coresecurity
by HelpSystems

2021 Penetration Testing Report

Introduction

Penetration tests have become an essential way to stay proactive in identifying and demonstrating the impact of security weaknesses before they are discovered and put to use by a threat actor.

Last year, Core Security, A HelpSystems Company launched its first penetration testing survey in order to better understand the role penetration testing plays in the cybersecurity landscape and provide a comprehensive picture of the effectiveness of ethical hacking strategies and the resources required to deploy a successful pen testing program.

With this second annual global survey, we continue to build on the strong baseline established by our inaugural survey and begin to track year over year changes, trends, challenges, and areas of improvement.

The results will be explored in detail in this report, providing valuable data on the following key issues related to pen testing:

- Shifting priorities with increased remote work
- Getting buy-in and funding
- Remediation and retesting
- Compliance concerns
- In-house pen testing team efforts and challenges
- Using and selecting third-party teams
- Selecting pen testing toolsets

In this report, we'll show a comparison to the results of the 2020 survey and also uncover new insights, analyzing the general evolution and advancement of the penetration testing field.

Reasons for Pen Testing

Organizations continue to pen test for multiple reasons, with 74% reporting that they perform pen tests for vulnerability management program support, 73% for measuring security posture, and 70% for compliance (Figure 1). The 3% increase in compliance from the 2020 survey may reflect the increasing number of organizations that have to adhere to specific industry standards or regulations, while the 4% increase in vulnerability management program support may be because these programs are beginning to mature and focus more on overall risk to the organization.

Common Security Concerns

Respondents reported misconfiguration (80%), phishing (79%), and poor passwords (60%) as top concerns, which aligns with last year's results (Figure 2).

Concern over misconfigurations is easily justifiable, as the switch to telework caused many IT departments to lose a certain amount of visibility into the security of network connections. While they would have controlled the Wi-Fi networks within their office buildings, home offices have private routers that may be unknowingly misconfigured. For example, many Wi-Fi networks permit remote administration by default, which can serve as a primary vector for attackers.

As organizations continue to adjust to a remote work environment, security teams may have to take more of a defensive stance, using solutions like network traffic analysis (NTA) tools, which watch network traffic instead of specific assets or the network itself. This allows security teams to monitor their entire IT environment, looking for and confirming malicious activity.

Additional concern over phishing and passwords illustrates the persisting threat that employees inadvertently pose to organizations, either by carelessly opening an email or choosing a password that is both easy to remember and easy to guess. While password tools can help enforce strong password policies to reduce risk, organizations must also take the time to frequently train and retrain employees on the importance of practicing vigilance and adhering to security policies. Making regular penetration testing routine can help employers track the efficacy of these trainings.

Reasons for Penetration Testing

Figure 1: Reasons for performing penetration tests

Why does your organization perform penetration tests?

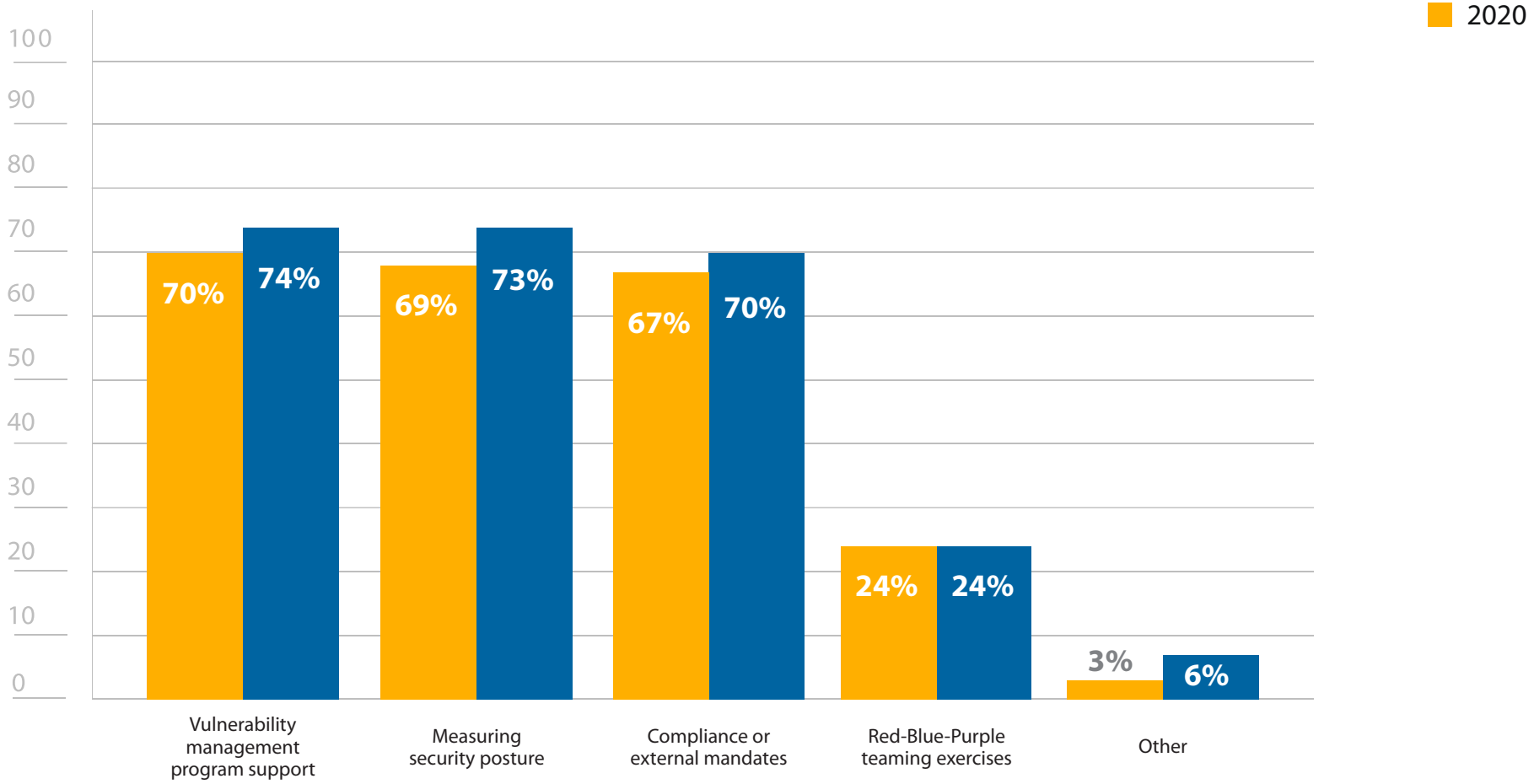
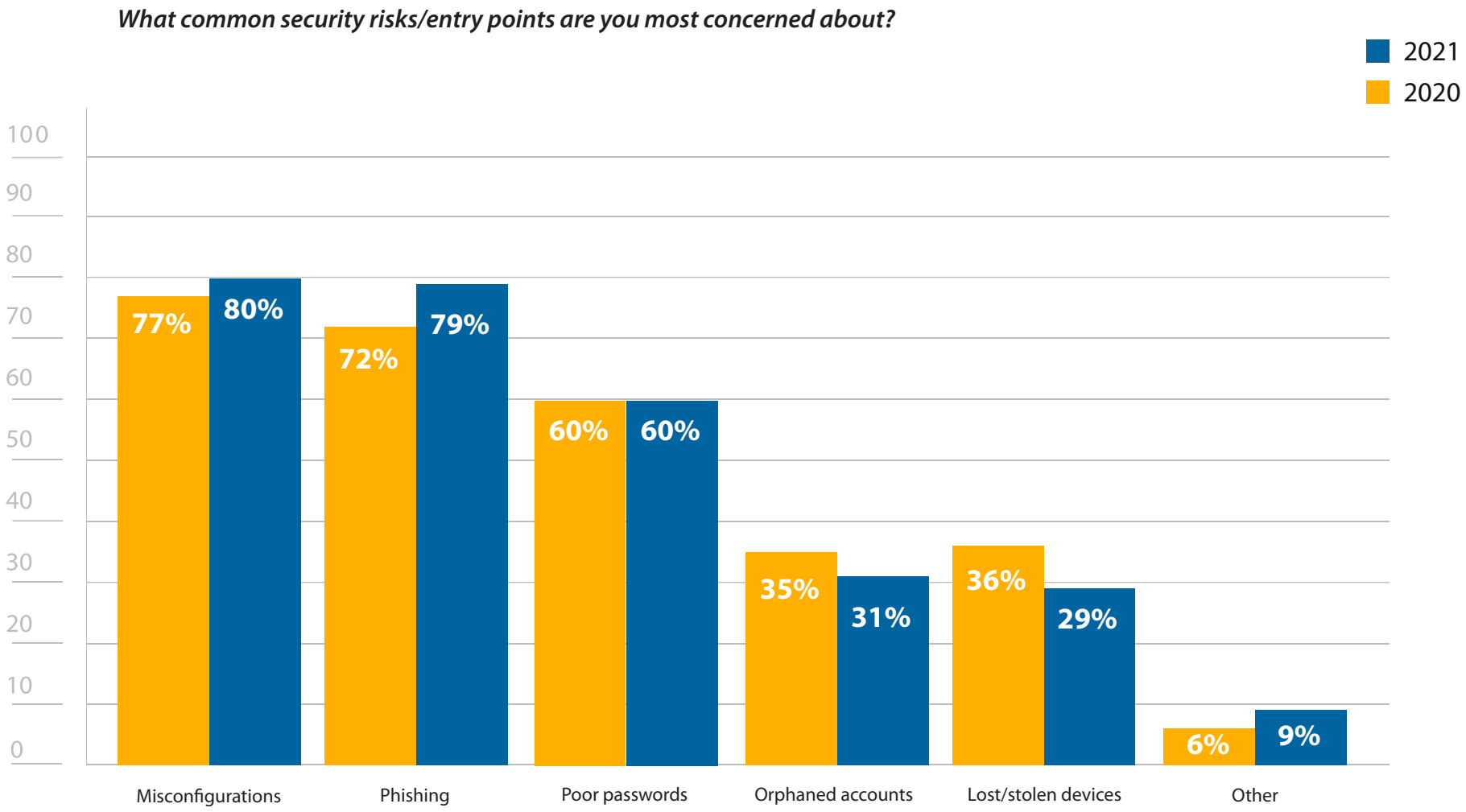


