Enterprise Strategy Group | Getting to the bigger truth.™

2021 Bot Management Trends:

Harmful Attacks Drive Interest in Specialized Solutions

John Grady, ESG Senior Analyst
Adam DeMattia, ESG Director of Research

APRIL 2021

Commissioned By:

HUMAN formerly White Ops

CONTENTS

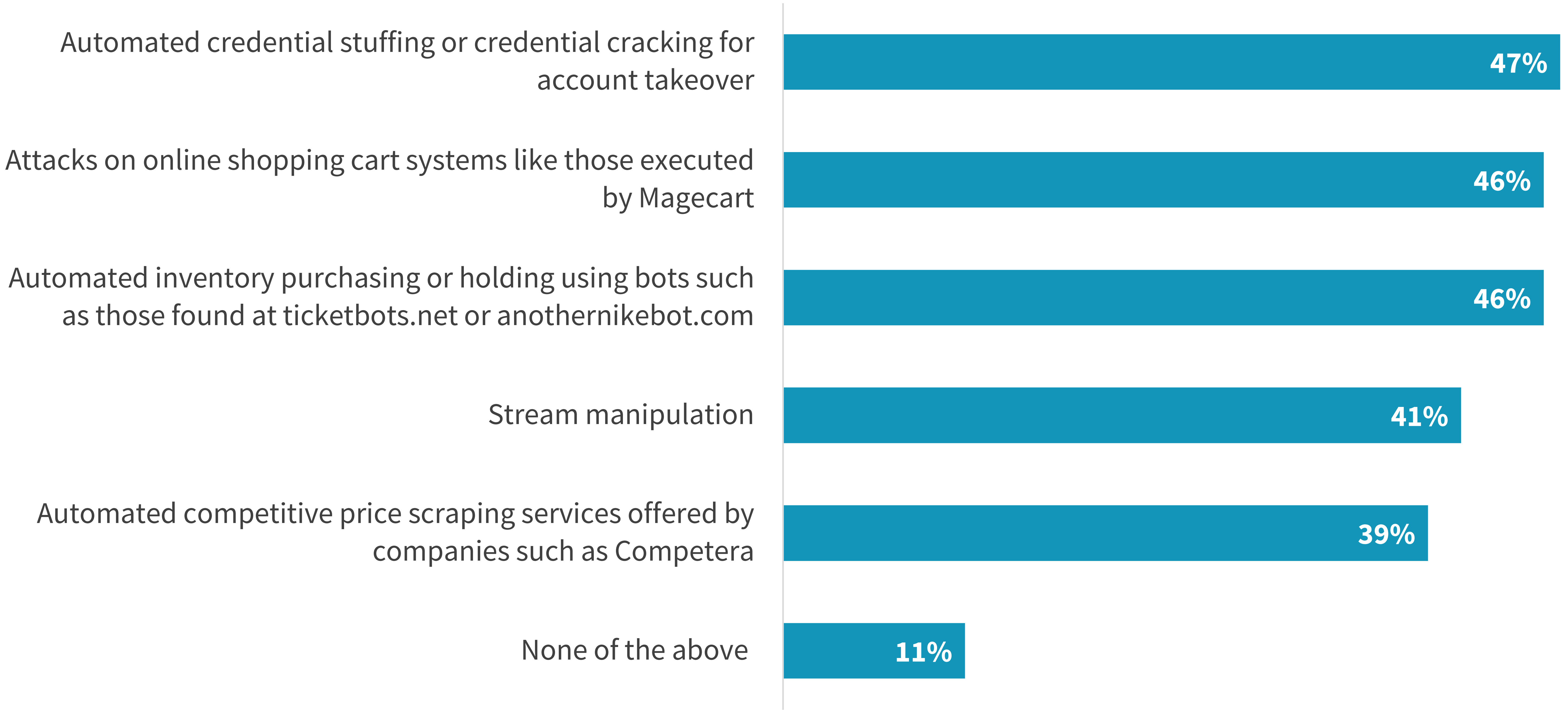
CLICK TO FOLLOW

Attackers Increase Their Use of Automation Through Bots

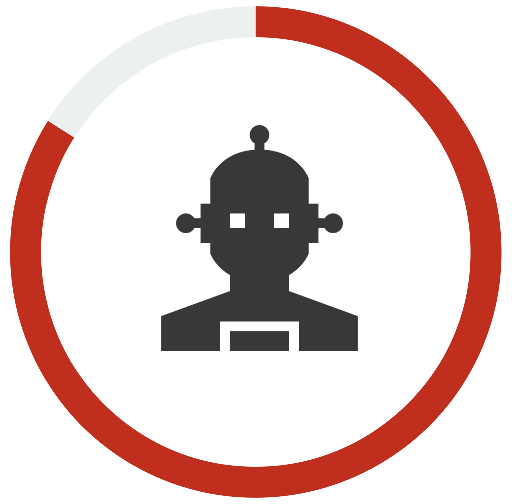
Bots are certainly not a new problem to cybersecurity. Attackers use bots to automate their attacks and increase the scale with which they can target organizations. Historically, bots have been associated with denial-of-service attacks, with the attention given to bots varying depending on the volume and frequency of attacks. As organizations have shifted to more online-focused business operations, a trend further accelerated by the pandemic, attackers have doubled down on their efforts and increased the frequency of bot-driven fraud and logic abuse. As a result, awareness of the issues posed by bots is growing. Nearly half (47%) of cybersecurity professionals have seen examples of credential stuffing or cracking attacks used for account takeover (ATO) in just the last 6 months. A similar percentage (46%) of respondents are aware of attacks on online shopping cart systems and instances of automated inventory purchasing or holding. In all, only 11% of our respondents have not seen publicized examples of sophisticated bot attacks.

> “***As organizations have shifted to more online-focused business operations,*** *a trend further accelerated by the pandemic, attackers have doubled down on their efforts and increased the frequency of bot-driven fraud and logic abuse.*”

Awareness of publicized bot incidents.



