensive security path.**

DEFINING OFFENSIVE SECURITY

Offensive security is a form of proactive security that comprises the constant process of identifying and fixing exploits before attackers can take advantage of them. Offensive security tactics include pen testing, red/purple teaming, bug bounty engagements, and vulnerability disclosure programs (VDPs). Offensive security should be part of a larger risk management strategy.



The crossover between hackers and CISOs

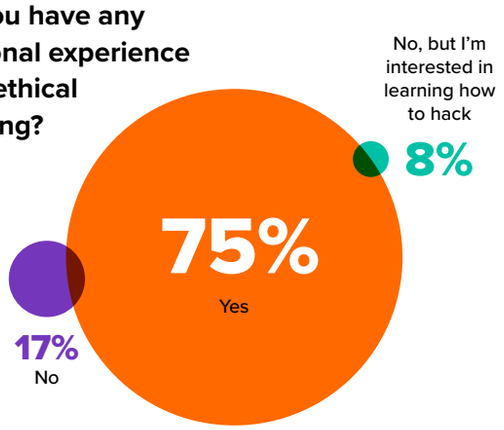
It wasn't that long ago when hacking was a ticket straight to the slammer.

> **Now, hackers have an incredible number of career opportunities thanks to their technical skills.**

There is a misconception that hackers and security leaders are two separate entities. In reality, they are two parts of a Venn diagram with a large amount of overlap. *Inside the Mind of a Hacker* found that **77% of hackers work full-time roles in security or IT.** Chances are, every organization has security team members who hack or pen test on the side for some extra cash.

It isn't just the junior employees who are hacking on the side—it's the leaders too.

Do you have any personal experience with ethical hacking?



Let's take a moment to put this into perspective. For so long, hacking has been stereotyped by the media and portrayed as a criminal activity reserved for evil entities wearing hoodies and occupying dark basements. The data shows that this simply isn't true—**hackers and security leaders are often one and the same.**

> **Hackers are occupying boardrooms, leading massive teams, and building cohesive security strategies.**

Interestingly enough, even though this crossover exists, some security leaders remain hesitant to embrace working with hackers. At Bugcrowd, we call this **Crowd Fear.**

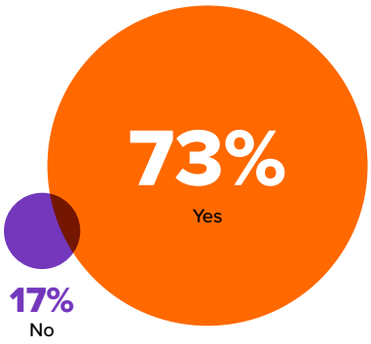
CROWD FEAR, DEMYSTIFIED

At Bugcrowd, we call the hesitancy to embrace working with hackers "Crowd Fear." Crowd Fear comes from the misconception that working with hackers exposes an organization to more risk. Unlike threat actors, hackers are fueled by a desire to help combat cyberattacks using their technical skills and expertise, and they don't operate with any malicious intentions. 75% of hackers identify non-financial factors as their main motivators to hack. They hack to develop personally, challenge themselves, seek excitement, and give back to the community.

It's important to note that even if you choose not to give hackers access to your assets and infrastructure for testing purposes, it's impossible to extend the same rules to threat actors. Threat actors aren't asking for permission. Working with the hacking community doesn't increase risk; it simply increases the number of eyes testing your assets and keeping your organization protected.

The number of security leaders who view hackers in a favorable light continues to grow. To those security leaders still hesitating to embrace the Crowd, it's important to take into account the fact that most of your peers and many members of your team have previously hacked or are currently hacking on the side. The skills that come from hacking are a powerful tool in a CISO's toolbox.

Do you view ethical hackers in a favorable light?



How one CISO hacked his way to the top

To learn more about how hacking and offensive security experience as a whole can positively impact a security leader's strategy, we sat down with former CISO and current CEO at Arcanum Information Security, **Jason Haddix.**

Haddix has been in security and IT for almost two decades. He started as an IT generalist at Citrix before shifting to pen testing. At HP Fortify, Haddix directed a team of over 150 pentesters, all while actively pen testing and hacking as part of bug bounty engagements on the Bugcrowd Platform. He eventually joined the team at Bugcrowd full time, where he led the triage team and became VP of Hacker Growth. Following his time at Bugcrowd, he worked as the CISO of Ubisoft, and later, the CISO of BuddoBot. He is now a part-time field CISO at Flare and is the founder and CEO of Arcanum Information Security.

Having been on the offensive side, I know the tips and tricks that attackers use to break into an organization.

"Coming up from an offensive security background really shapes how I prioritize risk in an organization. Having been on the offensive side, I know the tips and tricks that attackers use to break into an organization. I know where to defend better and where to spend my budget, which is knowledge I wouldn't have gotten without 20 years of offensive security experience," Haddix says.

Haddix approaches his priorities as a CISO as **three pillars**—attack surface management, general "table stakes" items like email protection and antivirus, and hardcore application and corporate security. The third pillar comes from his time pen testing and hacking as part of bug bounty engagements. When one looks at modern breaches and attacks, we can see that many are the result of corporate security and web applications flaws.

Leveraging his offensive security background was actually one of the ways Haddix differentiated himself during the interview process at Ubisoft.

Jason Haddix · CEO at Arcanum Information Security

Given the endpoints he could see, he conducted a full attack surface management assessment and put together a presentation pitching how he would run a security program based on his **observations detected using his offensive skills.**

"I really think an offensive security practitioner is one of the best CISOs you can hire," Haddix says. "They have a very unique idea of how to defend a program because they've been the attacker before."