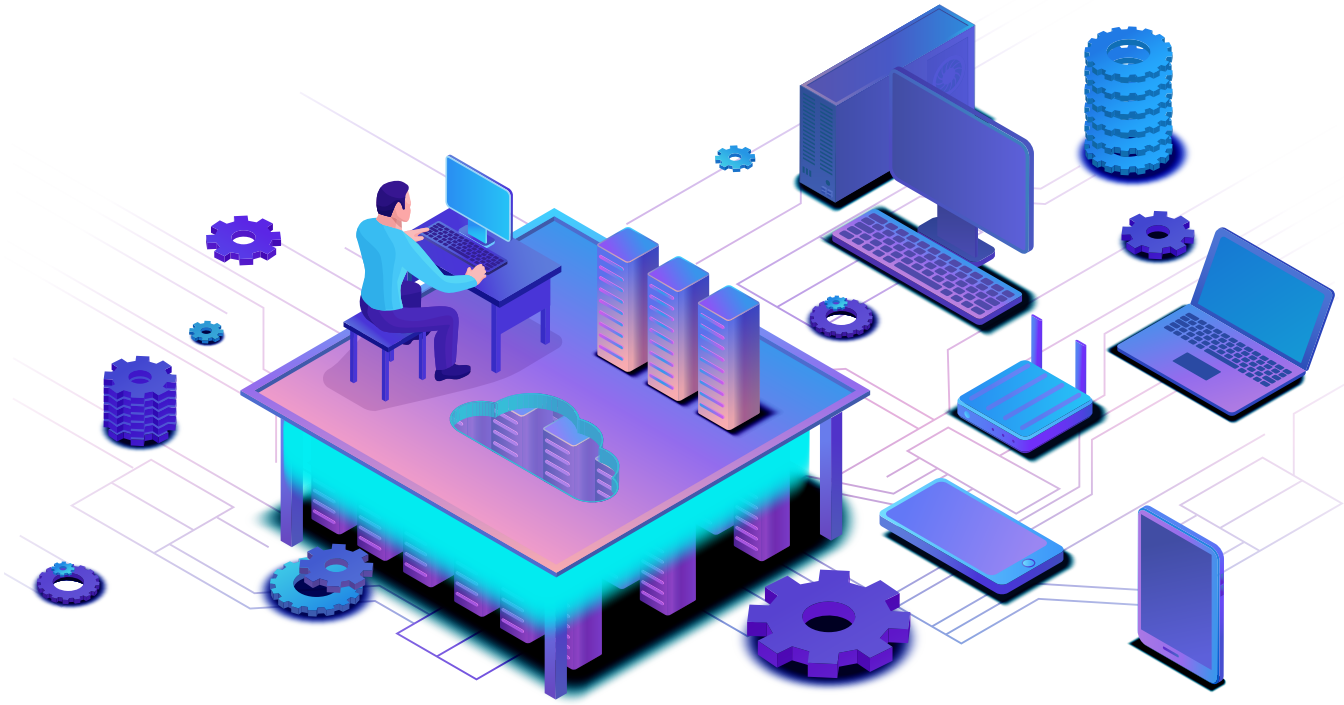
Figure 2: Common security concerns



General Penetration Testing Challenges

The value of pen testing is easily agreed upon—91% of respondents noted that penetration testing is at least somewhat important to their security (Figure 4). However, organizations continue to struggle to get others to act on the findings of pen tests, with 50% of respondents noting this as a big concern—up 4% from last year's survey (Figure 3). The mismatch between the belief that penetration testing is critical and the priority it is given seems to have grown.

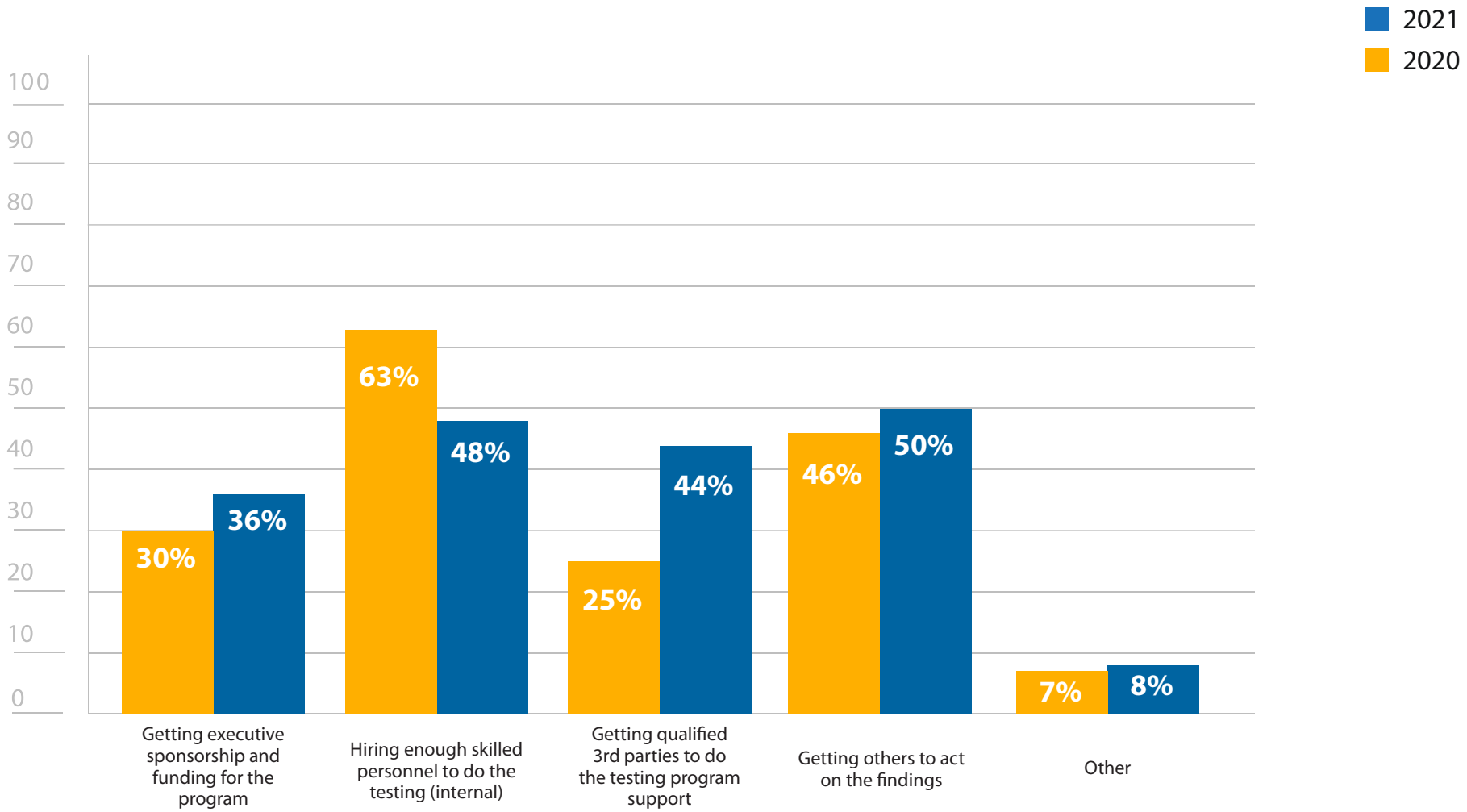
Adding to this mismatch is the 5% increase in confidence that respondents felt in their security posture, indicating that overconfidence remains a common and troubling issue (Figure 5). This overconfidence may be a factor in why there is a resistance to acting upon test findings, but more weight needs to be given to post-penetration test actions. Running a penetration test exposes security weaknesses, raising awareness about potential attack vectors. But if you don't fix the problems that you uncover and a breach occurs, you risk culpability for not acting on an issue that you knew existed.



General Penetration Testing Challenges

Figure 3: Pen testing challenges

What challenge(s) does your organization face with your penetration testing program?



General Penetration Testing Challenges

Figure 4: Importance of penetration testing

How important is penetration testing to your organization's security posture?

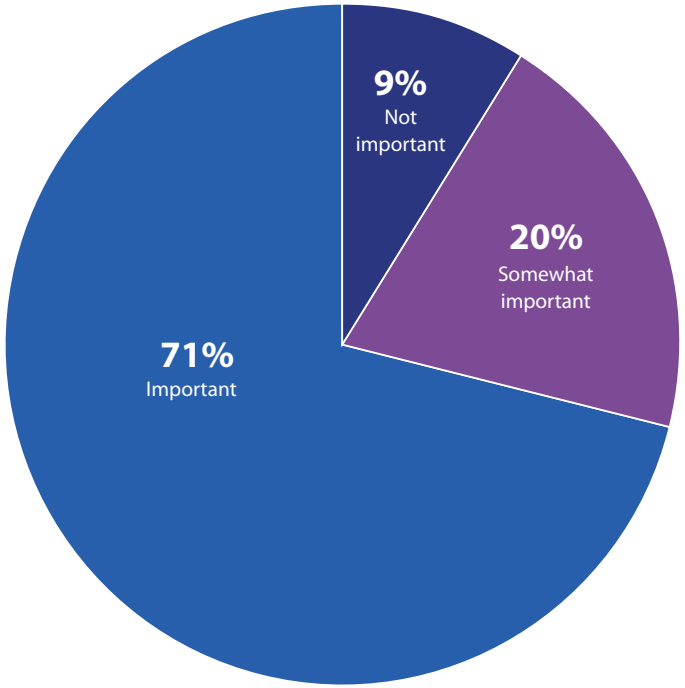
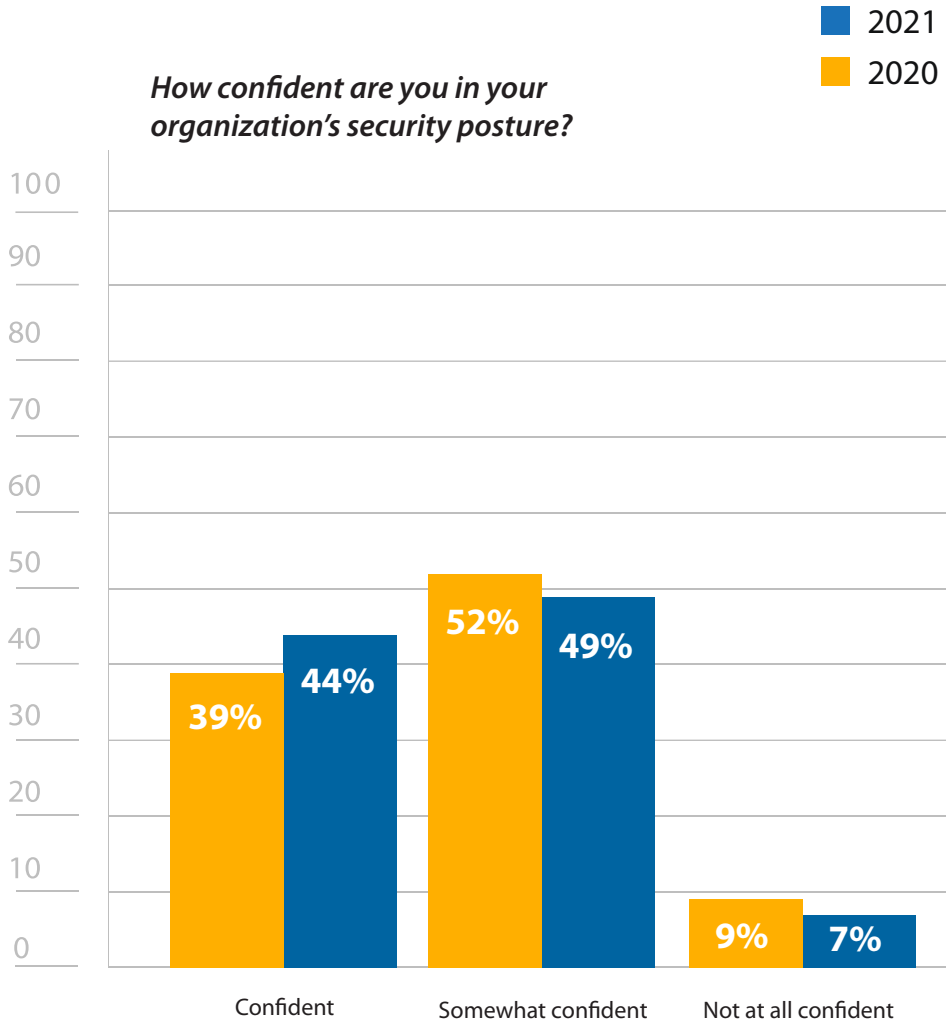


Figure 5: Confidence in security posture

How confident are you in your organization's security posture?



Compliance and Pen Testing

As seen in Figure 1, compliance to external mandates was one of the primary reasons respondents conducted penetration tests. In fact, 99% of respondents reported that pen testing held some level of importance for their compliance initiatives (Figure 6).

Every organization has some type of data that is vulnerable, so it's not unexpected that compliance has become such a large concern. Customer and patient data ranked highest at 66%, but employee data (59%), financial (50%), and intellectual property (46%) weren't far behind, illustrating just how valuable sensitive data has become to threat actors (Figure 7).

Many regulations like HIPAA, PCI DSS, SOX, GDPR, or the CMMC require proof of compliance. Pen tests are not only a way to evaluate an organization's security posture, they can help verify adherence for auditors or other authorities. Pen testing is even mandated to comply with PCI DSS. Requirement 11.3 of the Payment Card Industry Data Security Standard (PCI DSS) states that a comprehensive pen testing program must be implemented. By testing an organization's infrastructure, pen testing provides insight on security weaknesses and how an attacker could gain access to these different types of data. Additionally, for auditors, these tests can also verify that other mandated security measures are in place or working properly.