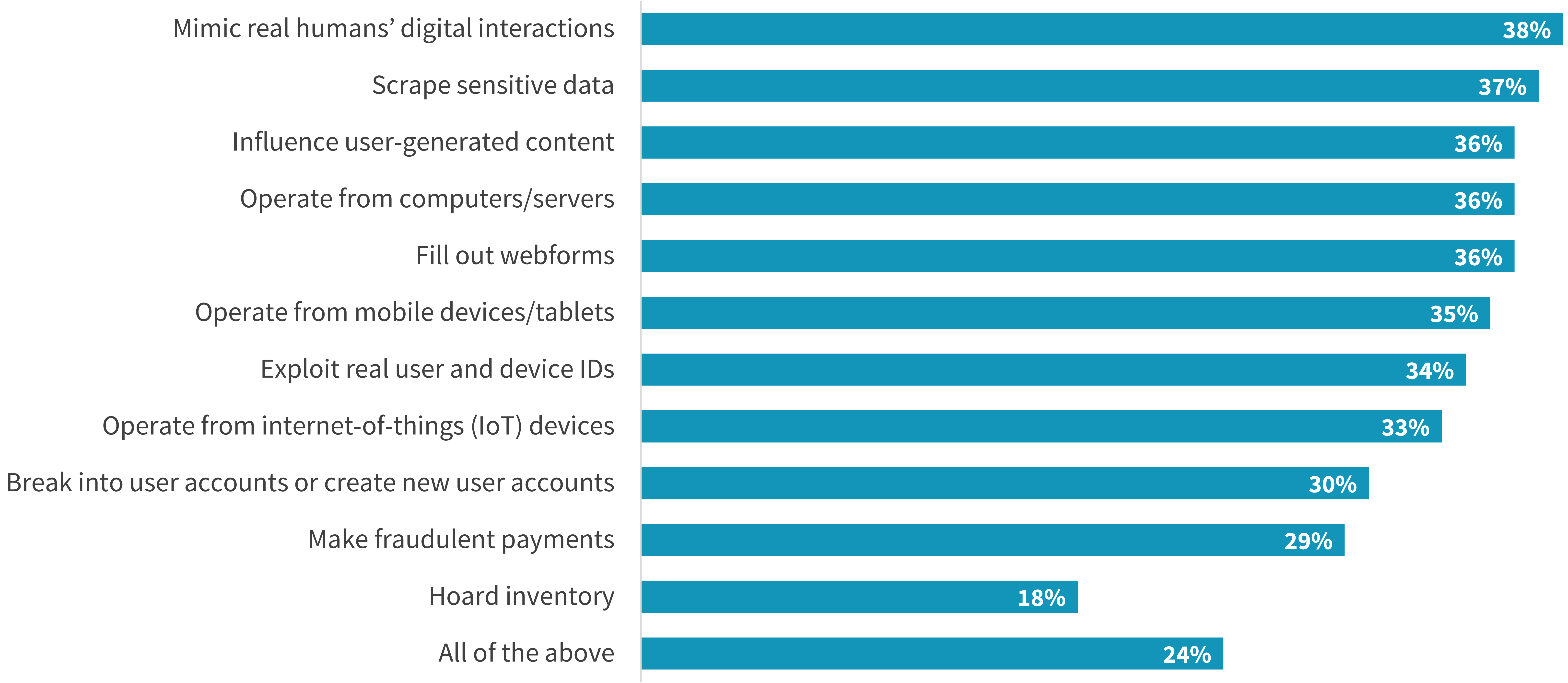
Back to Contents



84%

of respondents believe sophisticated bots are often controlled by organized cyber-criminals

Perceptions of bot capabilities.



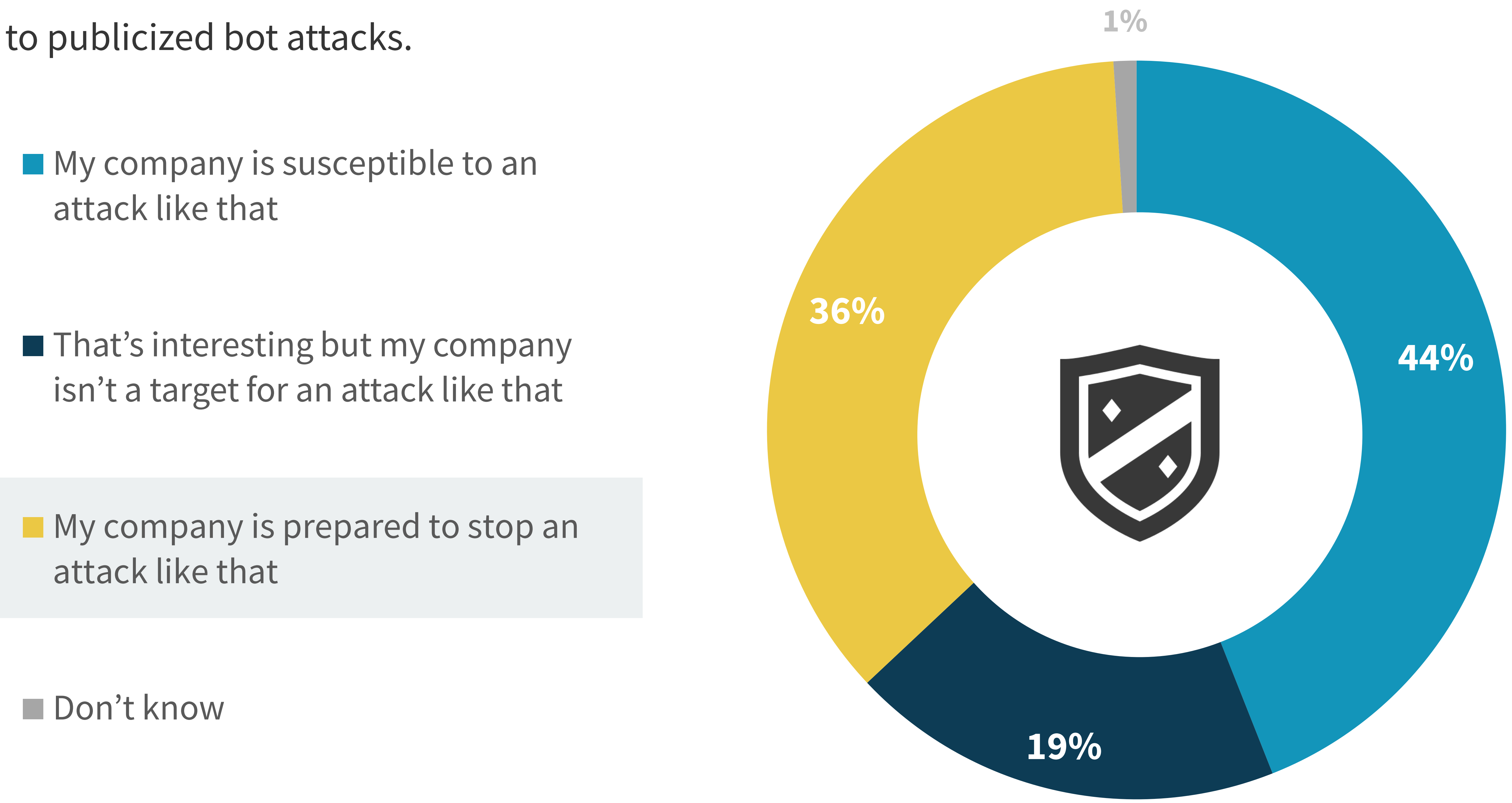
Bots Are More Sophisticated Than Ever

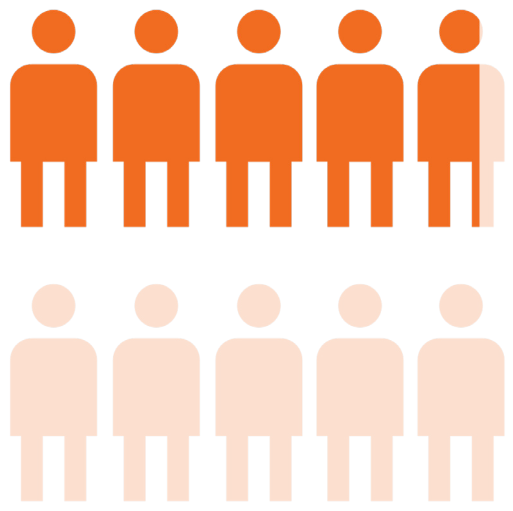
There is a general understanding that sophisticated bots are capable of a diverse range of activity from mimicking human digital interactions to scraping sensitive data and filling out webforms. Yet, even though 84% of respondents believe sophisticated bots are often controlled by organized cyber-criminals, they are somewhat less likely to believe bots are capable of criminal activity such as breaking into user accounts or making fraudulent payments. Finally, while sophisticated bots are capable of all the actions on our list, only 24% of respondents agreed with that sentiment. For as far as awareness and understanding about sophisticated bots has come, additional education must take place.

Many Feel Unprepared to Prevent a Bot Attack

As a result of publicized incidents and the broad range of attacks sophisticated bots are capable of launching, nearly half of our respondents (44%) believe their organizations would be vulnerable to a sophisticated bot attack. Surprisingly, 19% of respondents do not believe their organizations would be a target for a sophisticated bot attack. As mentioned previously, the dramatic shift towards online business models and e-commerce allows attackers to impact a broader set of companies than ever before. Finally, it is important to note that organizations using specialized bot management tools are nearly twice as likely (48% versus 25%) to feel prepared to stop a sophisticated bot attack.

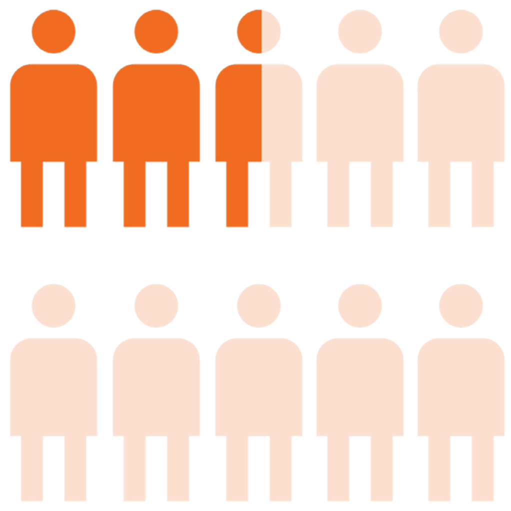
Reaction to publicized bot attacks.