I really think an offensive security practitioner is one of the best CISOs you can hire.

Hacking to stay sharp

Throughout his almost two decades of security work under many leadership titles, Haddix has never stopped hacking and pen testing on the side. "It will never not be cool to do offensive security work. It's such a rush breaking into an organization and then helping fix it," Haddix says.

One aspect of traditional CISO roles that many security practitioners struggle with is that they may have to sacrifice some technical aspects of their job to take on tasks like budget management, stakeholder relationship management, and presentation building. This is especially true for enterprise CISO roles. By hacking on the side, CISOs can **maintain their technical touchpoints and skills.**

This practice also keeps CISOs truly on the bleeding edge of the **evolving threat landscape.** Hacking pushes and challenges people to constantly learn new techniques and stay up to date on the latest threats. Hacking also keeps CISOs connected to a **large community of hackers and security researchers** globally who regularly share knowledge and expertise.

It's such a rush breaking into an organization and then helping fix it.

"Bugcrowd's community of hackers is special and unique—you get to engage with some of the smartest people in the world at their particular specialization," Haddix shares. "When I was a kid, these types of jobs didn't exist. Now, hacking is a really alluring role."

There are many different paths a security practitioner can take to become an exceptional CISO. By nature of the role, CISOs need a breadth of experience, and this experience informs their approach to the role. However, there is no denying that an offensive security background and hacking experience are powerful tools in creating **impactful security leaders.**

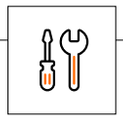
The CISO's approach to AI as a tool, target, and threat

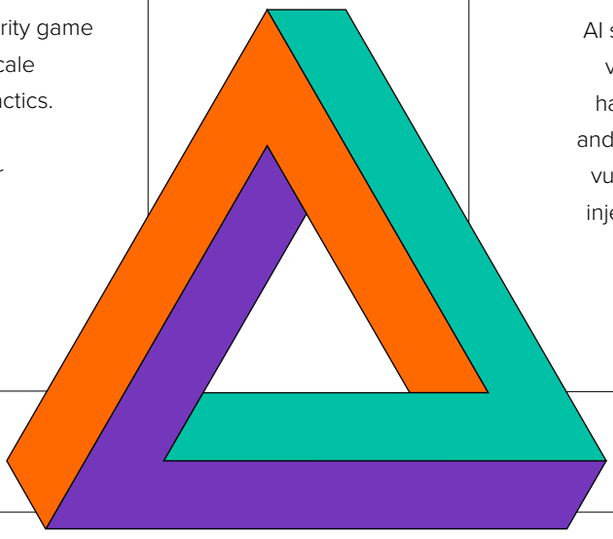
The public and policymakers alike have spent a lot of time discussing the future of AI. How powerful will the next models be? How will AI regulation impact organizations? Will AI lead to workforce reductions down the road?

But the impact of AI is already here. CISOs and security leaders have been thinking about AI for a while and have some strong opinions on its **value, risks, and defensibility.** They think AI will play three different roles in security, acting as a **tool, target, and threat.** So, we asked your peers how they're preparing for each.

AI as a tool

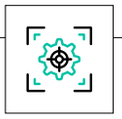
Both sides of the cybersecurity game will use AI to increase the scale and sophistication of their tactics. For example, threat actors can create convincing spear phishing attacks at scale and defenders can use AI models to detect intrusions within milliseconds.





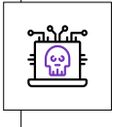
AI as a target

AI systems will be a new attack vector. Many new AI systems have access to company data and resources, and unmitigated vulnerabilities (such as prompt injection) will give threat actors a new avenue into these resources.



AI as a threat

AI systems can cause harm to users. This harm could range from realistic (saying biased things) to speculative (future models could be used to create weapons). In the context of this report, we look at harm in the form of AI models replacing human cybersecurity workers.



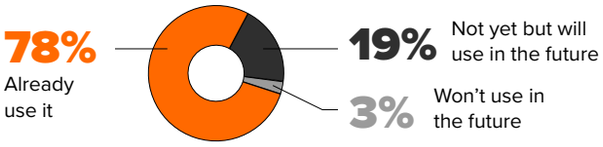
AI as a tool

78% of CISOs are already using AI to help their security teams. A further 20% are waiting to see more powerful models and better AI security tools before they adopt.

Interestingly, 91% of CISOs believe AI will be better than members of their own security teams. Almost half of the CISOs believe Gen AI has *already surpassed* the abilities of their team.

Does AI outperform security professionals?

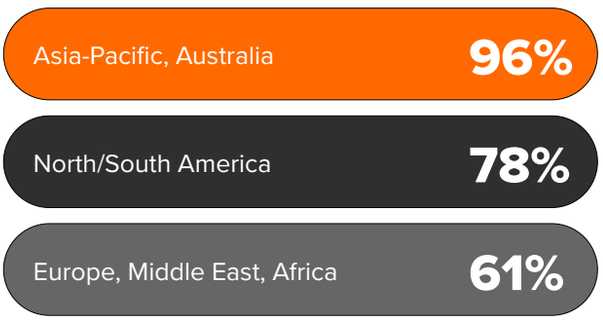
Overall AI adoption by security teams



AI SECURITY USES

Although some organizations may use AI for offensive security, the most common use case is **automating repetitive or tedious security tasks**. For example, organizations are using AI tools to help write data queries to get the security information they need much quicker. This, in turn, lets them run analyses, communicate, and take action in less time.