Compliance and Pen Testing

Figure 6: Importance of penetration testing for compliance

How important is penetration testing to your compliance initiatives?

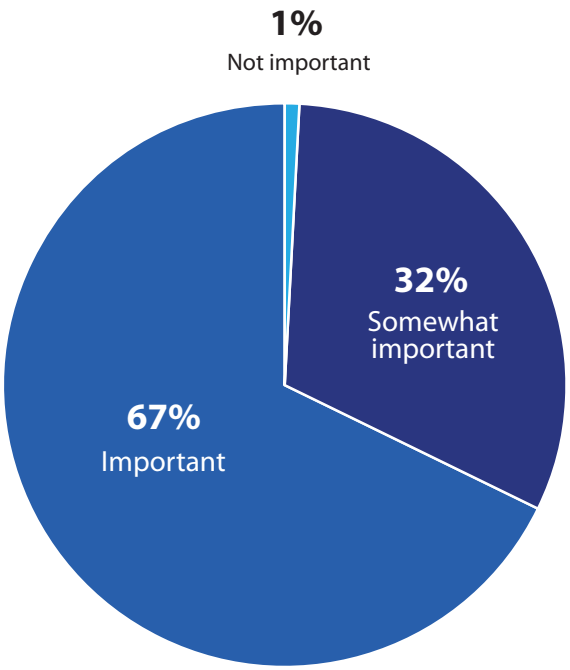
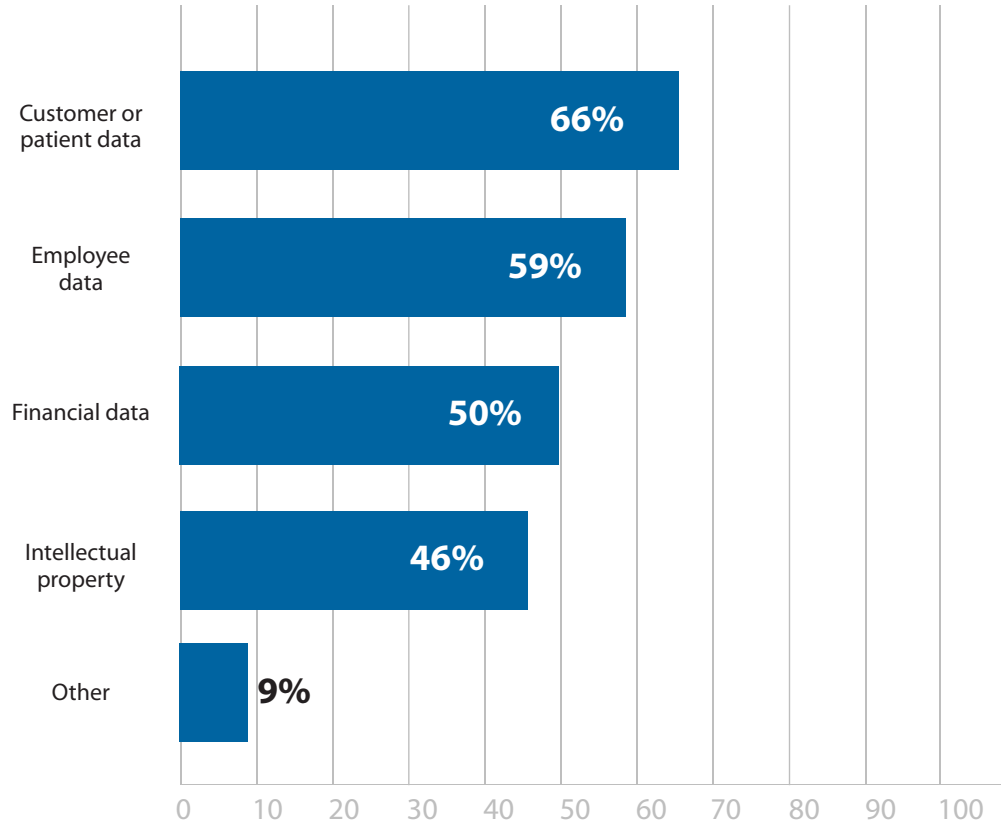


Figure 7: Data most vulnerable to hackers

What types of data at your organization is most valuable to hackers?



Phishing

Phishing attacks seem to be a never-ending threat that has only grown more sophisticated. A well-crafted phish can be easy for anyone to fall for, especially if they aren't looking for the signs. Given how many successful breaches used a phishing email as their attack vector, it is unsurprising that 79% of respondents listed it as a top concern (Figure 2).

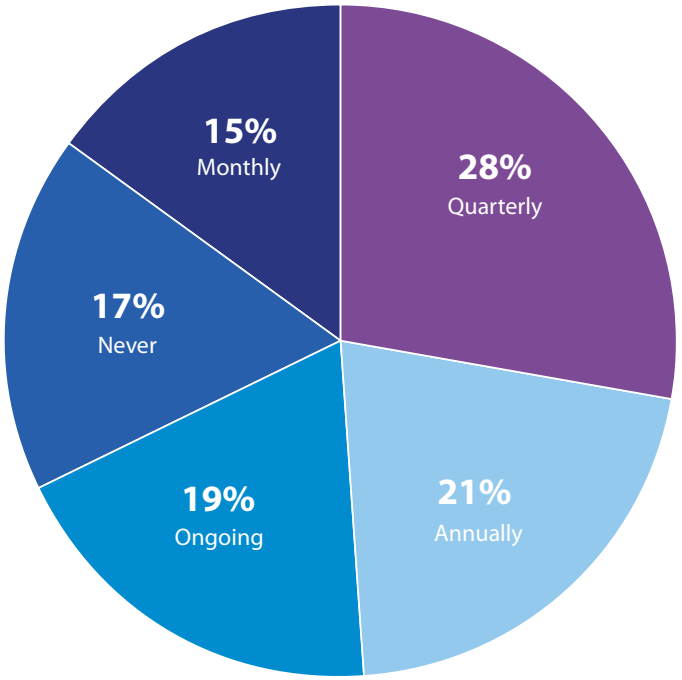
The 7% increase in phishing concerns from last year's survey (Figure 2) may be due to the surge in phishing attempts that resulted from the COVID-19 crisis. These increased phishing attempts also had more of chance to succeed. Global upheaval and heightened anxiety can cause people to become careless, clicking on an email they would normally mark as spam, particularly if it is made to look like important information that is at the top of everyone's mind.

Client-side penetration tests are more important than ever to see who is more susceptible to such attacks in your organization. In fact, they remain one of the primary ways to reduce the risk of phishing, serving as a reminder to be mindful of what's in your inbox. The results of these tests also provide a starting point when crafting employee education efforts.

However, 17% responded that they never conduct phishing simulations, which may indicate a lack of awareness of the value of phishing simulations, or a lack of resources (Figure 8). Additionally, 21% only conduct them annually, which is typically not frequent enough to accurately validate remediation efforts.

Figure 8: Frequency of phishing simulations

How often does your organization conduct phishing simulations?



Penetration Testing Frequency

This year's results are quite similar to last year. Though it would have been nice to see a drop in the number of people who never pen test (15%), it is at least promising that the number did not go up, and perhaps illustrates that once an organization introduces penetration testing, they tend keep it as part of their security strategy (Figure 9).

Of those who never pen test, many reported a lack of executive sponsorship (49%), talent/skillset (44%), or organizational maturity (44%) as primary reasons (Figure 10). This may also demonstrate a misunderstanding of the flexibility of pen testing and the many ways tests can be conducted—internal teams, third-party teams, automated penetration testing tools, etc. While it may seem like a large, expensive undertaking, penetration testing can be done on any scale or budget. For example, pen tests don't have to cover the entire infrastructure, but can instead be strategically scoped to focus on the most critical systems.

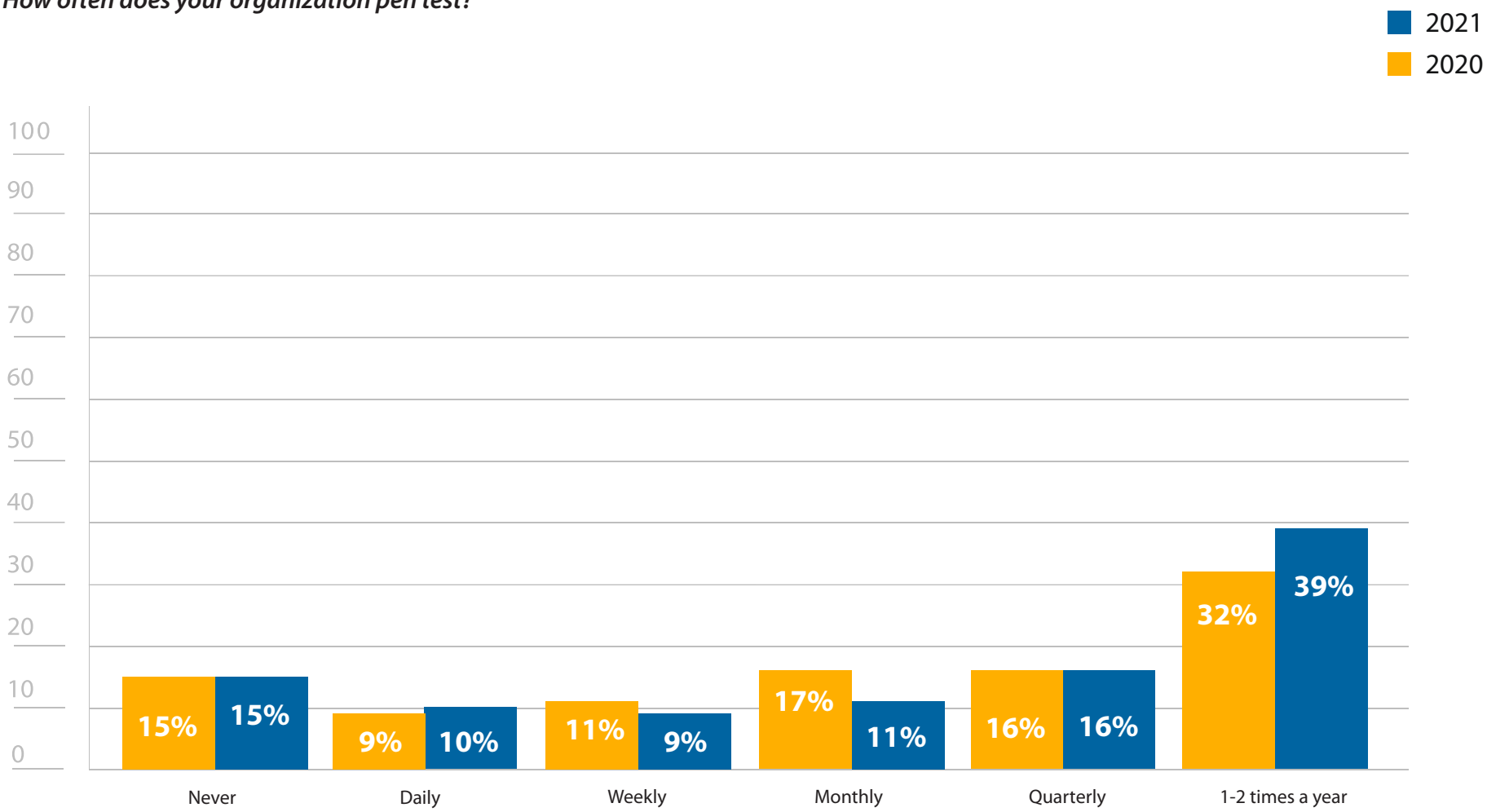
With the majority of respondents still only testing one-two times a year, retesting needs to be given more priority. An initial test helps to determine a prioritized list of security weaknesses so organizations know what remediations are most urgent. But how do you know if problems have been properly fixed? Retesting against the baseline of an initial test ensures improvements have been successfully implemented and security holes are closed.

