coresecurity
by HelpSystems

2020 Penetration Testing Report

Introduction

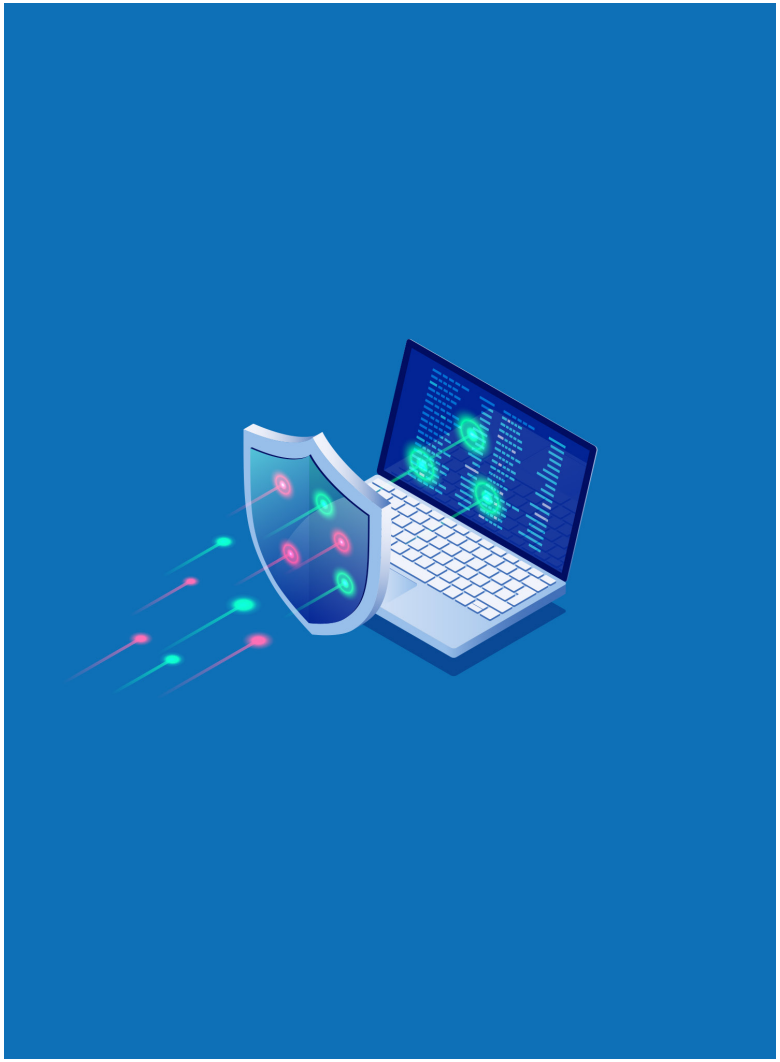
Penetration testing is a vital method to evaluate the security of an organization. By attempting to exploit potential security weaknesses of all kinds, from misconfigurations to end user mistakes, organizations can proactively take action before an attack occurs.

Having spent over two decades observing and participating in the evolution of penetration testing, Core Security, A HelpSystems Company, wanted to ascertain the role penetration testing plays across organizations of different sizes and industries. This survey aims to provide a comprehensive picture of the effectiveness of ethical hacking strategies, and the resources required to deploy a successful pen testing program.

The results of this global survey, which will be explored in detail in this report, provide valuable data on the following key issues related to pen testing:

- Why to pen test
- Remediation efforts
- Finding skilled personnel
- Executive buy in
- Choosing toolsets
- How results are reported
- Compliance concerns

This survey data establishes a strong baseline to track year over year changes, trends, and areas of improvement. With its inauguration, we have sought to create a valuable resource from which the community of cybersecurity professionals can benefit.