48%

use specialized bot management solutions

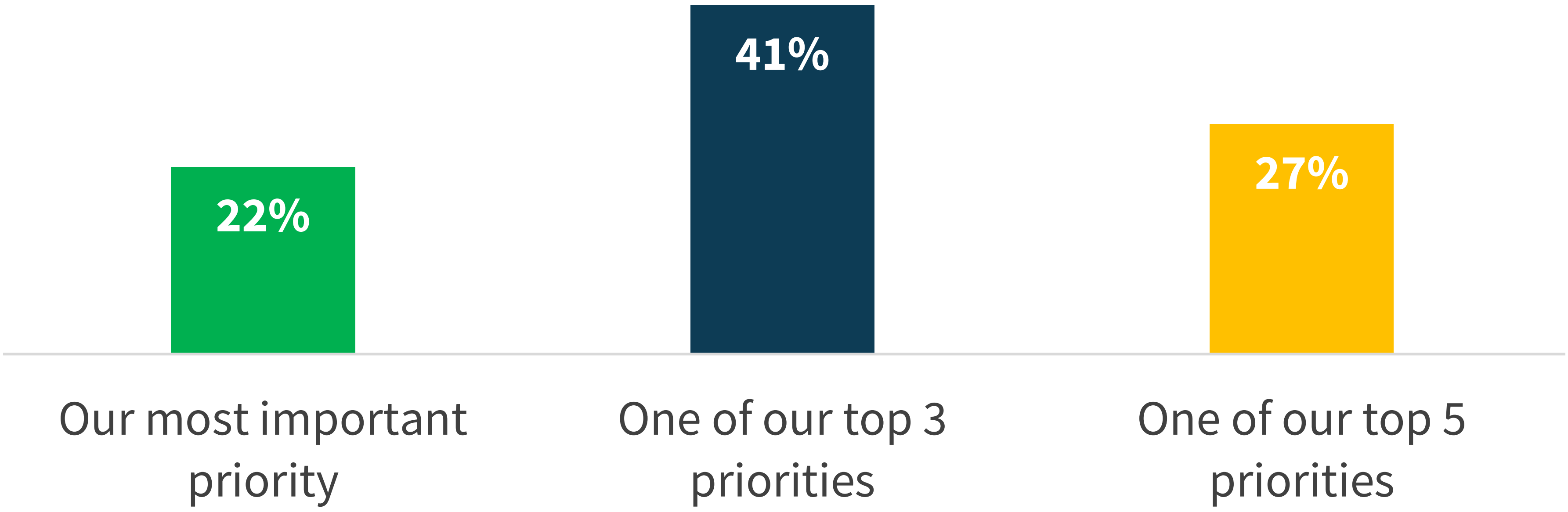


25%

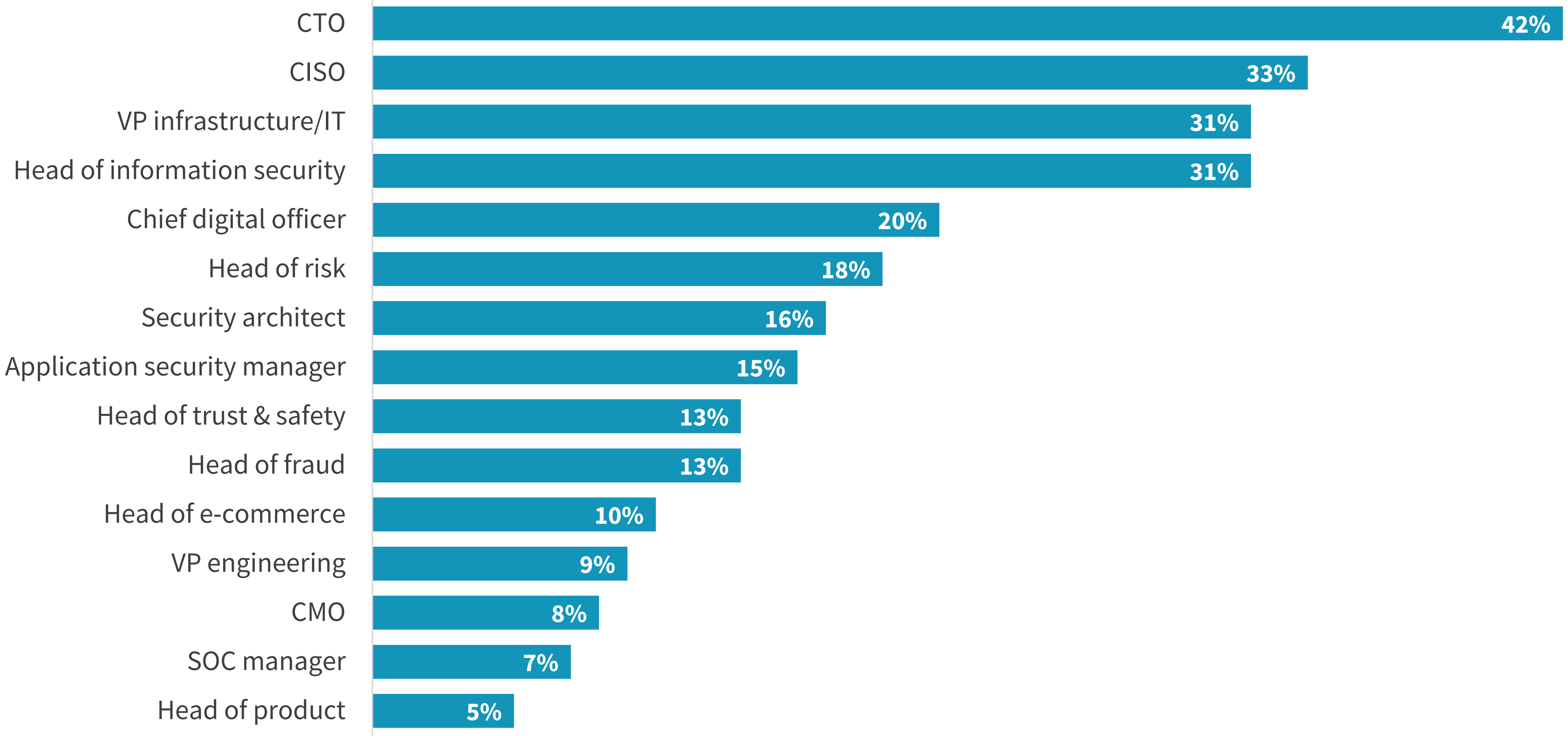
use bot features in tools such as WAF

Back to Contents

Bot management as a cyber priority



Decision-maker for bot management solutions.