19% of respondents reported pen testing daily or weekly, which is likely a result of confusion around the difference between vulnerability scans, which can be run daily or weekly, and a full pen test (Figure 9). This means that more of an effort likely needs to be made by the cybersecurity community in general to help make a clear distinction between the two practices and how they can work together to improve security.

Penetration Testing Frequency

Figure 9: Frequency of penetration testing

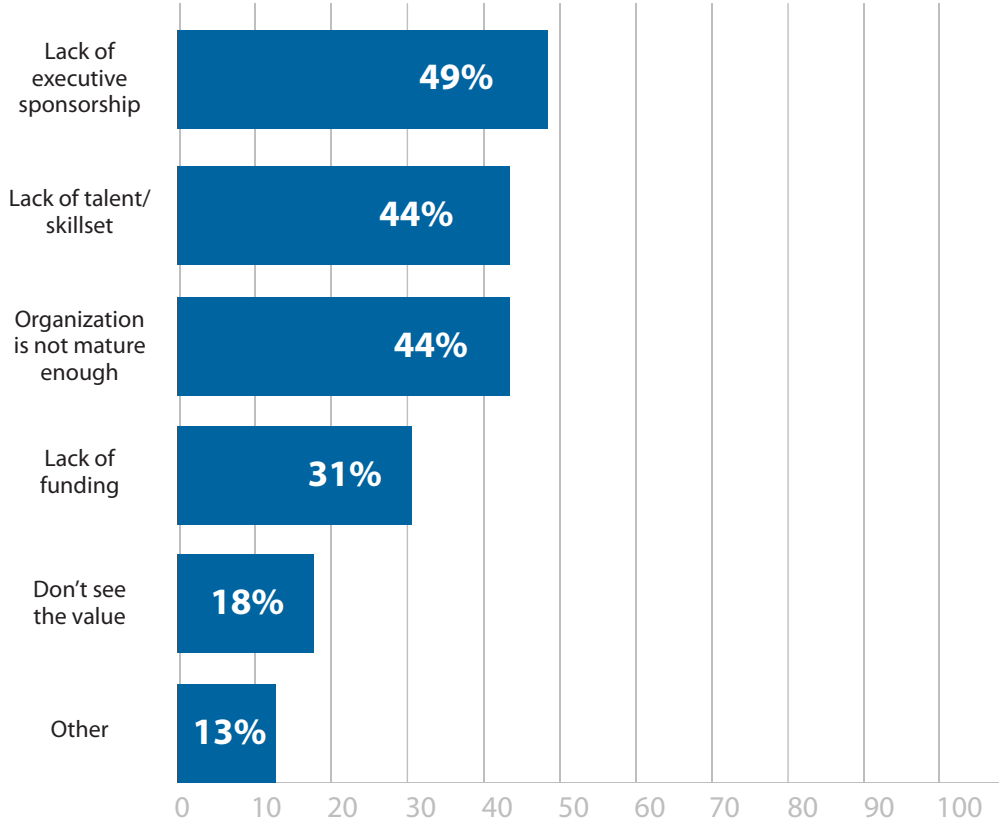
How often does your organization pen test?



Penetration Testing Frequency

Figure 10: Reasons for not pen testing

Why does your organization not conduct penetration tests?



In-House Penetration Testing Efforts

There is a noteworthy increase in the number of respondents who have an internal pen testing team at their organization (56%), with a 14% increase from last year's survey (Figure 11). This may indicate that more organizations are investing in their own pen testing teams so they don't have to rely entirely on third-party services. While third-party pen testing teams are often required or recommended for verifying compliance or conducting particularly complex tests, in-house teams are able to consistently test to ensure that compliance and security is continuously maintained.

The 3% increase in respondents with 1-2 team members (56%) from last year's survey (53%) may correspond to the rise in in-house pen testing teams (Figure 12). Often times, pen testing programs start off small, either adding a single team member or reassigning an existing security team member penetration testing duties.

Internal teams continue to boost confidence in an organization's security stance, with 46% of respondents that have internal teams noting that they are confident in their security posture, versus 31% for those without an internal team (Figure 13).

In-House Penetration Testing Staffing Challenges

There are still many reasons cited for not having an in-house penetration testing team. However, it is worth noting that at 52%, lack of funding is a 10% increase from last year's survey (Figure 14). With the economic downturn that resulted from the global pandemic, it is likely that many organizations saw their budgets significantly pared down. Given the cost of hiring skilled penetration testers, this may well have been an area that was cut.

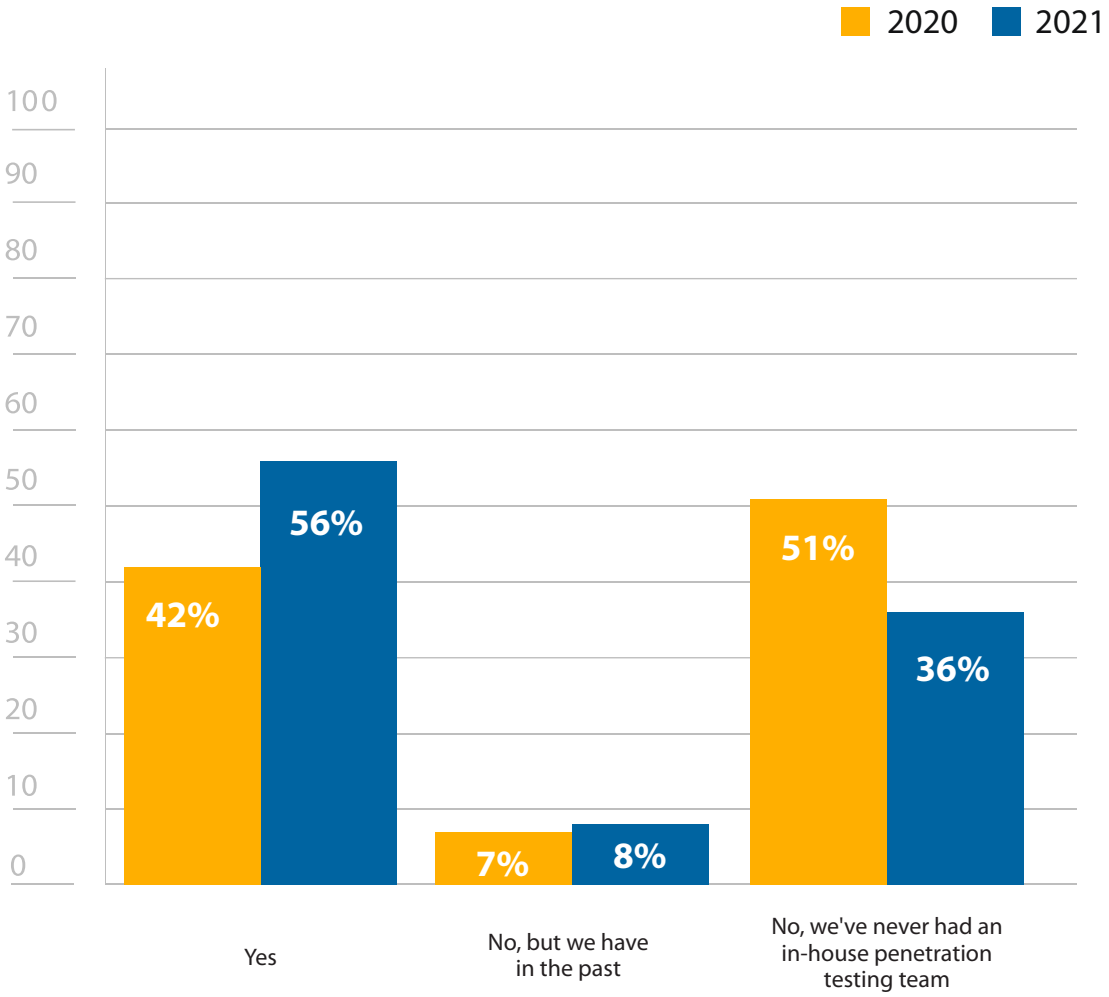
The decrease in respondents selecting lack of talent (34%) from last year (40%) may correspond to these funding issues—those not able to fund their programs wouldn't be looking for employees in the first place (Figure 14). Similarly, the increase from 28% to 43% for lack of executive sponsorship may also reflect budget reductions. Finally, the decrease from 19% to 4% of respondents that have pen testers with one year or less of experience on their teams may also reflect the unsteady economy (Figure 15). Many organizations were forced to put hiring freezes in place, so there would be limited positions for which pen testers new to the field could have applied.

The role that technology plays for internal testing was up by 9%, with 69% of respondents noting that pen testing technology has some influence on whether or not they have an in-house team (Figure 16). This demonstrates the continuing role that pen testing tools can play for in-house pen testing. Particularly as organizations begin to recover financially, penetration tools can be an affordable way to enhance pen testing efforts without increasing headcount.

In-House Penetration Testing Efforts

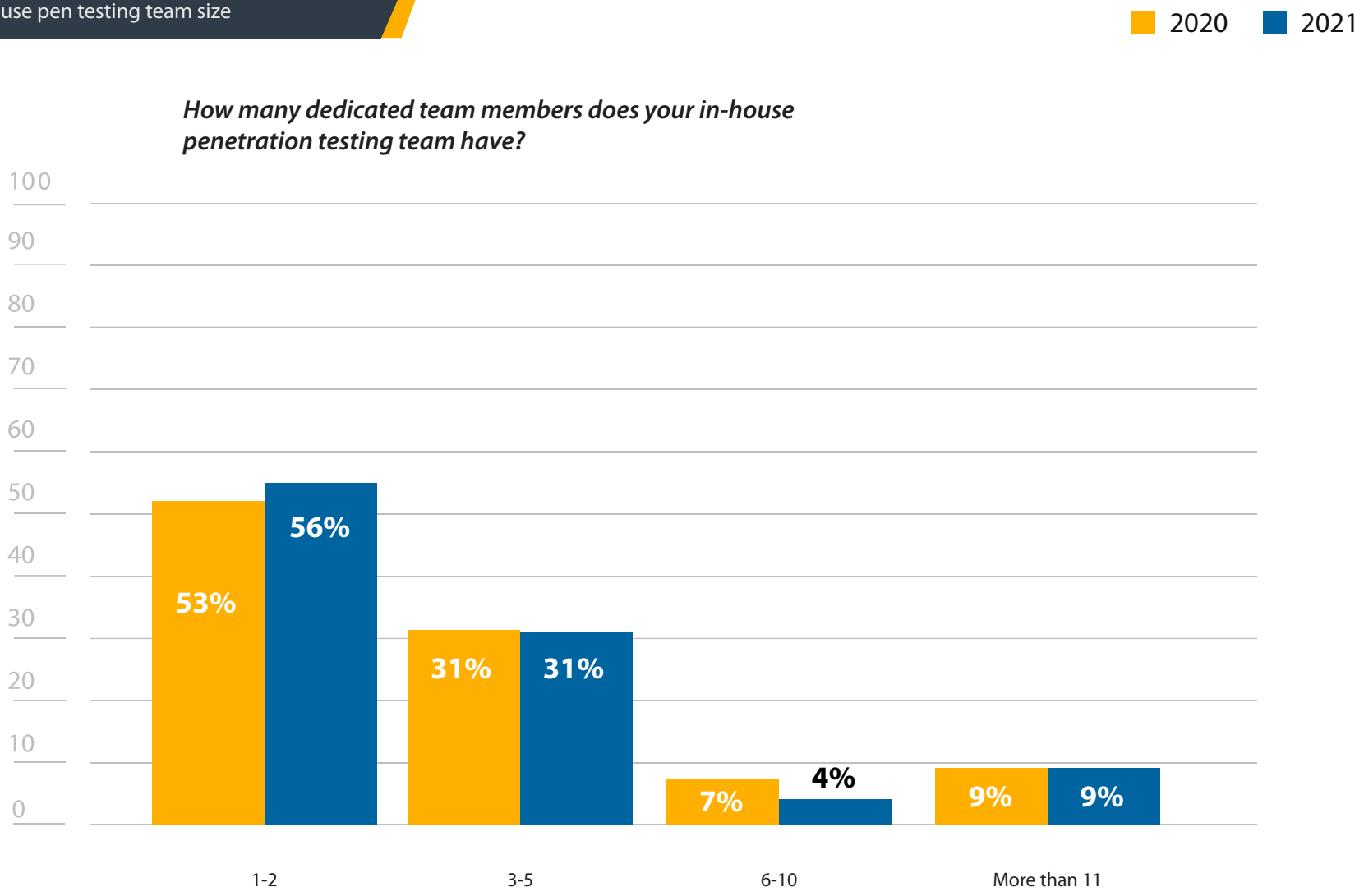
Figure 11: In-house penetration testing

Do you have an in-house penetration testing team?