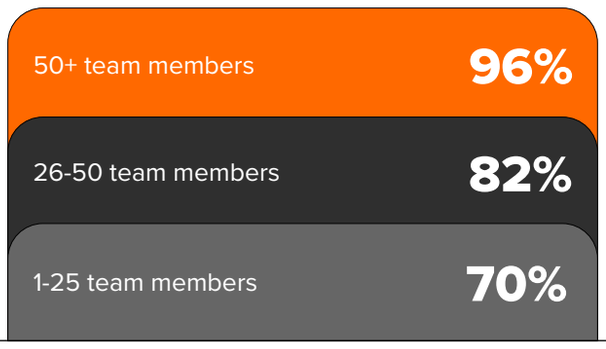
AI adoption by region



Asia-Pacific and Australian organizations are far more willing to use AI in security. 96% already use it, and the remaining 4% plan to in the future. This stems from a few big reasons. These CISOs are much more likely to believe AI already outperforms their team members (66% agree with this). They are also more likely to say that the security of AI tools is adequate (96% agree with this).

Other reasons may have to do with cybersecurity skills gaps being more significant in Asia-Pacific and Australian markets or less regulation on the use of Gen AI (e.g., compared to European countries).

AI adoption by security team size



At first, it may seem like smaller organizations would be more likely to be the **early adopters of AI**—they could use AI to increase the capabilities of their security teams. However, the biggest security teams are the ones using AI the most.

A reason for this may be that AI tools can't fully replace security team members. However, they can automate repetitive security tasks, and larger organizations may have more of these tasks (and a **larger AI budget**).

AI as a target

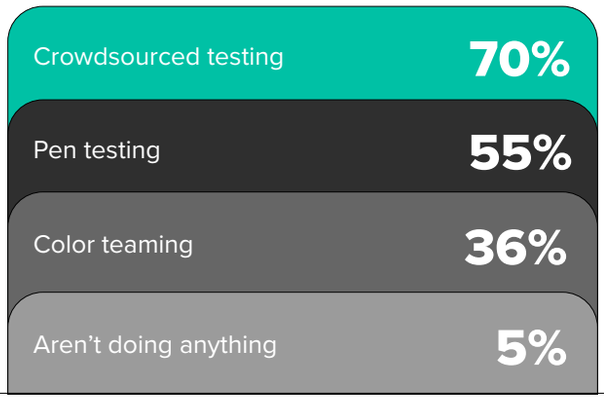
A majority of CISOs believe that existing products and solutions are enough to secure AI systems.

Interestingly, a majority of CISOs (76%) also think that AI is moving too fast to secure. What this points to is industry-wide uncertainty as to how rapidly AI will evolve from here on out. Teams are starting to get a handle on the current generation of Gen AI systems. But who knows what the **next wave of models** will bring?

Are existing solutions good enough to secure AI?

Is the AI threat landscape evolving too rapidly to secure?

Methods used for AI defense



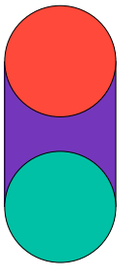
Almost every one of your peers is proactively defending their AI systems. Only 5% of CISOs aren't implementing AI defenses, which may be because they're not using AI tools at all.

Crowdsourced testing, including bug bounties and VDPs, most closely aligns with most CISOs' needs due to their **scalability and flexibility**. Pen testing is also commonly used for similar reasons. **Color teaming** is more common among larger security teams that have the requisite AI skills.

THE COLOR WHEEL OF SECURITY

Color teaming has been part of the cybersecurity industry for decades, but there is a surprisingly wide variety of definitions as to the different team colors, the skill sets they need, and how to build them.

Security leaders should think of purple teaming as a **continuous, two-way learning process** that bridges the blue and red teams. Instead of approaching color teaming as a Venn diagram, think of it as a bridge.



Red teams attempt to successfully attack without getting caught.

Purple teams unpack the lessons learned through the interactions between the two.

Blue teams attempt to prevent and catch the red team.

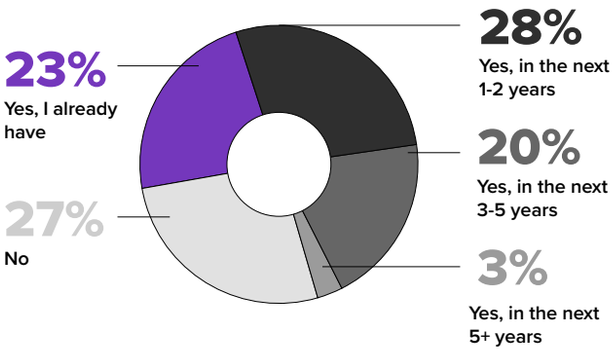
You can learn more about Bugcrowd's approach to color teaming here.

AI as a threat

23% of CISOs have already reduced the size of their teams. For mid-sized organizations (26–50 security team members), this number has climbed to 33%.

71% of security leaders have already reduced the size of their teams or plan to do so in the next five years with the adoption of AI. This number declines significantly for smaller security teams that are focusing more on building their teams and increasing **security maturity** than making size cuts to increase efficiency.

Plans to reduce headcount due to the adoption of AI technologies



Do the risks associated with AI outweigh the potential?

It's the **ultimate question** on everyone's mind—is this whole "AI thing" a net positive? What risks will it bring? What will happen to people's jobs? Are the efficiencies AI brings truly worth it?

Interestingly, the response from security leaders was close to 50/50. The widespread adoption of Gen AI is still new enough that many security professionals are still determining their AI strategies. As a result, they are often willing to sacrifice being an "early adopter" for a chance to observe the early wins and challenges other organizations are experiencing in their AI adoption journeys.