General Penetration Testing Challenges

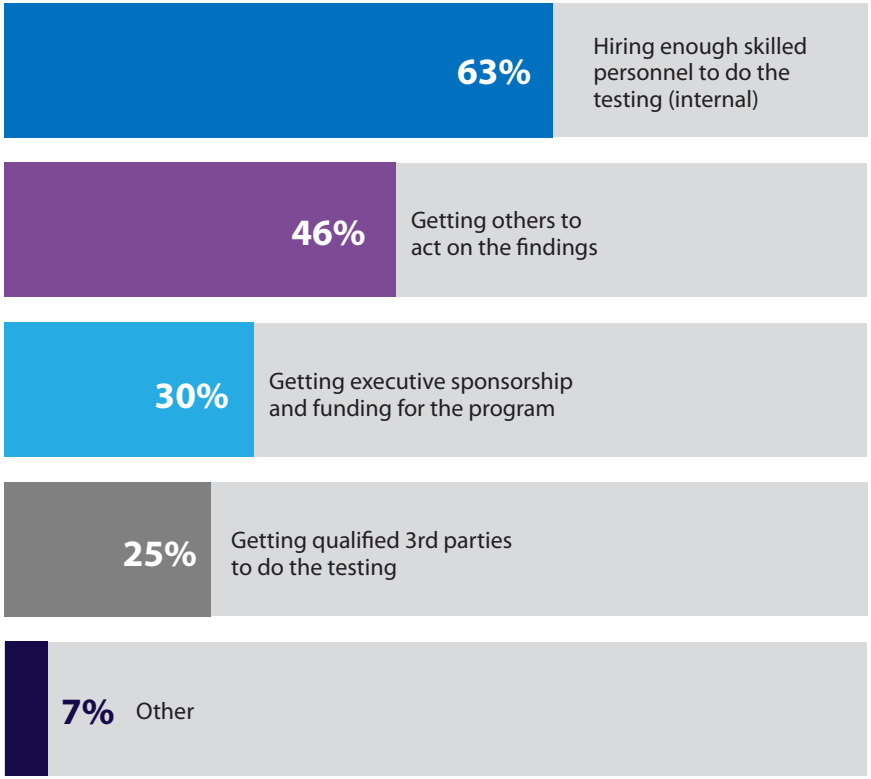
Figure 1: Pen testing challenges

One of the biggest concerns across organizations appears to be getting others to act on the findings (Figure 1). However, 97% of respondents noted that penetration testing was at least somewhat important to their security posture (Figure 2).

This implies that while pen testing programs are encouraged and supported, suggested remediations are not always implemented. This shows a mismatch between how important pen testing is seen and how much priority the results of a pen test are given. This may represent a lack of understanding of how security weaknesses correlate to business risks, such as the loss of revenue, or interruption of critical services.

Despite this, 39% of respondents reported being confident in their organization's security posture (Figure 3), which is an indicator of overconfidence and a common issue in the in the cybersecurity world. How can you be confident in your security posture if you do not effectively test it?

What challenges does your organization face with your penetration testing program?



General Penetration Testing Challenges

Figure 2: Importance of penetration testing

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

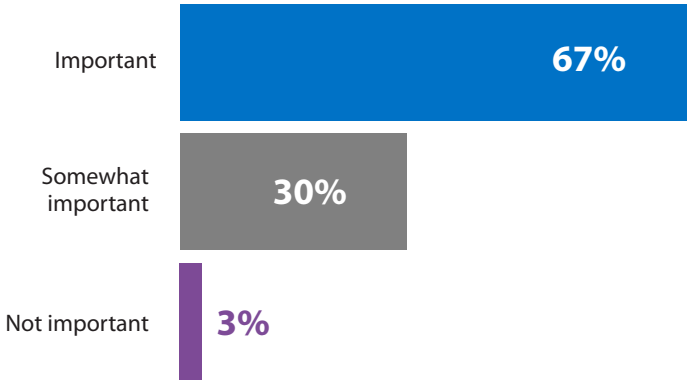
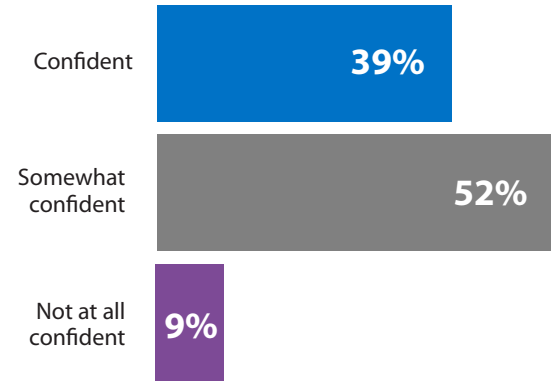