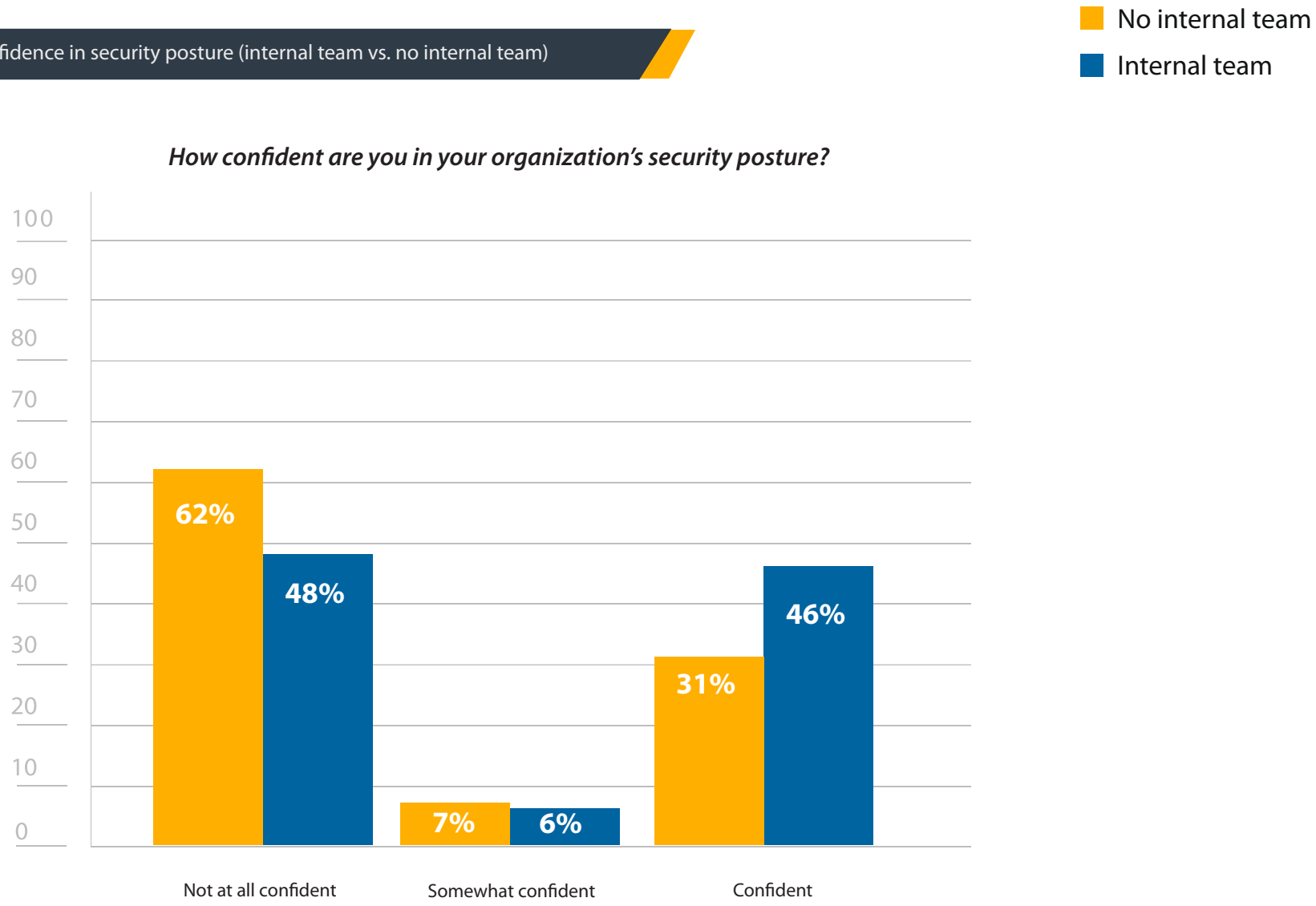
In-House Penetration Testing Efforts

Figure 12: In-house pen testing team size



In-House Penetration Testing Efforts

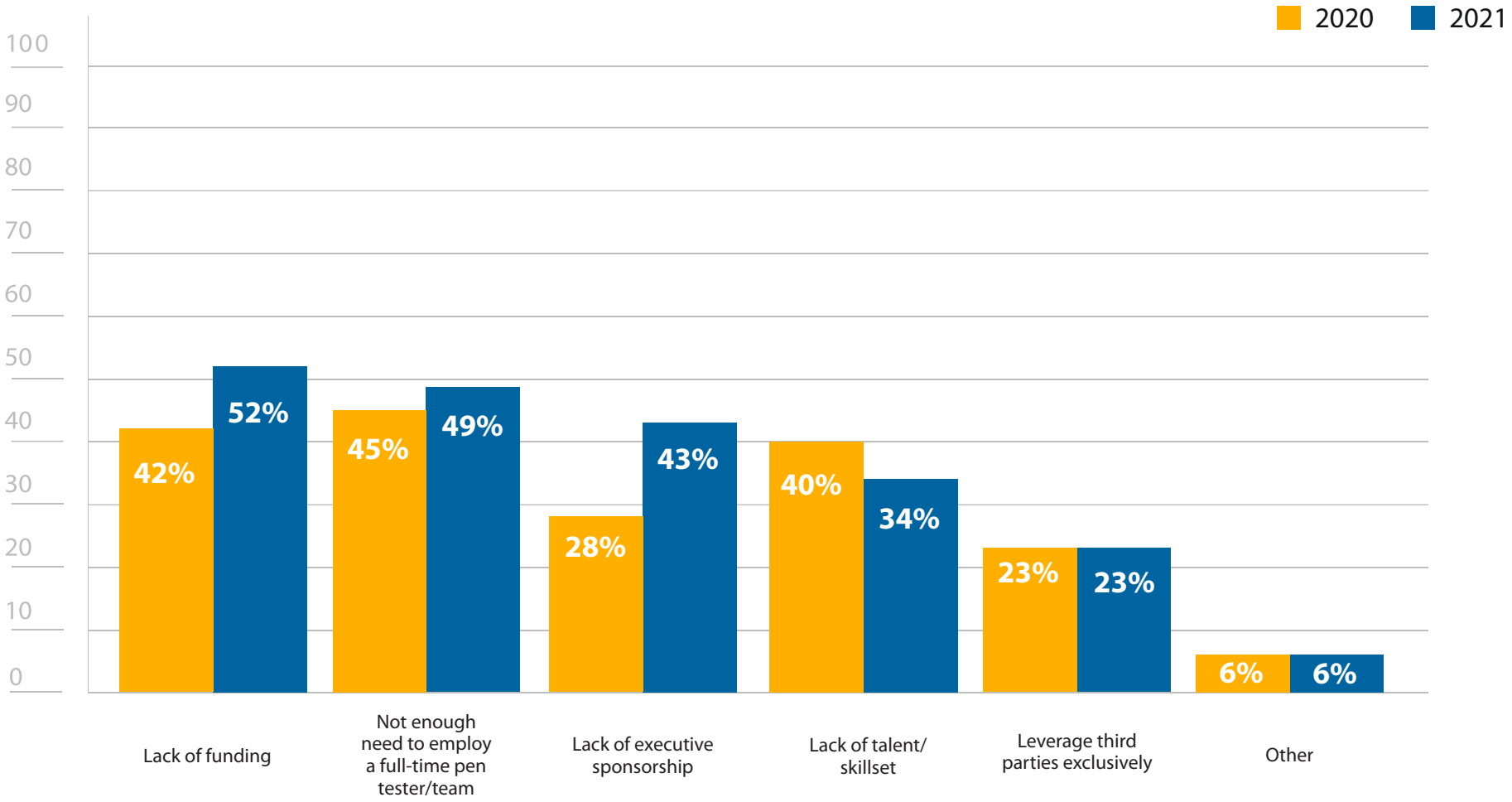
Figure 13: Confidence in security posture (internal team vs. no internal team)



In-House Penetration Testing Staffing Challenges

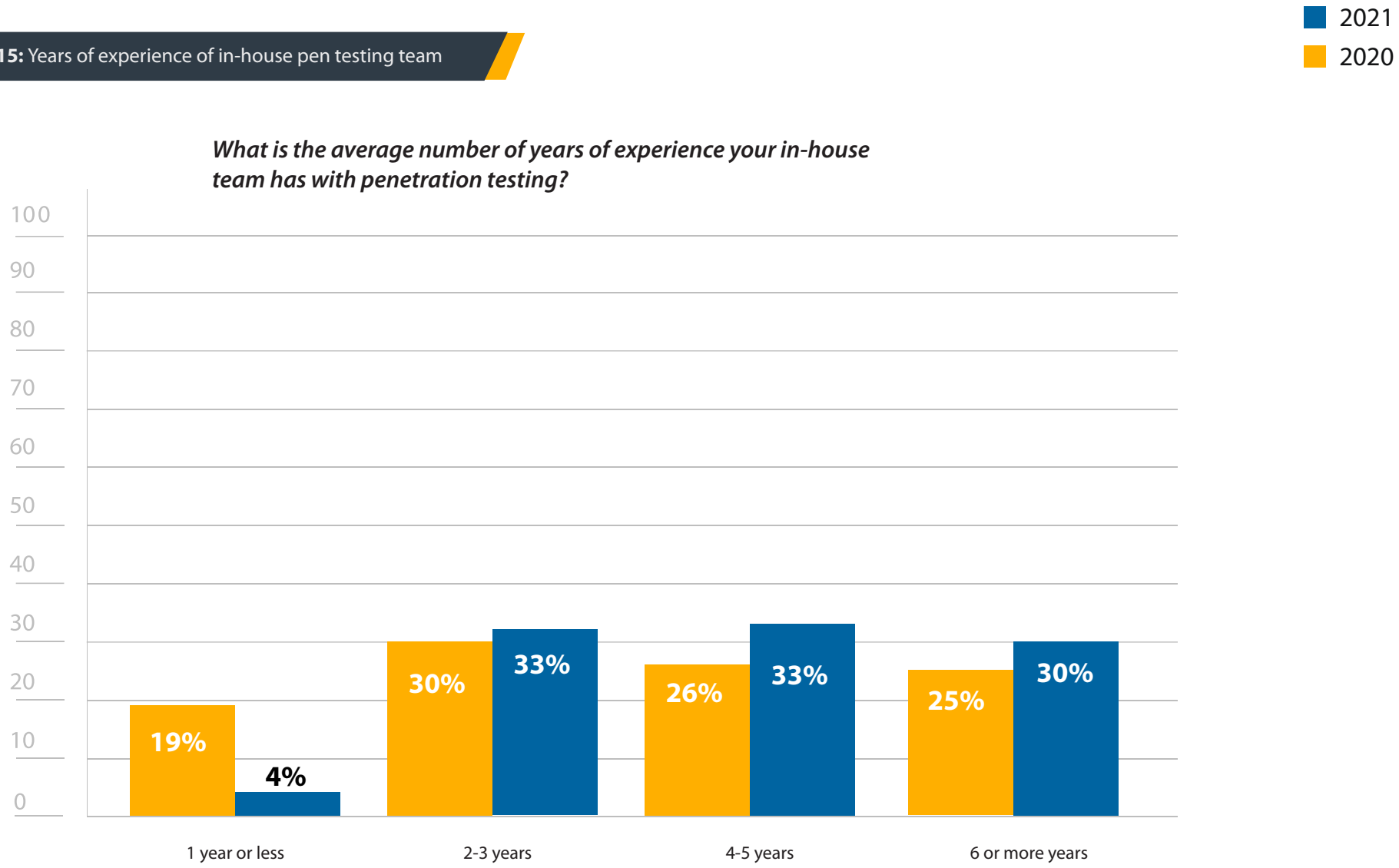
Why does your organization not have an in-house penetration testing team?