AI POLICY AND LEGISLATION

A key responsibility of CISOs is to oversee compliance requirements and incorporate new policy requirements into their overall security program. Governments around the world are responding to the rise of AI and its inherent safety and security risks. The regulation landscape is everchanging, but here are some of the first attempts at the government regulation of AI:

- **The European Union's AI Act:** This act assigns risk levels to different AI use cases and scopes. It bans use cases with unacceptable risk, such as facial recognition without consent, and introduces oversight mechanisms for high-risk use cases, such as using AI to sort through resumes.
- **Executive Order 14110:** The executive order lays out rules for how AI will be used in US federal civilian agencies and by federal contractors. It also requires organizations building large AI models to divulge training methods and datasets used. It delegates AI use in business to future regulation as well.

You can read more about considerations for rational, effective, and ethical AI regulation here.

Meet Ross McKerchar

CISO at Sophos

When it comes to cybersecurity expertise, leadership, and forward-thinking, look no further than Ross McKerchar—CISO at Sophos. Based in the southwest of the UK, McKerchar has built and led Sophos' security team for almost 17 years. Founded near Oxford, Sophos is a global cybersecurity company, leading the industry in managed threat detection and response, as well as endpoint, network, email, and cloud solutions.

As the CISO of Sophos, McKerchar oversees all aspects of Sophos' cybersecurity posture, including corporate, infrastructure, and product security.

McKerchar believes in building a security program with authenticity and transparency as its core values.

His mission is simple—**"I want to make Sophos the most trusted brand in cybersecurity."**

A TRANSPARENT APPROACH TO CYBERSECURITY

In his long tenure in the security space, McKerchar has witnessed a lot of FUD (fear, uncertainty, and doubt) tactics and tropes such as web pages promising "military grade encryption," boasts of having never been hacked, and cliches promising the organization takes security seriously.

He believes in taking the opposite approach. "At Sophos, we like to talk about the issues we may have. If you're transparent about issues and how you're overcoming them, it shows strength in your security program," McKerchar says.

This approach focuses on the fluctuating nature of the modern attack surface. New challenges are always surfacing, and it is unrealistic to expect security teams to constantly outpace these challenges on their own.

"Security is never 'done.' Every company has to work really hard to maintain their security posture. By taking a different approach, leaning in to demonstrate continual efforts with facts and actions instead of just words, organizations can better respond to security challenges," McKerchar says.

DEMONSTRATING TRUST UP AND DOWNSTREAM

As the CISO of a cybersecurity vendor, McKerchar needs to think both about the risk from his "upstream" suppliers and the risk to his "downstream" customers.

First, from a downstream perspective, Sophos has over 600,000 customers and is the world's most widely-used MDR provider. For these organizations, McKerchar and his teams work continuously to foster trust and ensure that Sophos' products are as secure as possible.

From an upstream perspective, McKerchar must evaluate the security of vendors in his own supply chain. After all, an organization is only as strong as its weakest link.

One unique method he uses to evaluate vendor security is a bug bounty engagement.

"Bug bounty programs are an underutilized way of evaluating a vendor. Security teams send out those long security questionnaires, but ultimately, words are cheap, it can be very hard for teams to understand the underlying security posture of potential vendors. To get a good signal on a vendor, my team looks at their bug bounty program. Like our own program, we are looking for a wide scope, competitive rewards, and good engagement levels.

"You can't fake a good bug bounty engagement."

ZOOMING OUT ON RISK

Sophos is a large organization with a very diverse set of products. This naturally creates a large attack surface that requires protection in a variety of different ways.

One strategy McKerchar leverages to do this is by "zooming out on risk" to see the bigger picture. "I've seen organizations get caught up in the perceived risk of security protection measures such as bug bounty engagements. They feel like by using crowdsourced solutions, they're inviting attacks. If you worry too much about that, you're missing the bigger risk—the potential impact of serious vulnerabilities across your organization."

By zooming out to look at the bigger picture, the Sophos team reduces risk overall, and in turn, becomes more secure. This is especially crucial now, when the time that threat actors take to exploit vulnerabilities on an organization's perimeter has dropped from weeks to days to hours to minutes.

Sophos takes a multi-layered approach to attack surface management. Common misconfigurations and weaknesses are managed via bespoke tooling combined with Sophos Managed Risk, providing 24/7 support to identify and address high-priority issues. By partnering with Bugcrowd, Sophos uses a Bug Bounty program to spot the hidden and emerging issues that tools can miss. "The hacker community can outrun threat actors at an unprecedented pace. It's like having hundreds of extra people working for you and keeping an eye on your perimeter, without the logistics and challenges of actually hiring people.

"Not even the largest security teams can do what a well-managed bug bounty engagement can achieve."

Advice for aspiring CISOs

This report was written with CISOs and other security leaders in mind, but all security practitioners can benefit from its findings. Before we wrap up this edition of Inside the Mind of a CISO, we want to speak directly to the security practitioners who are considering their career paths and interested in the CISO role.

For aspiring CISOs, the role can feel daunting. **CISO training courses** often don't do the role justice, and no matter how much experience you may have, remember that it's rare for anyone to come to the table with every skill needed for the job. A CISO must have **technical know-how** while also being a manager, a storyteller, a negotiator, a cheerleader, a budgeter, a therapist, and a team captain.