Figure 3: Confidence in security posture

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



Reasons for Penetration Testing

Reasons for Pen Testing

Organizations appear to have an even balance for why they pen test, with 70% reporting that they perform pen tests for vulnerability management program support, 69% for measuring security posture, and 67% for compliance (Figure 4).

Common Security Concerns

Respondents also reported misconfiguration (77%), phishing (72%), and poor passwords (60%) as top concerns (Figure 5). This may indicate that pen testing is a desirable way to test for risks related to user error. These common entry points are typically best solved through a combination of retraining efforts and security tools.

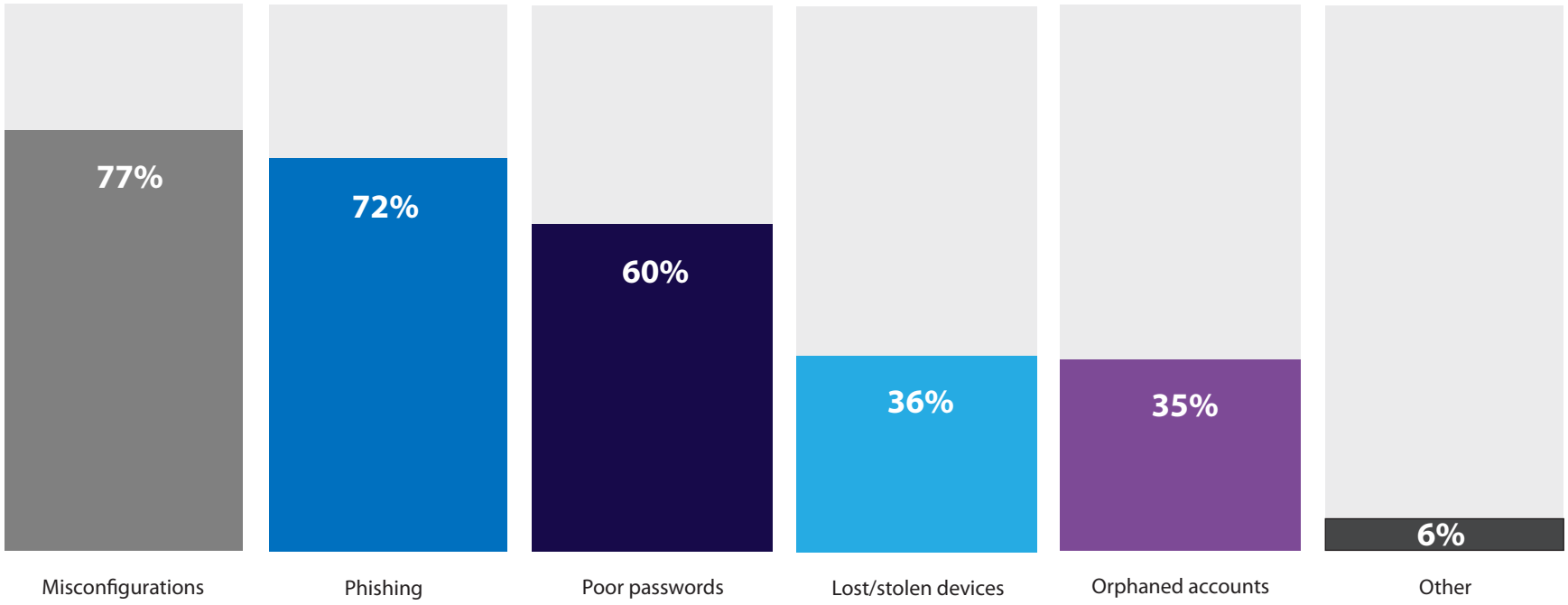
Misconfiguration issues can be alleviated with routine training for the IT teams that are responsible for these systems. Additionally, automation tools can handle routine administration tasks to maintain consistent policies. Problems like phishing and poor passwords can occur throughout the organization, and will need consistent reeducation sessions, particularly for those who fail phishing simulations. Password tools can enforce strong password policies to reduce risk. Ultimately, maintaining your security posture over time requires regular penetration testing and retesting to see if these efforts are effective.