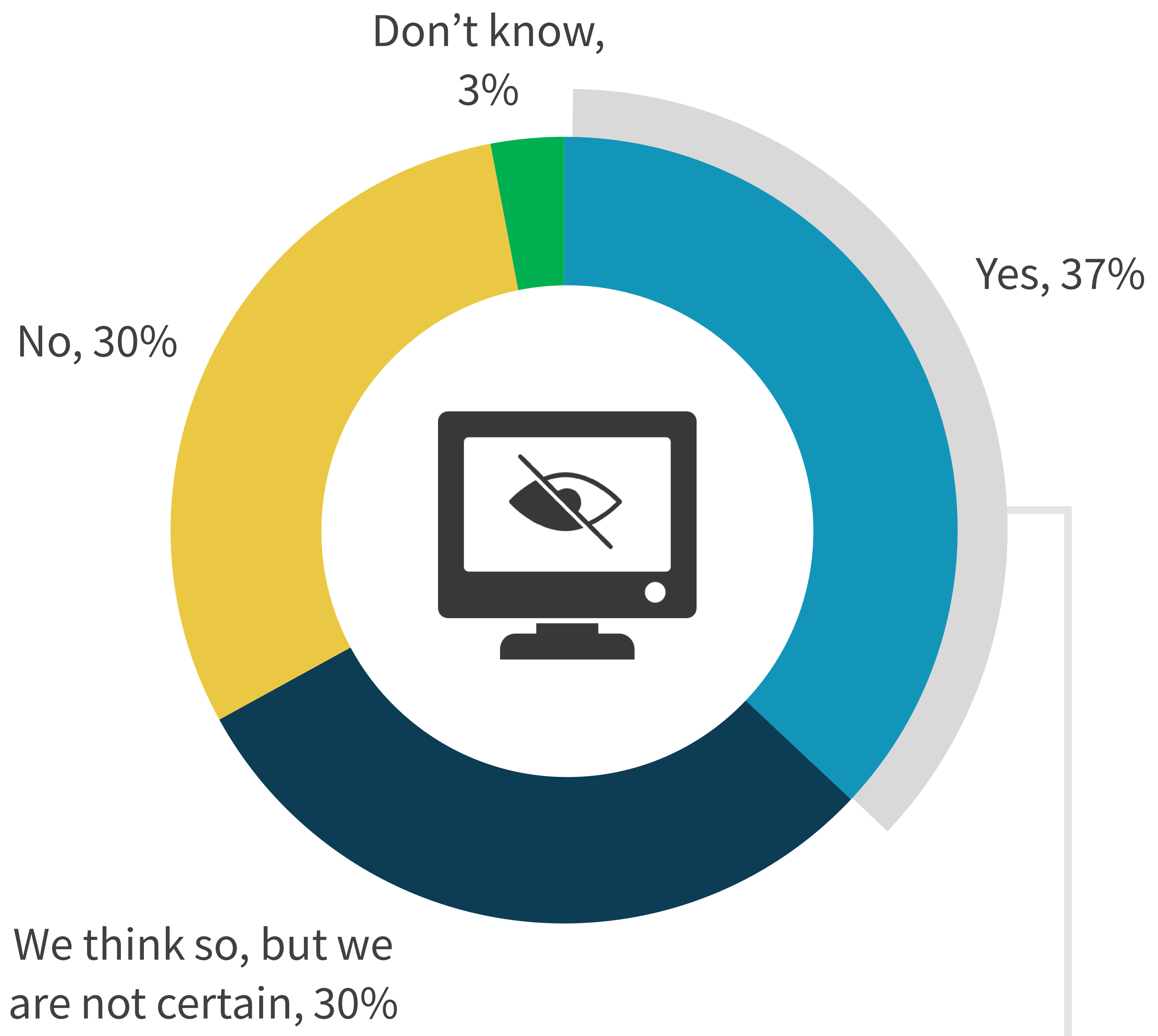
9 in 10 View Bot Management as Top 5 Cyber Priority

Cybersecurity teams have a lot on their plate these days. Supporting digital transformation initiatives, securing cloud migration, providing secure access to remote employees, and implementing zero-trust strategies are top of mind for many organizations. Considering that long, albeit incomplete, list of projects, it is extremely telling that 9 in 10 respondents indicate their organizations views bot management as a top 5 priority. Further, 63% say their organization will increase focus on protecting applications from bot-driven fraud and logic abuse moving forward. As a result, bot management has been elevated to an executive-level issue, with the CTO, CISO, and other leaders owning budget and final say over the tools implemented to address sophisticated bot attacks. So, while it is absolutely true that bot management is a team sport, requiring close collaboration across the security, IT, web, application, and fraud teams, the criticality of the issue calls for executive leadership.

Bot Attacks Are Common, But Visibility Is Inconsistent

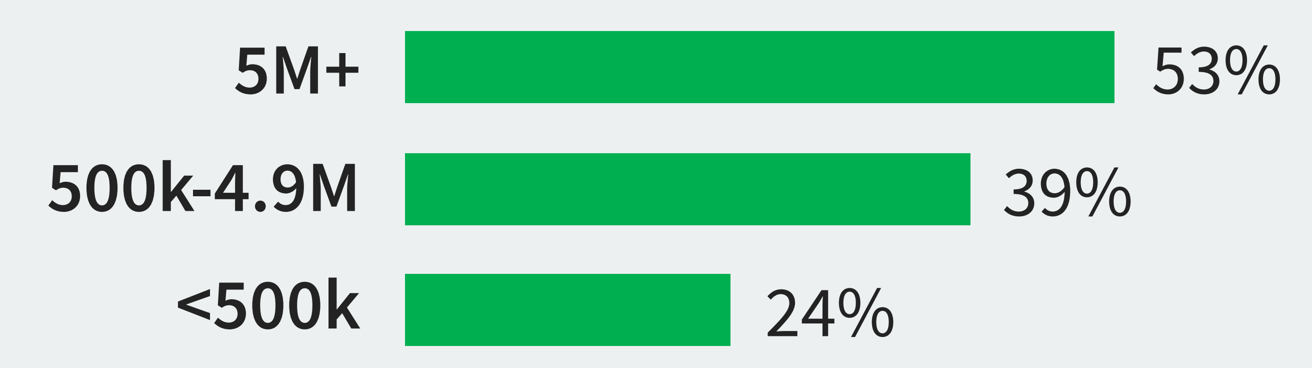
Over a third of organizations (37%) have been impacted by sophisticated bots over the last year. Unsurprisingly, organizations with large websites (over 5 million monthly visitors) are more likely to have been attacked than those with smaller sites (less than 500k monthly visitors). More worrisome, though, is the fact that 30% believe they have been impacted by sophisticated bots but are not sure. This points to a critical lack of visibility into these organizations' website and application traffic. The adage says you can't defend what you can't see, and the priority in bot management must be implementing tools that provide granular visibility into the type of traffic connecting to a website to help organizations begin to understand the impact from sophisticated bots.

Two-thirds believe they may have been victimized by a bot attack over the last 12 months.



> *More worrisome, though, is the fact that 30% believe they have been impacted by sophisticated bots* ***but are not sure.***"

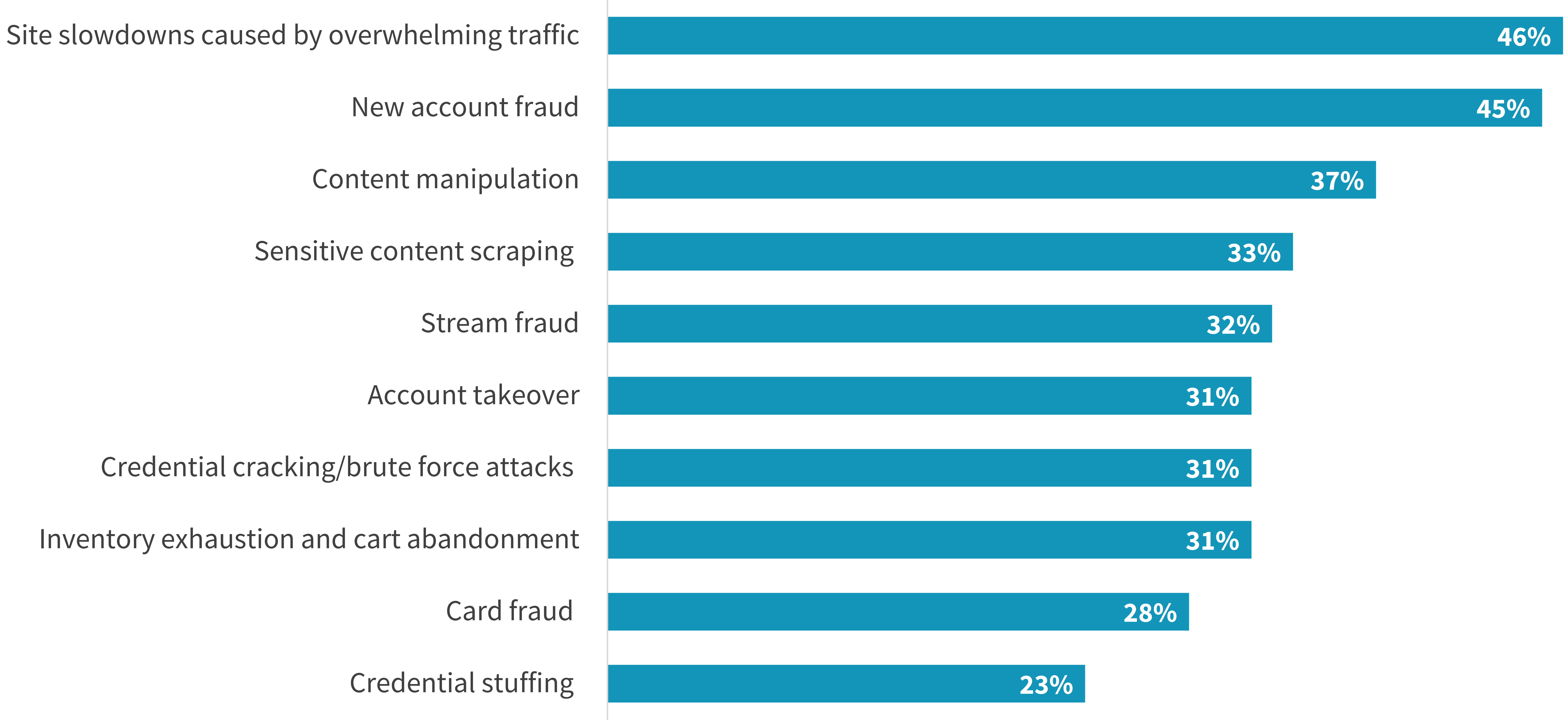
RESPONDENTS BY SITE VISITS:



Back to Contents

> “**Account takeover represents an increasingly popular attack vector** *and is of particular concern for organizations due to the potential compliance violations that can result through the loss of personally identifiable information.*”

Types of bot attacks.



Attacks Target Resource Availability, Fraud, and Credentials

The level of diversity in the types of attacks experienced by our respondents of the last year highlights the difficulty in defending against sophisticated bots. While some campaigns may focus on website or inventory availability, many organizations have been targeted by content manipulation and stream fraud attacks. Account takeover represents an increasingly popular attack vector and is of particular concern for organizations due to the potential compliance violations that can result through the loss of personally identifiable information. While 31% of our respondents have been subject to ATO attacks, an additional 31% reported credential cracking attacks, and 23% saw credential stuffing attacks, both of which can be used as the first step towards account takeover.

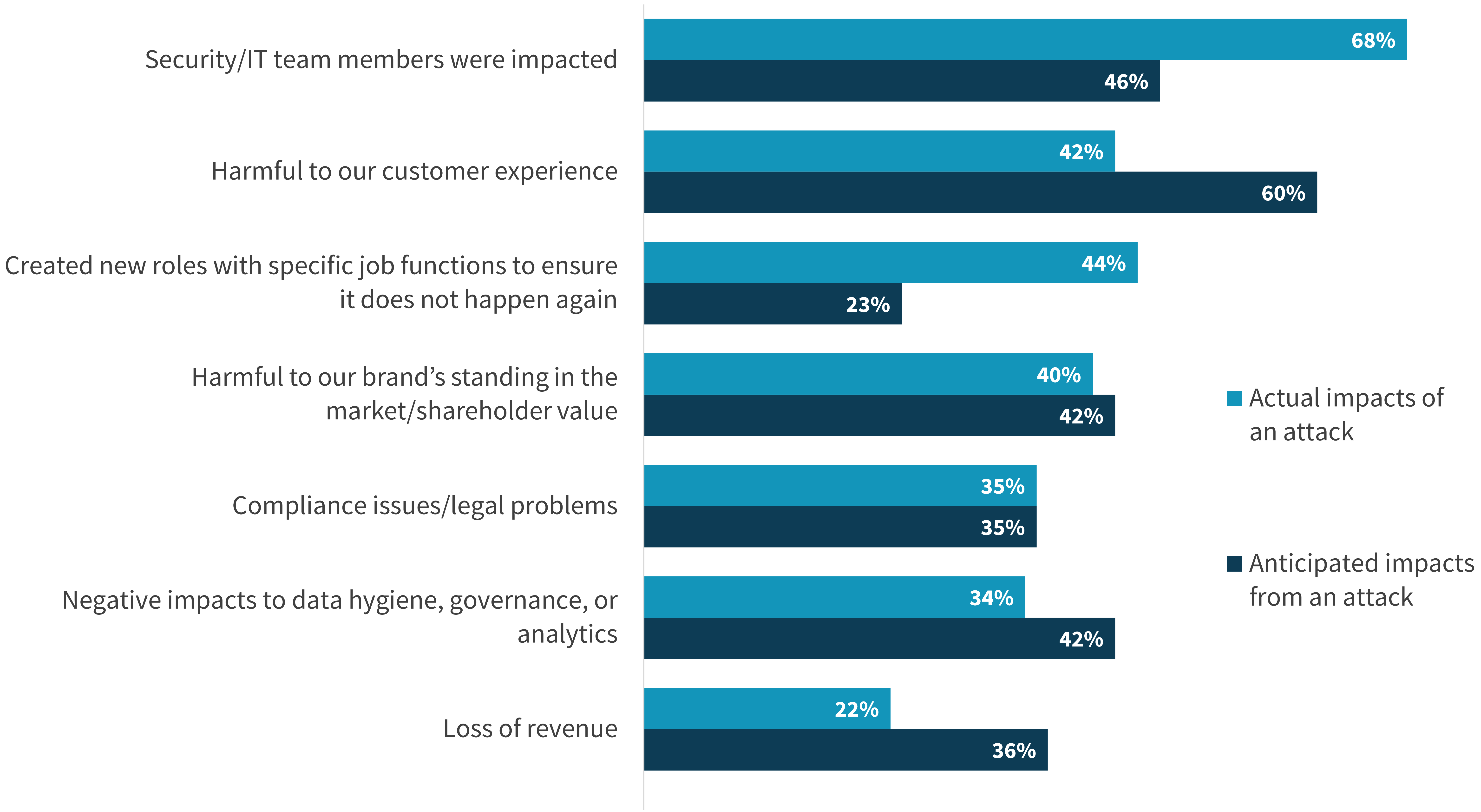
Organizational and Customer Experience Impacts Are Most Common

Among organizations that have experienced bot attacks, the most frequently cited impacts were organizational. Specifically, 68% indicated security or IT team members were impacted (i.e., disciplined, reassigned, or potentially terminated), while 44% reported their organization created new roles to better prevent bot attacks in the future. These outcomes are underappreciated among those companies who have yet to experience a bot attack, with only 46% expecting team members to be impacted and 23% anticipating new roles being created. The biggest concern of organizations yet to experience a bot attack is the negative impact to customer experience, cited by 60% of respondents. While a slightly lower percentage of organizations that have been subject to a bot attack saw this impact (42%), it remains a problematic outcome when it does occur due to the time it takes to rebuild trust.

68%

of respondents indicated security or IT team members were impacted by bot attacks.

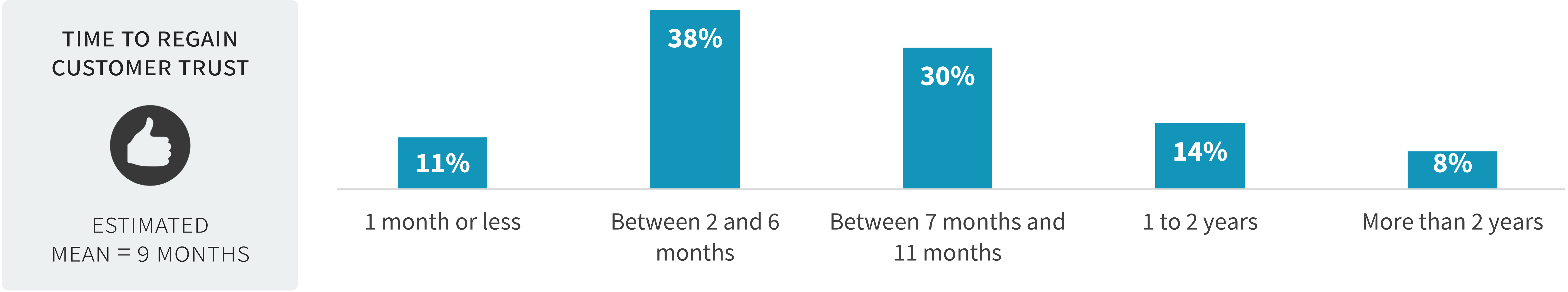
Impacts generated and expected from bot attacks.