That being said, aspiring CISOs shouldn't be discouraged by the responsibilities of the role. To better understand what it takes to be a CISO, take a closer look at the following, where we explore the **experiences of CISOs** and the trends and insights that shape their roles and responsibilities. Read on for a better understanding of the security leaders of today and learn what it takes to be at the **forefront of cybersecurity leadership**.

Security leaders' years of experience

< 2 years	**3%**
2–5 years	**13%**
6–10 years	**37%**
11–15 years	**29%**
16+ years	**17%**

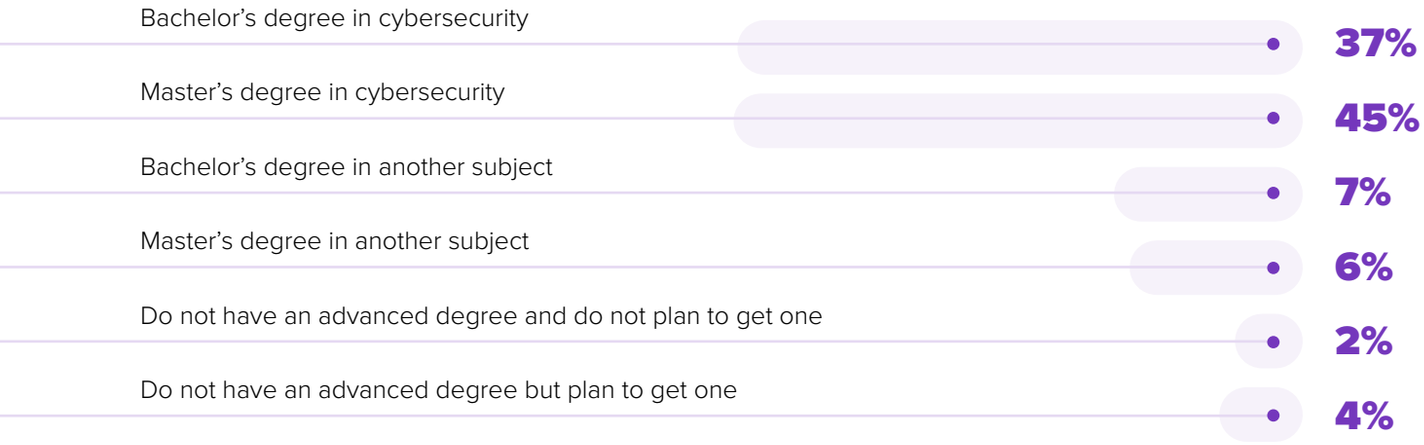
Security leaders bring a **wealth of experience** to the table, with 84% of them having at least six years of experience in the field.

But the true veterans of the field, those with over a decade of experience, make up an impressive 47% of the security leadership landscape. This impressive number shows that can prepare someone for the rigorous task of being at the forefront of security quite like **learning on the job**.

But don't let their years of experience fool you—these leaders are far from being stuck in their ways. In fact, it's their ability to combine deep industry knowledge with a willingness to **embrace new ideas and technologies** that sets them apart. They understand that **continuous learning** is the key to success in a field that's quickly growing and changing.

FOR ASPIRING CISOS

Average education completed by security leaders



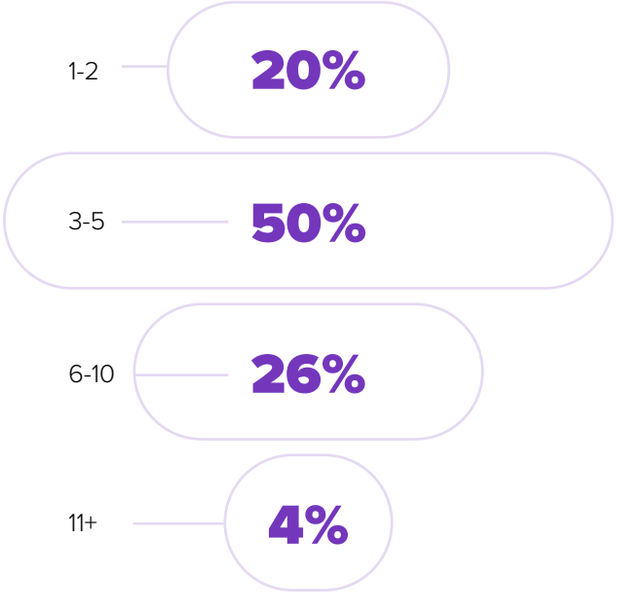
Security leaders are a well-educated bunch! A staggering 94% of security leaders have a university education, and 82% have a degree specifically in cybersecurity.

Almost half have invested extensively in their technical education and earned a master's degree or above in cybersecurity. From cryptography and network security to risk management and incident response, cybersecurity degree programs equip individuals with the **cutting-edge knowledge** and practical skills needed to defend against the latest threats.

Of course, while a formal degree in cybersecurity is a powerful asset, education comes in many forms. Our study found that 13% of security leaders hold degrees in fields other than cybersecurity and 6% don't have a degree, bringing diverse perspectives to their organizations from a variety of life experiences and formal studies.

As the tech industry evolves, more organizations are starting to recognize the value of **real-world experience** alongside formal education. So don't be surprised if you see a shift in leadership backgrounds in the near future.

Average number of roles security leaders have held throughout their careers



It's a long way to the top...

Most security leaders have held at least two roles before landing their current role. Half have held 3 to 5 jobs throughout their careers. This supports the idea that **moving between roles** is welcome and even helpful in developing these leaders' skills.