Figure 14: Reasons for not having an in-house pen testing team



In-House Penetration Testing Staffing Challenges

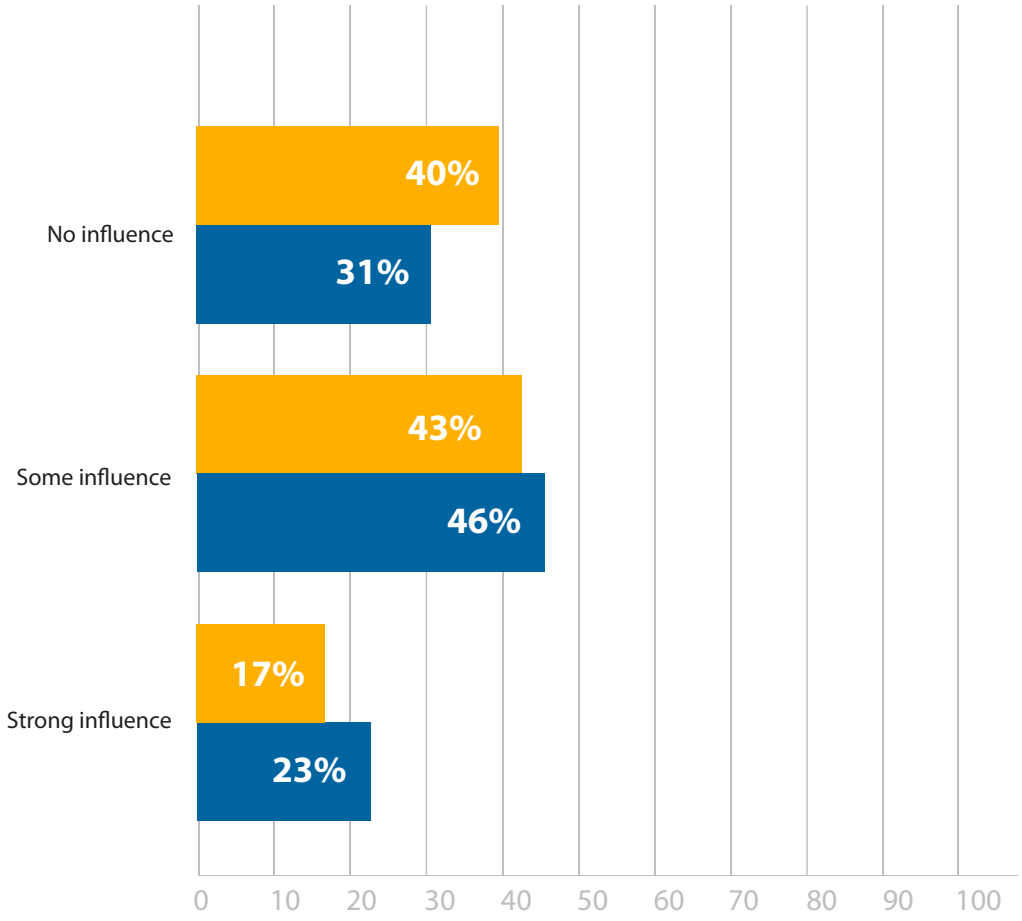
Figure 15: Years of experience of in-house pen testing team



In-House Penetration Testing Staffing Challenges

How does penetration testing technology influence your organization's decision to have or not have an in-house penetration testing function?

Figure 16: Influence of pen testing technology



Remote Work

As has been mentioned throughout this report, COVID-19 greatly impacted organizations within every industry in different ways. One of the most common changes was an unprecedented shift towards remote work, which increased the attack surface and presented additional cybersecurity challenges. Many organizations had to make this transition rapidly, which added additional challenges and increased the likelihood for misconfigurations and other errors.

It is encouraging to see that the most increased emphasis is on network security tests (45%), given how many new remote connections an organization may be experiencing (Figure 17). Many of these connections are potentially insecure, since security teams can't verify how employees are managing their home networks. Additionally, threat actors are also shifting their priorities to take advantage of these weaknesses, pivoting their strategies to focus on VPN connections or other types of network attacks. Running more network security tests will help to identify any new vulnerabilities that result from a newly remote workforce.

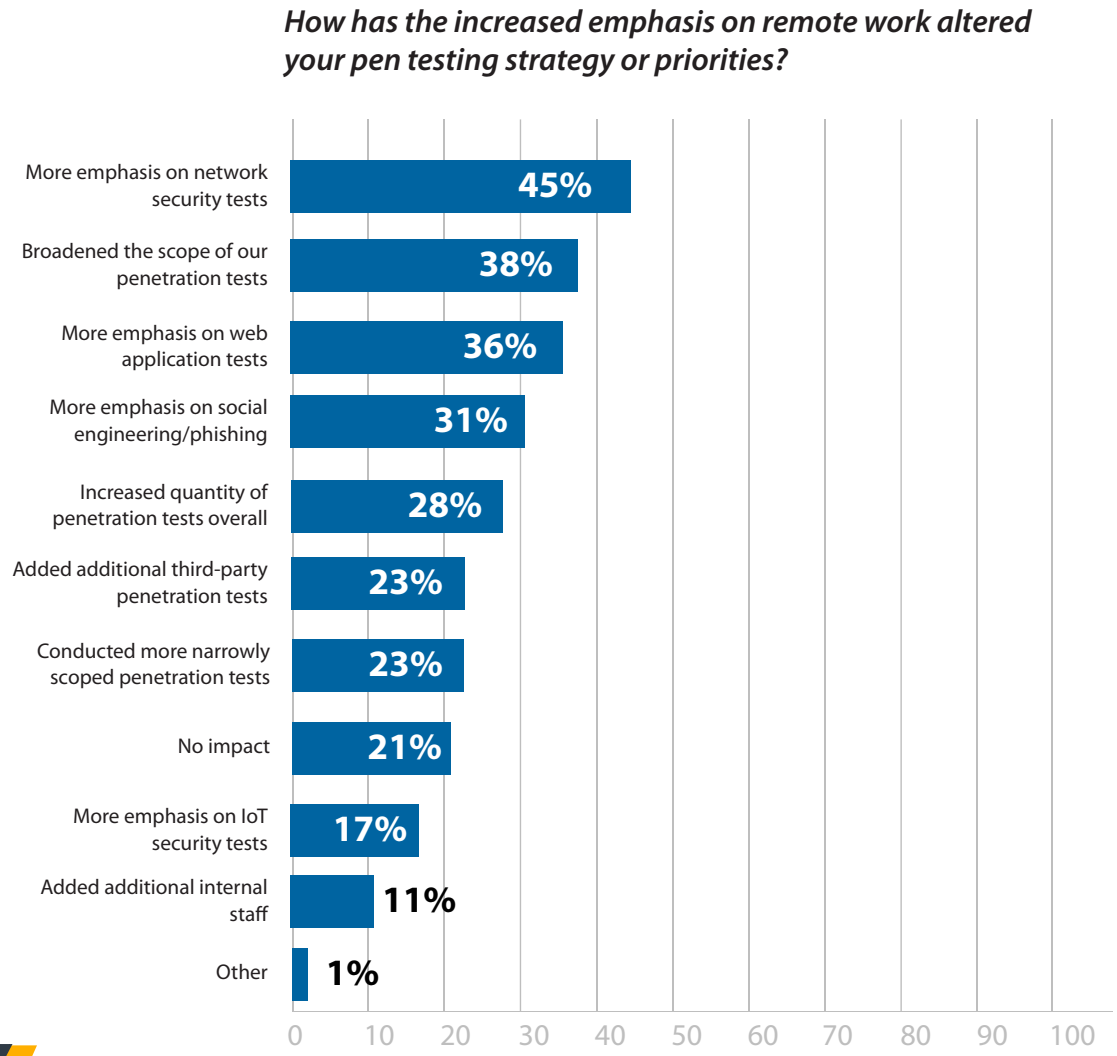


Figure 17: Effect of remote work on pen testing strategies and priorities

Third-Party Services

The frequency of conducting third-party pen tests aligns with overall testing rates, with the majority of respondents (53%) only using pen testing services annually (Figure 19). However, third-party teams are heavily used when penetration tests are conducted, with 57% of respondents noting they used third-party teams for at least half of their testing efforts (Figure 21).

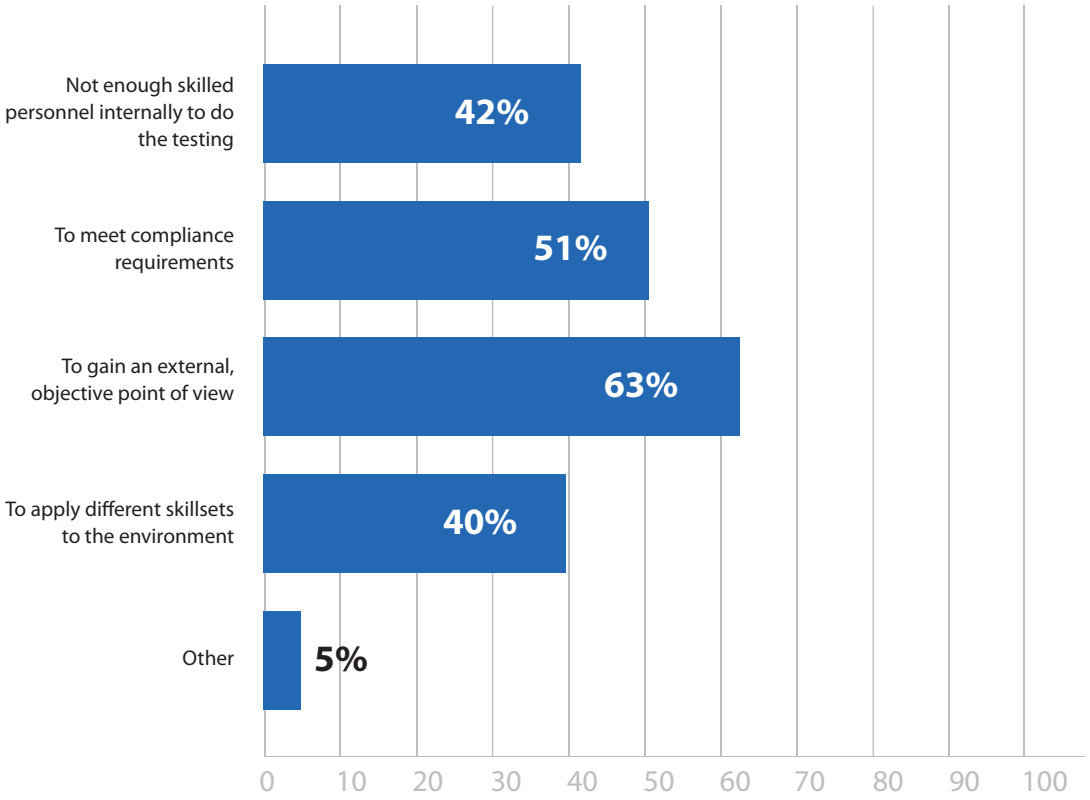
Ideally, organizations utilize both in-house teams and third-party services. Internal pen testing teams are great for ensuring consistent, standardized testing. IT environments are constantly changing, and small mistakes could easily open up new attack vectors. With ongoing testing from in-house teams, these security weaknesses can be uncovered faster. Third-party pen testers are valuable for providing different skills and an alternate view into how different threat actors may approach an attack, bringing in fresh perspectives from any internal testers. Respondents most frequently cited this external, objective mindset (63%) as a reason for why they utilize third-party teams (Figure 18).