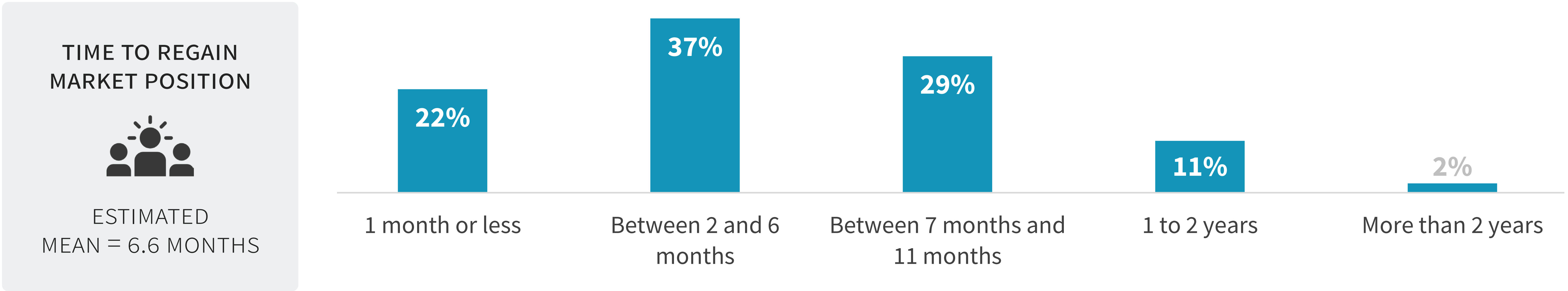


Back to Contents

> *Organizations experiencing bot attacks negatively impacting the user experience report the mean* ***time to regain customer trust is 9 months.***"

Time to recover from bot attacks.





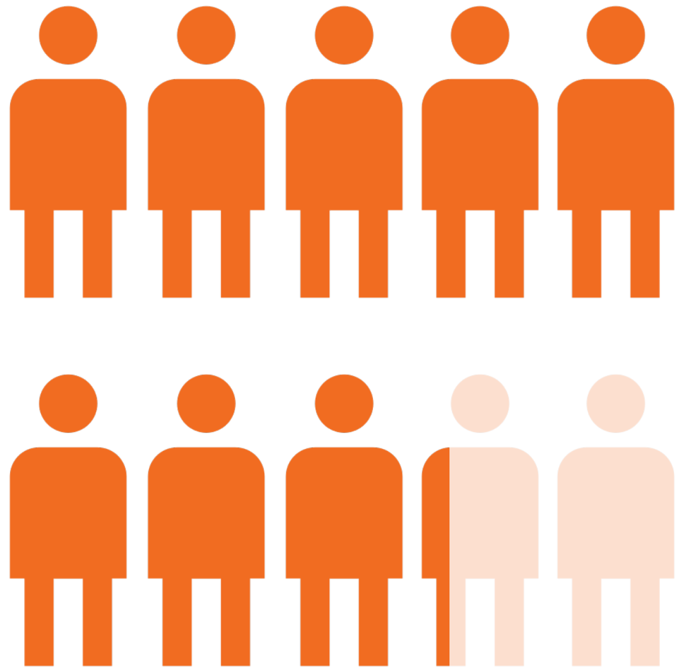
Customer Trust Can Be Difficult to Repair

Organizations experiencing bot attacks negatively impacting the user experience report the mean time to regain customer trust is 9 months. Further, 22% indicate that this exercise takes more than a year. Downstream, this can increase costs and adversely affect revenue. With one of the biggest threats to customer trust being ATO attacks, it should not come as a surprise that 40% of respondents are most concerned with account takeover over for the next year. While market position and shareholder value can be repaired slightly faster than customer trust, it remains a multi-month process for most and can take a year according to 13% of respondents. Regardless of the impact, recovering from a sophisticated bot attack does not occur overnight.

Back to Contents

Customer Experience Impacts Drive Investment In Bot Management Solutions

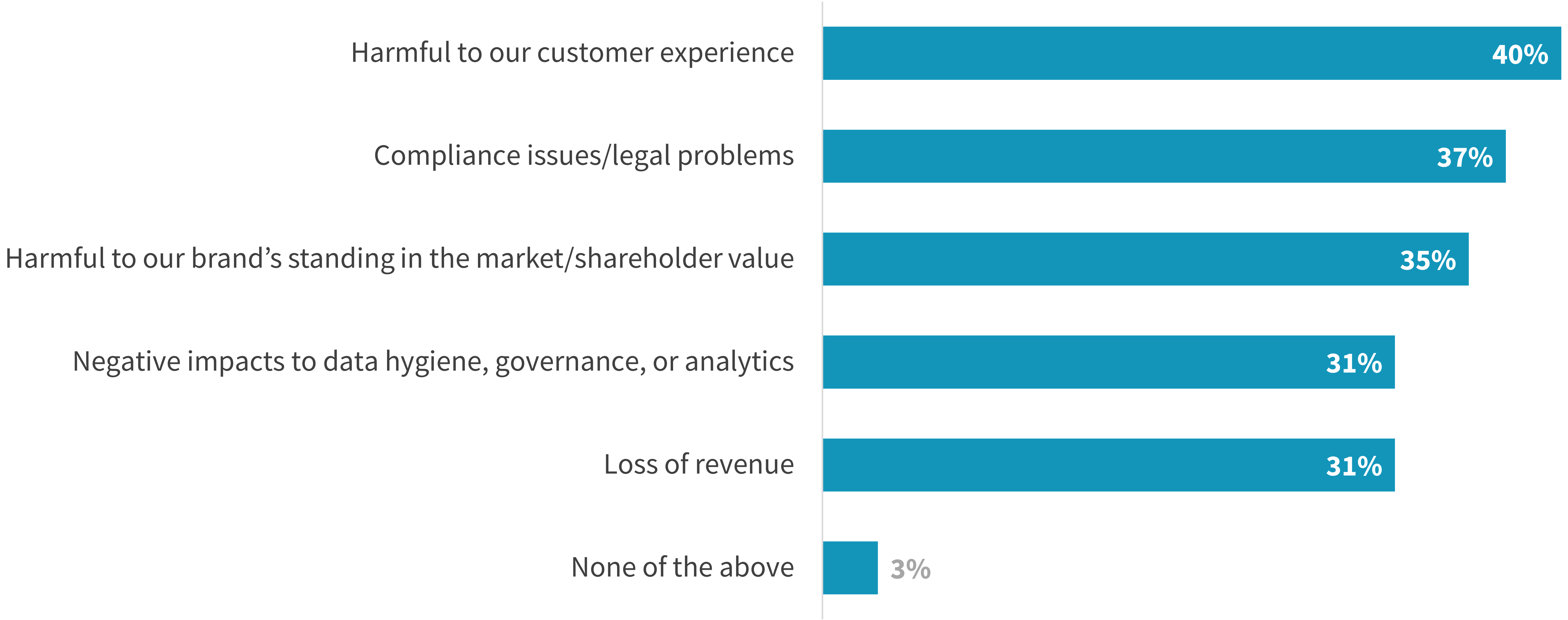
Our research found that, on average, 7% of the cybersecurity budget is allocated towards the prevention of bot attacks or bot-driven fraudulent traffic, engagement, and/or bad data. Further, 82% of organizations anticipate their spending on bot management to increase over the next 12-24 months. With negative impacts to customer experience among the most common results of a bot attack and regaining that trust a multi-quarter project, it is not surprising that these events create the greatest urgency for investment in these solutions. However, compliance issues, impacts to shareholder value, and lost revenue can all drive investment in bot management solutions as well.



82%

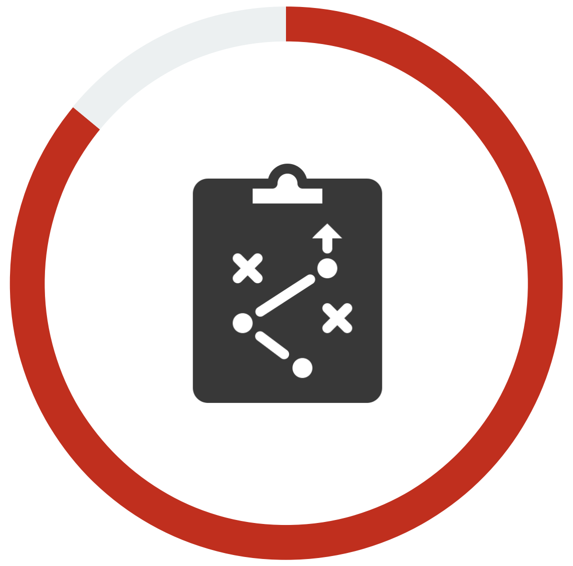
of organizations anticipate their spending on bot management to increase over the next 12-24 months.