The benefits of diverse job experiences extend far beyond technical expertise. As security professionals transition between roles, they also hone their **adaptability, resilience, and communication skills**. They learn to navigate complex stakeholder relationships, build bridges across departments, and effectively translate technical concepts for non-technical audiences. These skills set great security leaders apart, enabling them to drive organizational change, create a culture of security, and align cybersecurity initiatives with business objectives.

Three tips to keep in mind

Below are three pieces of advice for those considering working their way up to the CISO position:

Determine your true motivations.

"CISO" is a cool title, but to be an effective CISO, you need to truly grow to love the role itself. There is little training behind the CISO position because it's such a catch-all role.

Oftentimes, CISOs must focus more on business development, regulators, finance, and other external bodies instead of focusing on the technical aspects of security. If you're extremely passionate about day-to-day technical aspects and not as interested in people management, building slide decks, and presenting at meetings, the position of CISO might not be the right fit for you.

Move horizontally for diverse experience.

In an enterprise security team, there can be anywhere from 10 to 15 different security groups, all with unique roles and responsibilities.

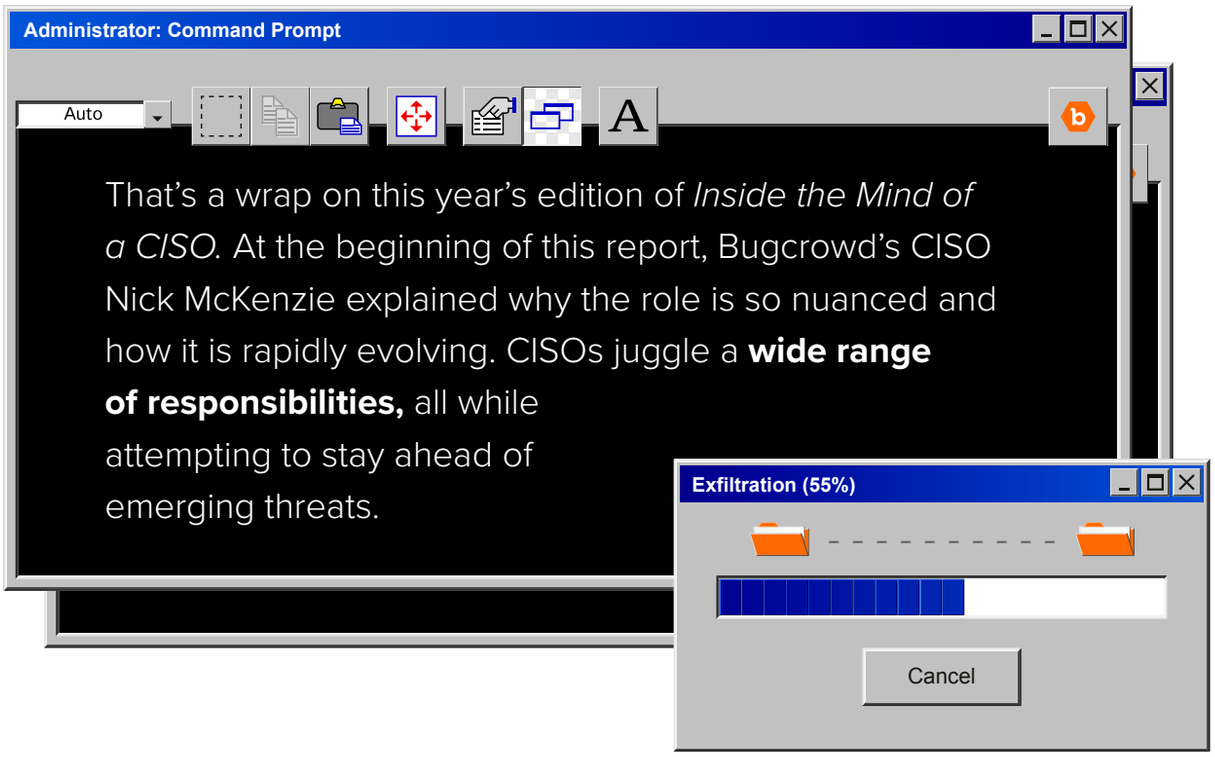
To be an effective CISO, you must spend time in as many different areas of security as possible. Decide if you ultimately like working in each of these different areas. Then, learn to up-level, bringing your diverse experience to a management capacity. This experience will help you prioritize smaller initiatives in the grand scheme of a larger security program.

Refine your storytelling skills.

So much of the CISO role is learning how to describe technical subjects to non-technical stakeholders to secure the resources needed.

If you can create a compelling slide deck and present it in a way that tells an effective story, you'll be able to move the needle as a CISO. These storytelling skills will help you advocate for the needs of your team.

Conclusion



There is no denying the complexity of the CISO role, especially in the past few years. In addition to their other responsibilities, CISOs have to carry the burden of breaches.

A security breach is **incredibly jarring** and often leads to **CISO burnout,** which is one of the reasons why the tenure of a CISO is relatively short compared to other roles. When a breach occurs, a CISO must manage the response within their team, protect their team, and communicate to the C-suite what is happening and what the team is doing about it. For the organizations that deal with breaches two to three times a year, this can really **take a toll.**

Given the challenges and high-stakes nature of the role, some may wonder what attracts security leaders to the CISO role in the first place.

Ultimately, the CISO position is an **amazing opportunity** to make a **wide-reaching impact.** CISOs can engage in the technical aspects of security while building cohesive security strategies, bringing teams together and leading groups. CISOs act as a bridge between the wider organization and technical folks, translating critical security needs to business outcomes.