The desire for a fresh perspective may also help explain why organizations frequently change third-party teams. 77% of respondents indicated that they shift to a different team at least every two-three years (Figure 20). Additionally, while it is not mandated by any specific compliance requirement, rotating between at least two firms is typically considered an industry best practice. Given how many respondents cited compliance (51%) as a reason for using third-party teams, this may also be part of why changing providers is so common.

Third-Party Services

Figure 18: Reasons for utilizing third-party pen testing services

Why does your organization utilize third-party penetration testers?



How often do you conduct third-party penetration tests?

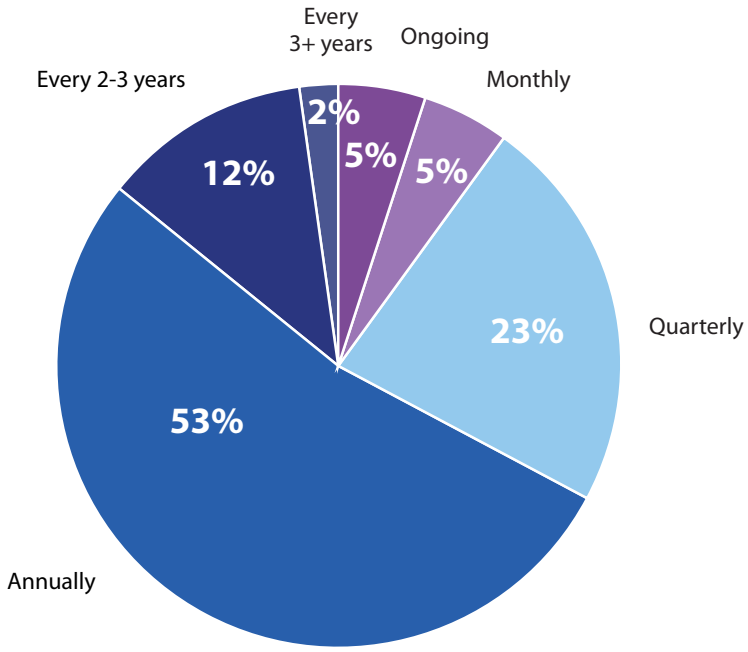
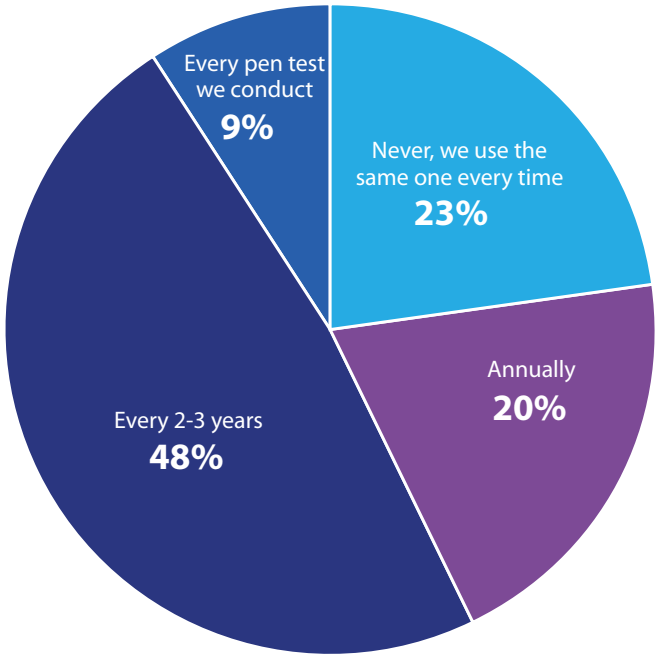


Figure 19: Frequency of third-party pen tests

Third-Party Services

Figure 20: Rotation frequency of third-party pen testing services

How often do you change which third-party pen testing service you work with?



What is the current split between using internal and third-party pen testing resources?

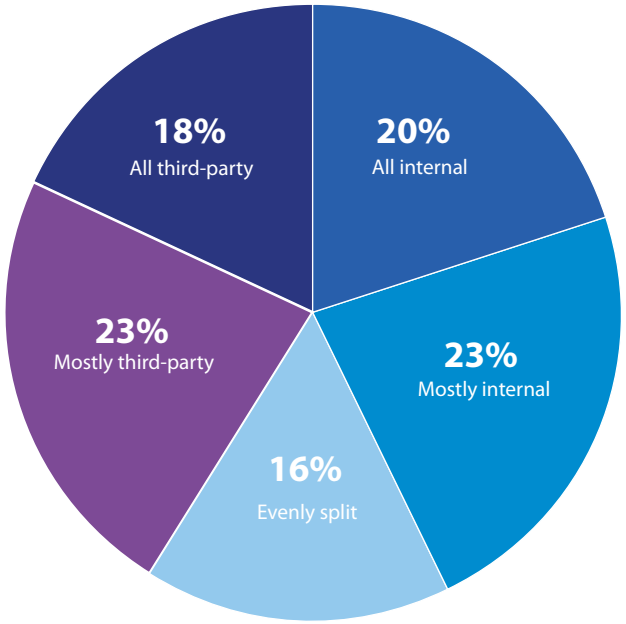
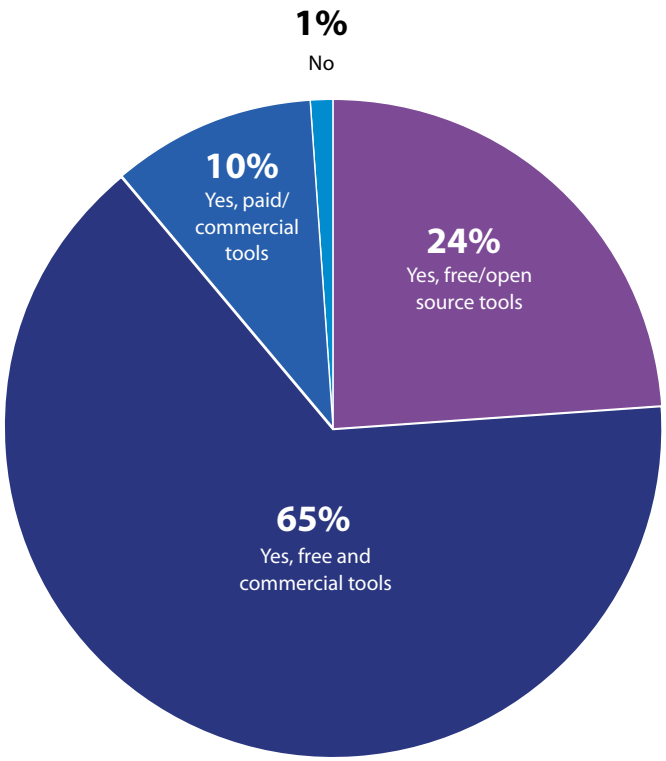


Figure 21: Rotation frequency of third-party pen testing services

Penetration Testing Tools

Figure 22: Active use of penetration testing software

Does your organization actively use penetration testing software or tools?



Only one percent of respondents indicated they don't use any type of penetration testing tool, which underscores how crucial solutions are to the pen testing process, and how important it is to find ones that are reliable and effective. The preference appears to be a combination of enterprise and open source tools, with 65% of respondents indicating that they use both (Figure 22). Given the complexity of penetration tests, a full tool stack is required, with each solution meeting different needs. For example, enterprise pen testing tools are often lauded for their reliable commercial grade exploit libraries, which are not only regularly kept up to date, but also expertly written and verified.

Though a variety of tools appear necessary, some organizations may be looking to simplify with more comprehensive tools, since features and functionality (85%) were the most commonly cited criteria for evaluation solutions (Figure 23). While no single tool can do it all, some solutions do prioritize centralization and integration, so that testers can have a more streamlined experience.

Reporting was the most sought after feature in paid penetration testing tools, with 71% of respondents listing it as an important feature (Figure 24). While every aspect of a penetration test is important, it is almost meaningless if the findings aren't well presented in clear, standardized report. Manual reporting can be time consuming and often varies considerably in quality. Automated reporting functionality can both maintain consistency and increase efficiency, producing thorough reports that can be used for remediation prioritization, or for auditors evaluating for regulatory compliance.

Penetration Testing Tools

Figure 24: Most important features in pen testing software

What features are most important in paid penetration testing software/tools?

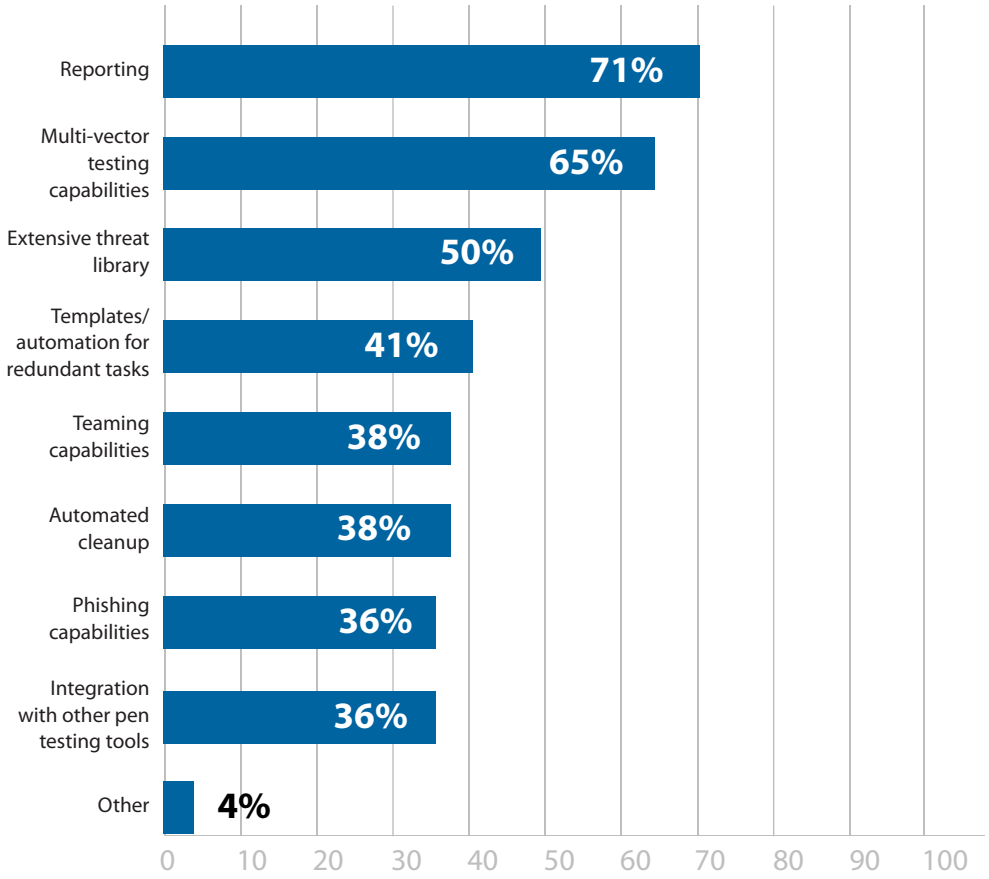
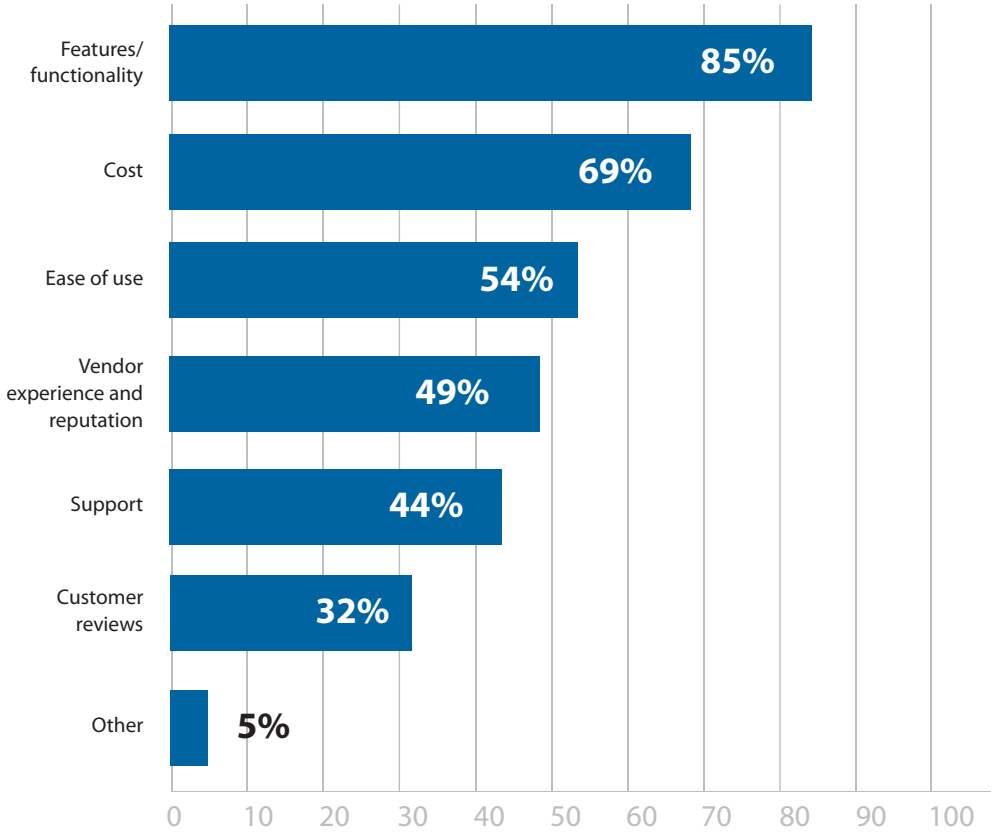