Impacts Creating the Most Urgency for Bot Mitigation Investment.



Back to Contents

> “*While a consolidated approach can be attractive from an operational and cost perspective,* ***any efficiency gains are quickly lost if the solution is not effective in detecting and preventing attacks.***”



86%

of respondents share that most bots are capable of bypassing simple protections

Most Believe Sophisticated Bots Can Circumvent Simple Protections But Use Embedded Features

Despite an acute awareness of the sophisticated bot issue and a belief that 86% of respondents share that most bots are capable of bypassing simple protections, the majority of organizations continue to rely on embedded bot mitigation features. Nearly half (46%) use application security platforms while another 30% use the features available in discrete tools such as web application firewalls (WAF). While a consolidated approach can be attractive from an operational and cost perspective, any efficiency gains are quickly lost if the solution is not effective in detecting and preventing attacks.

Back to Contents

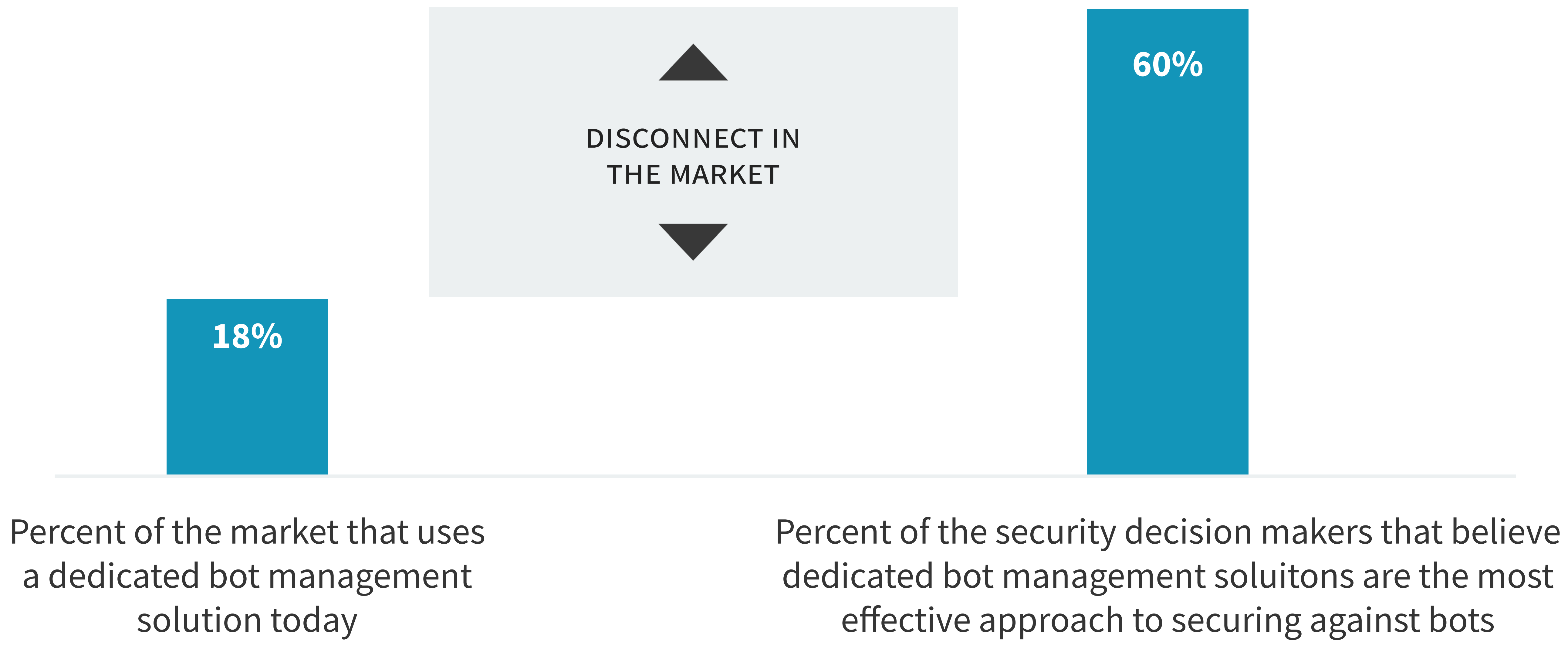
Strong Belief Specialized Bot Management Solutions Are Most Effective

There is a disconnect in the way organizations secure against bots today and the approach they believe would be most effective.

While 75% of organizations surveyed primarily leverage bot management tools that are embedded in another platform, the majority of respondents (60%) believe using a specialized, dedicated solution is the most effective approach to bot mitigation.

The question is: Are organizations going to resolve this disconnect? Our research indicates an emphatic "yes." Nearly two-thirds of respondents (65%) that believe dedicated solutions work best but work at organizations using bot management features indicate that their organization has definitive plans to change its approach to bot management within the next 12 months. The market may be at an inflection point, with a pronounced pivot toward dedicated bot management solutions on the horizon.

Usage of Dedicated Bot Management Solutions vs. Those Believing Dedicated Solutions are Most Effective



> **"Nearly two-thirds of respondents (65%) that believe dedicated solutions work best** *but work at organizations using bot management features indicate that their organization has definitive plans to change its approach to bot management within the next 12 months."*

ABOUT ESG

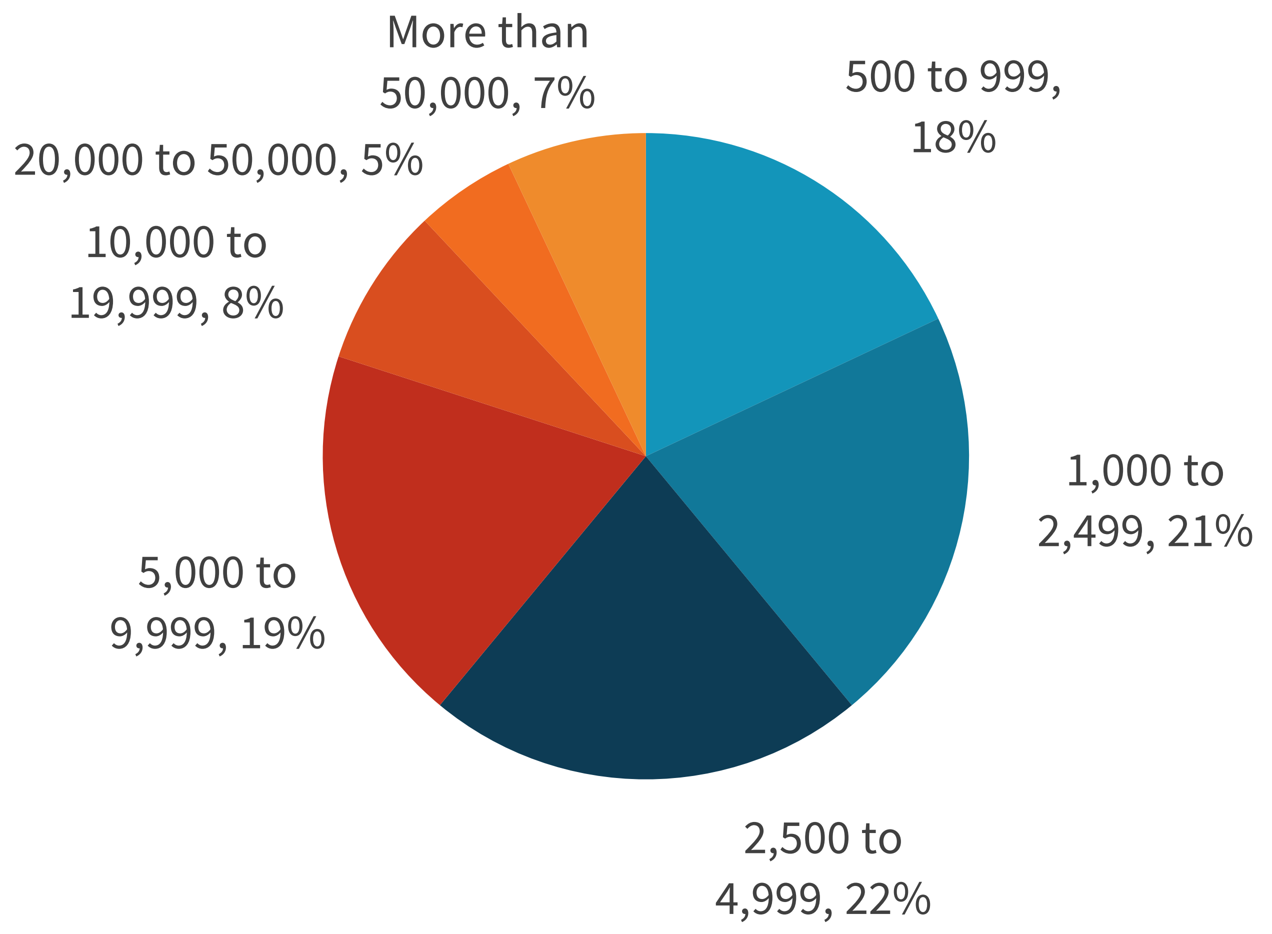
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Research Methodology