CONCLUSION

Documents

The research in this report provides an overview of the CISO role, looking at what is top of mind for many security leaders. Additionally, it provides an overview of the industry as a whole, highlighting trends and best practices to benchmark against. Here are **three major takeaways** from the research:

takeaway_01

Security is a competitive advantage

Security is more than just a best practice—Security is more than just a best practice—it is a competitive advantage. As threats become more serious and more ubiquitous, consumers are becoming more aware of the importance of security, and they use this as a factor in their buying decisions. As the C-suite and boards continue to recognize this fact, the pressure will be on security leaders to deliver a superior security experience.

takeaway_02

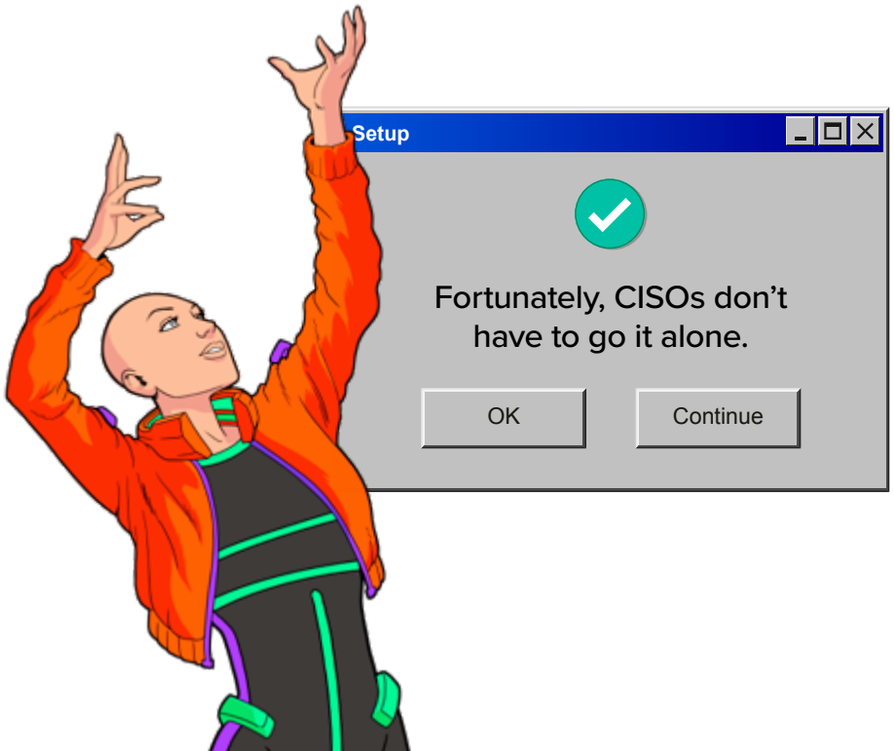
AI is controversial, but it's here to stay

The jury is still out on how exactly security teams need to approach AI as a tool, a target, and a threat. Teams are leveraging AI, which is already starting to affect headcounts, but many leaders are hesitant to become early adopters of AI. The one consensus is that AI is here, and it is the responsibility of security leaders to quickly build their AI strategy.

takeaway_03

Security requires diverse skill sets and experience

CISOs need experience in many different types of security roles to best build a cohesive strategy and know how to prioritize resources. Their teams also need these varied skill sets. This is one reason why partnering with ethical hackers is so popular among CISOs—it gives organizations access to countless skill sets without needing the resources to employ these experts full time.



Bugcrowd combines an **AI-powered platform** with the **collective ingenuity** of the hacking community to extend the reach of every CISO's security team. These hackers help CISOs secure their attack surface before threat actors can even think about striking.

KEEP READING

Content recommendations

Chow down on more hearty stories from Bugcrowd below

Inside the Mind of a Hacker

Analysis on how Security Researchers are Using Generative AI

DIGITAL MAGAZINE

PRODUCT TOUR

5-Minute Virtual Product Tour

Defend Against Cyberattacks with Data, Technology, and Human Intelligence

GUIDE

The Ultimate Guide to AI Security

The basics of AI security plus ways to prevent attacks against AI systems

ANALYST REPORT

Forrester Total Economic Impact of Bugcrowd

The Cost Savings and Business Benefits Enabled by Managed Bug Bounty

Glossary

a

AI Bias: Systematic errors in the output of an AI system resulting from underlying biases in the training data or algorithm design.

Antivirus: A software or computer program used to prevent, detect, and remove malware.

Artificial Intelligence: The simulation of human intelligence processes by machines, particularly computer systems, to execute tasks akin to learning and decision-making found in humans. Subsets of AI include expert systems, neural networks, deep learning, natural language processing, speech recognition, and machine vision. In cybersecurity, AI applications include attack surface management, automated detection and response, and intelligent authentication and fraud prevention.

Asset: Any data, device, or environmental component that supports information-related activities. Assets generally include hardware, software, and confidential information.

Attack Surface: The sum of the different points in a software environment where an unauthorized user can enter or extract data. Minimizing the attack surface is a basic security measure.

Attacker: An individual or group who performs malicious activities to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset.

b

Bounty: Monetary rewards offered in exchange for a vulnerability finding, discovery, or report.

Breach: A cyberattack in which sensitive, confidential, or otherwise protected data have been accessed or disclosed in an unauthorized manner.

Bug: A software defect that can be exploited to gain unauthorized access or privileges on a computer system.

Bug Bounty: Bug bounty programs allow independent security researchers to report bugs to an organization and receive rewards or compensation.

c

Chief Information Officer (CIO): The senior-level executive within an organization responsible for overseeing the people, processes, and technologies within a company's IT organization to ensure they deliver outcomes that support the goals of the business.