Figure 23: Most important criteria for evaluating pen testing software



What criteria do you consider most important when evaluating penetration testing software?

Demographics

Figure 25: Regions surveyed

Which region is your organization headquartered?

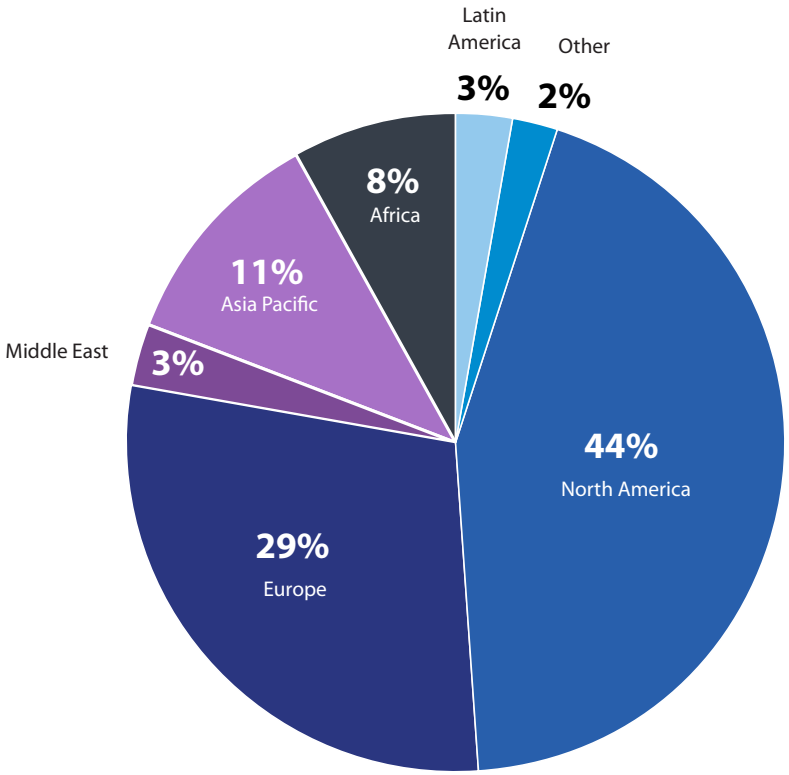
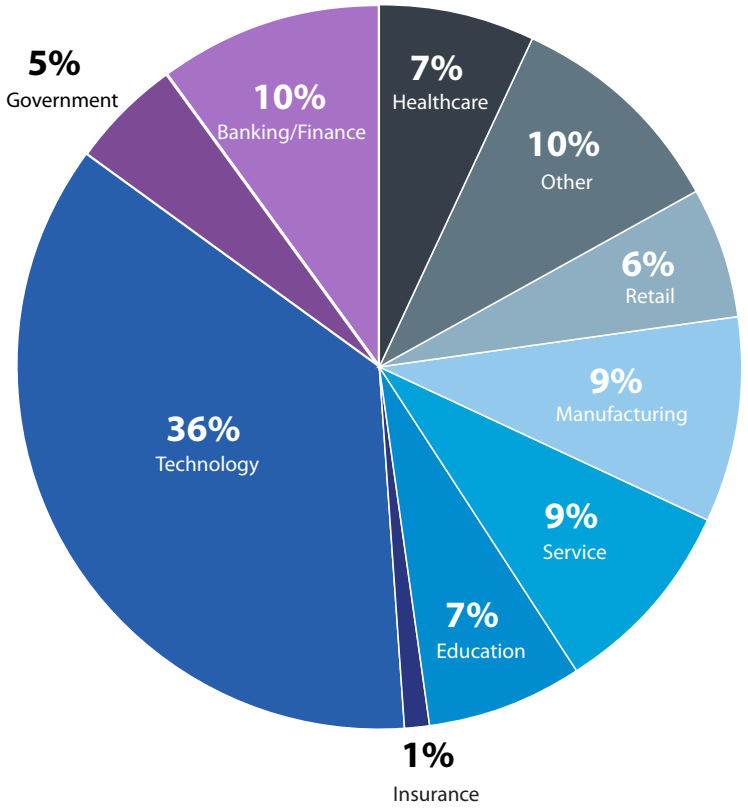


Figure 26: Industries surveyed

What is your primary industry?



This report is based on the results of a comprehensive survey of cybersecurity professionals around the globe with the aim of presenting an accurate picture of how penetration testing is utilized by different organizations and to provide insights about the effectiveness of ethical hacking strategies. The respondents represent a diverse cross-section of industries, company size, job level, and region.

Demographics

Figure 27: Job levels surveyed

What is your job level?

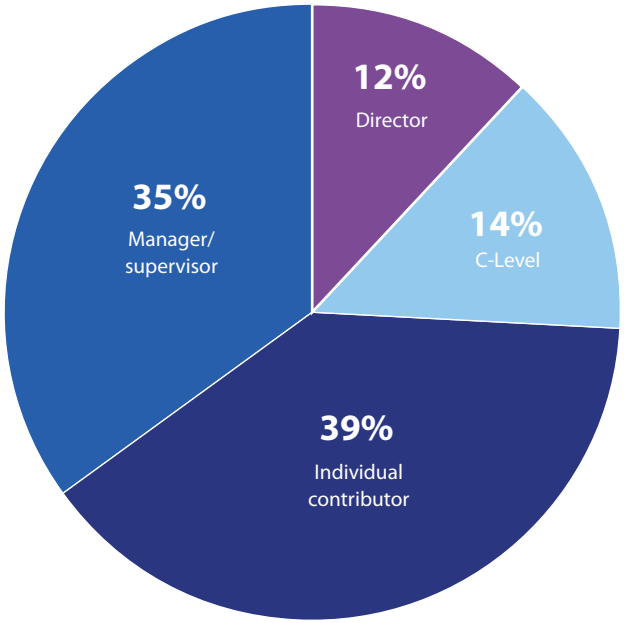
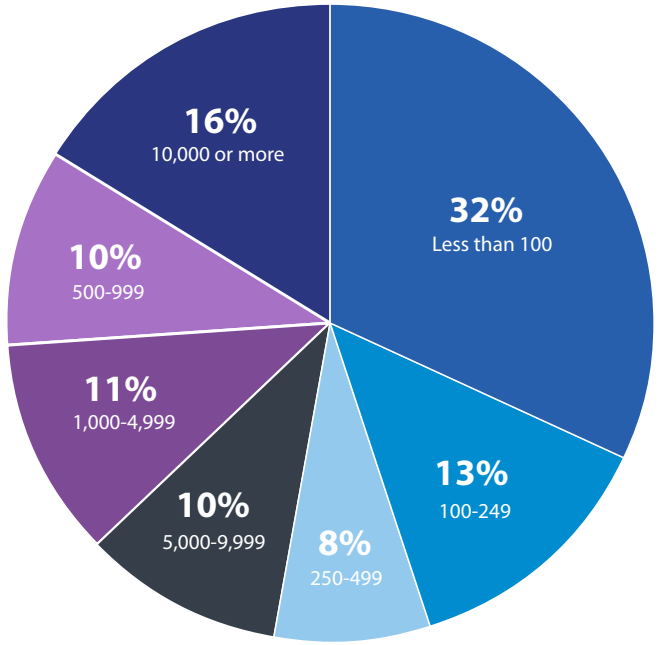


Figure 28: Size of organizations surveyed

How many employees does your organization have?

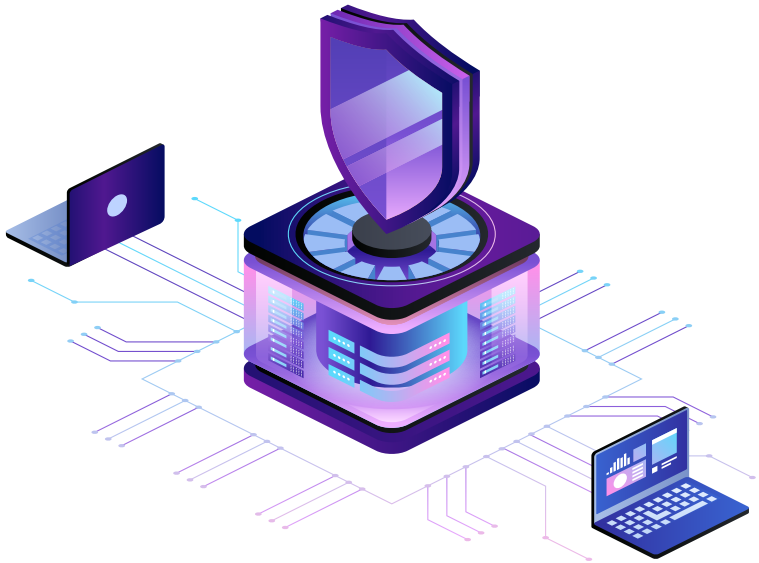


Conclusion

The goal of this survey was to provide continued visibility into how cybersecurity professionals are utilizing pen testing. The results revealed the broad range of ways organizations pen test. Third-party services and pen testing tools are widely used, and in-house teams appear to be on the rise. This is a positive indication that any organization can tailor a program to suit their needs and available resources. And with issues like compliance and remote work, penetration testing shows every sign of remaining a crucial practice for years to come.

While COVID-19 provided potential funding obstacles, continued challenges of overconfidence, lack of remediation validation, and inattention to pen testing findings prove more concerning long term. Putting your organization to the test on a regular basis is still the best way to ensure you're continuously reducing your cyber risk exposure. The goal of pen testing shouldn't simply be to check it off the to-do list.

Penetration testing not only provides short term value by finding and prioritizing the security weaknesses that currently pose the highest risk, it can also provide long term value if the findings are incorporated into your long-term security goals. For example, an excess of weak passwords may be fixed in the short term by having them changed, but should also prompt an organization to overhaul the password policy, adding tools like multi-factor authentication and reeducating employees about password crafting and storage. By allowing penetration testing to serve as a guide for your overall cybersecurity strategy, organizations will deserve to feel confident in their security posture.



coresecurity
by HelpSystems

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.

cs-gd-0621-79d