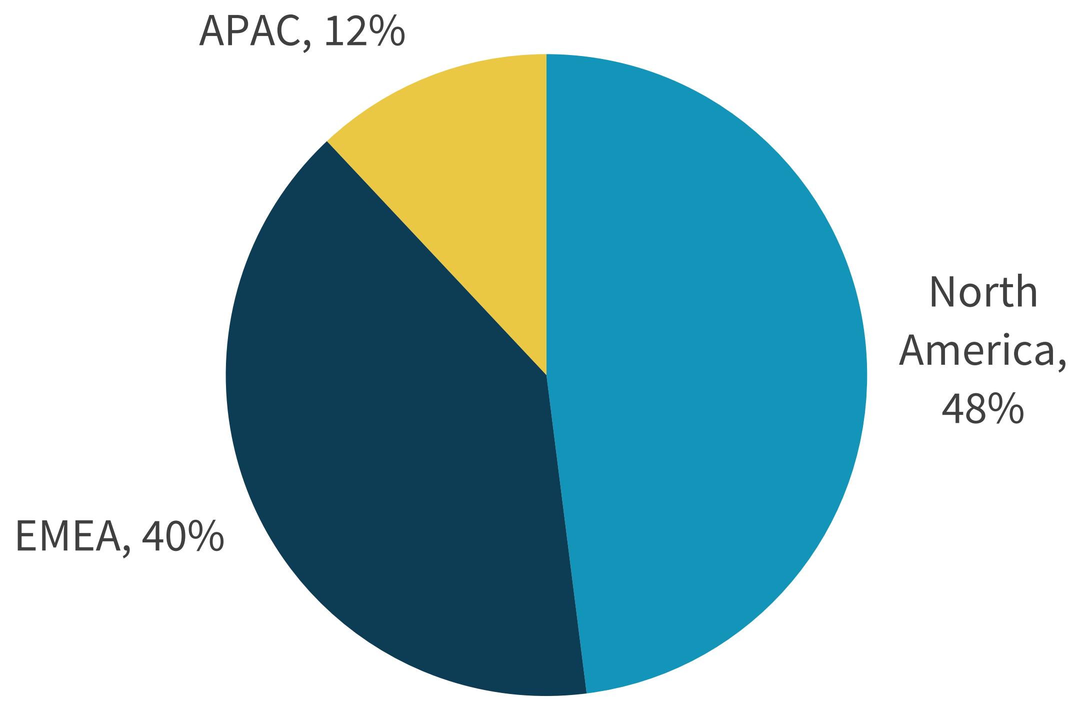
To gather data for this eBook, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America, EMEA and APAC between January 5, 2021 and January 16, 2021. To qualify for this survey, respondents were required to be senior security decision makers that are knowledgeable about the controls in use for application security at their organization. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 425 IT and cybersecurity professionals.

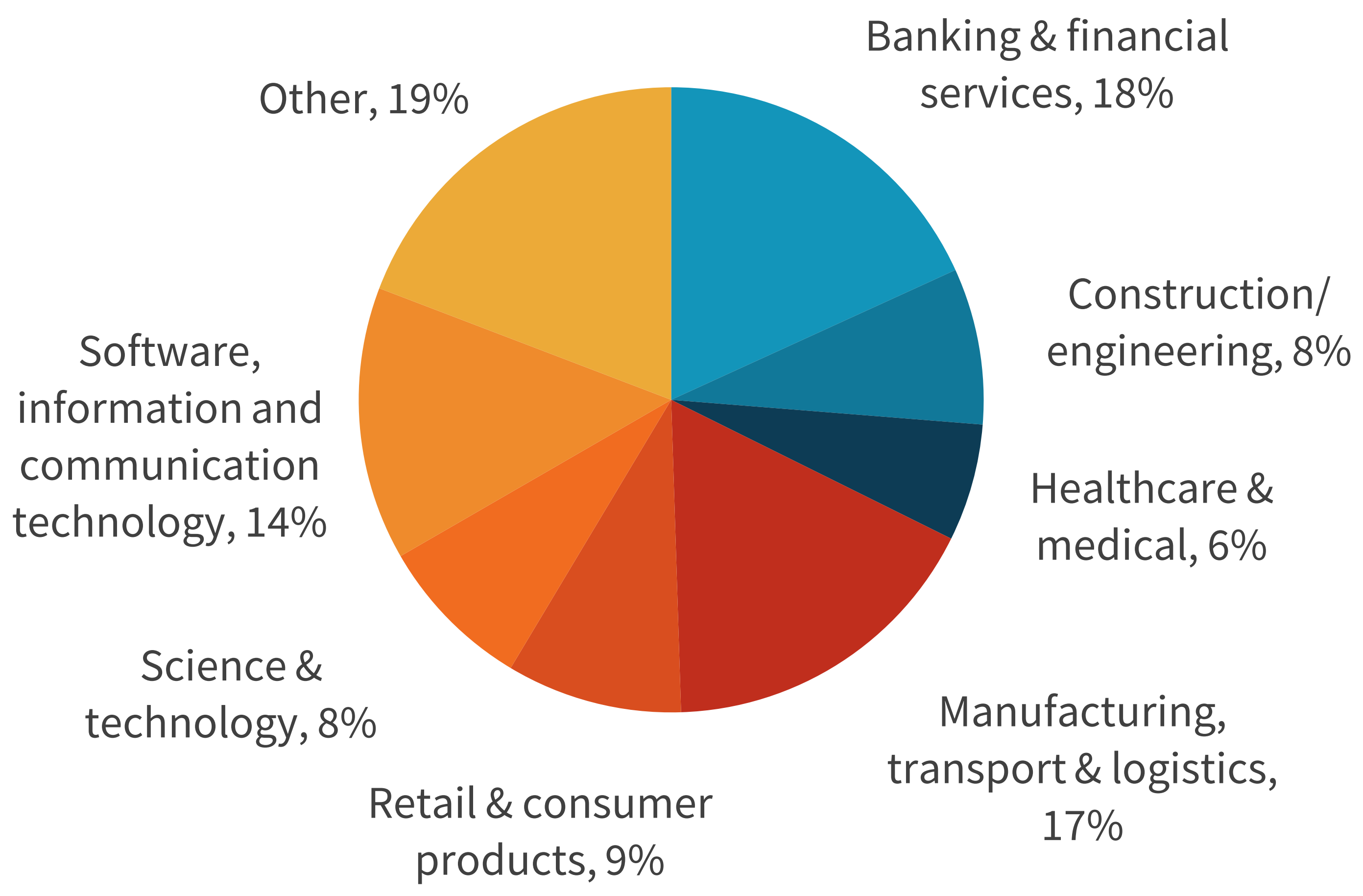
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY REGION



RESPONDENTS BY INDUSTRY



ESG
a division of TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.