Chief Information Security Officer (CISO): The senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure assets and technologies are adequately protected.

Chief Security Officer (CSO): The senior-level executive within an organization responsible for managing security risks for an organization, from cyber attacks to physical intrusion.

Chief Technology Officer (CTO): The senior-level executive within an organization responsible for overseeing the entire information technology department and integrating business needs and requirements into IT planning.

Color Teaming: The approach to security testings where internal teams are assigned colors (blue, red, and purple) to represent attack, defense, and collaboration.

Compliance: The process an organization takes to protect its assets and meet internal security and legal requirements.

Crowd Fear: The hesitancy to embrace working with hackers, coming from the misconception that working with hackers exposes an organization to more risk.

Crowdsourced Security: An organized security approach wherein ethical hackers are sourced and activated to search for and report vulnerabilities in the assets of a given organization. The power of crowdsourced security is derived from the proportion of active testers per asset/ecosystem versus more traditional testing methods.

Customer: Organizations that leverage the Bugcrowd platform or its associated services.

Cyberattacks: A malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.

Cyber Insurance: An insurance policy that provides businesses with a combination of coverage options to help protect the company from data breaches and other cybersecurity issues.

Cybersecurity Skills Gap: The mismatch between the skills employers require in cybersecurity professions and the qualifications possessed by potential candidates.

d

Digitalization: The process of fundamentally changing an organization with technology and culture to improve/replace what existed before.

Disclosure: The practice of reporting security flaws in computer software or hardware.

D&O Insurance: Directors and officers (D&O) liability insurance covers directors or officers of a business or other organization if a lawsuit is brought against them.

e

Engagement: Measurable indicators of the level of interest, involvement, and influence that a crowdsourced security program generates among ethical hackers or custom-designed penetration testing solutions tailored to an organization's unique needs.

Ethical Hacker: A person who hacks into a computer network to test/evaluate its security, rather than to carry out an act of malice.

Ethical Hacking: An authorized attempt to gain unauthorized access to a computer system, application, or data.

f

FUD: The acronym standing for Fear, Uncertainty, and Doubt. It's known to be a manipulative way to present information.

g

Generative AI / Gen AI: Generative AI is a type of artificial intelligence technology that can produce various types of content, including text, imagery, audio and synthetic data in response to prompts. Generative AI models learn the patterns and structures of their input training data, and then generate new data that have similar characteristics.

h

Hacker: Someone who uses technical knowledge and tenacity to achieve a goal or overcome an obstacle within a computer system by non-standard means.

i

Identity Access Management: A framework of policies and technologies to ensure that the right users have the appropriate access to technology resources.

Incident Response: A term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the incident so that damage, recovery time, and costs are limited and collateral damage, such as brand reputation, is kept to a minimum.

m

Model: A program that analyzes mathematical representations of relationships between variables to make predictions or decisions in artificial intelligence systems.

o

Offensive Security: Offensive security is a form of proactive security that comprises the constant process of identifying and fixing exploits before attackers can take advantage of them.

p

Penetration Tester / Pentester: Someone who professionally attacks computer systems to find security weaknesses that can then be fixed.

Penetration Testing / Pentesting: A simulated cyberattack done by authorized hackers who test and evaluate the security vulnerabilities of the target organization's computer systems, networks, and application infrastructure.

Platform / SaaS Platform: Bugcrowd is an all-in-one SaaS platform that combines actionable, contextual intelligence with the skill and experience of the world's most elite hackers to help leading organizations solve security challenges, protect customers, and make the digitally connected world a safer place.

Point-in-Time Assessment / Security Testing: A point-in-time review of a company's technology, people, and processes to identify problems. Such assessments can find vulnerabilities at a single moment, but fail to monitor activity between assessments.

Program: A program—which can be public or private—permits independent researchers to discover and report security issues that affect the confidentiality, integrity, or availability of customer or company information and rewards them for being the first to discover a bug.

Prompt Injection: The malicious act of inserting unauthorized commands or data into a user's interactions with a system, often to gain unauthorized access or control.

r

Risk: The potential for loss, damage, or negative consequences resulting from threats to the confidentiality, integrity, or availability of information or systems.

s

Security Landscape: The entirety of potential and identified cyber risks affecting a particular sector, group of users, time period, etc.

Security Leaders: This report defines security leaders as anyone with one of the following titles—CISO, CIO, CTO, Head of Security, or VP of Security.

Security Research: The study of technology, algorithms, and systems that protect the security and integrity of computer systems, the information they store, and the people who use them.

Security Researcher: Refers to the diverse group of skilled participants who hunt for vulnerabilities using the Bugcrowd platform. These trusted experts are sometimes referred to as white hats or ethical hackers.

t

Target: A web or mobile application, hardware, or API that the Crowd tests for vulnerabilities.

The Crowd: The global community of white hat hackers on the Bugcrowd platform who compete to find vulnerabilities in bug bounty programs.

Threat Actor: An individual, group, or organization that poses a potential risk to the security of information or systems through malicious activities.

Triage: The process of validating a vulnerability submission from raw submission to a valid, easily digestible report.

v

Vulnerability: A security flaw or weakness found in software or in an operating system that can lead to security concerns.

Vulnerability Disclosure Program (VDP): Clear guidelines for researchers to submit security vulnerabilities to organizations while also helping organizations mitigate risk by supporting and enabling the disclosure and remediation of vulnerabilities before they are exploited. VDPs usually contain a program scope, safe harbor clause, and method of remediation.

INSIDE THE MIND OF A CISO

bugcrowd