Figure 4: Reasons for performing penetration testing

Reasons for Penetration Testing

What common security risks/entry points are you most concerned about?

Figure 5: Common security concerns



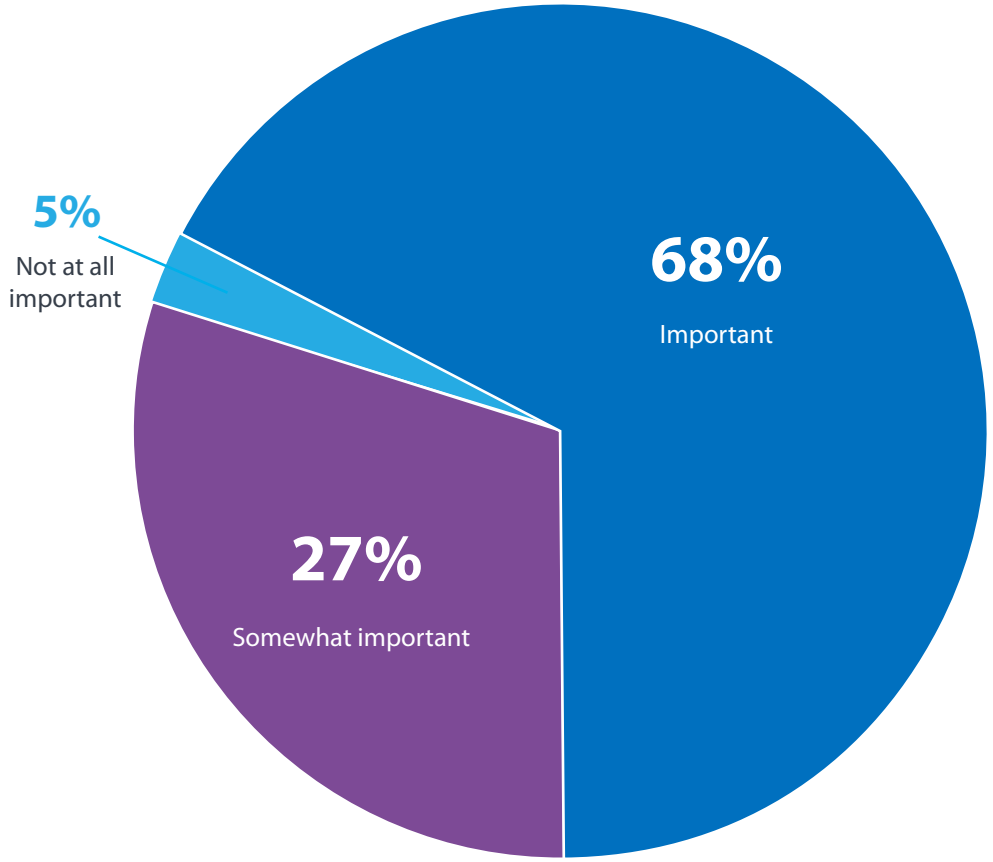
Compliance and Pen Testing

The need to stay compliant or adhere to external mandates was a primary reason respondents pen testing (68%), as seen in Figure 4. 95% of respondents reported that pen testing held some level of importance for their compliance initiatives.

Much of the most important data (Figure 7) for respondents to protect—customer, patient, financial, or employee—fall under some sort of regulation or industry best practice. NIST, SOX, NERC, HIPAA, CMMC, and GDPR will most likely be followed by additional mandates that emphasize the importance of protecting sensitive data, ensuring that pen testing will continue to be a critical tool for organizations needing to demonstrate the effectiveness of their security programs.

Figure 6: Importance of penetration testing for compliance

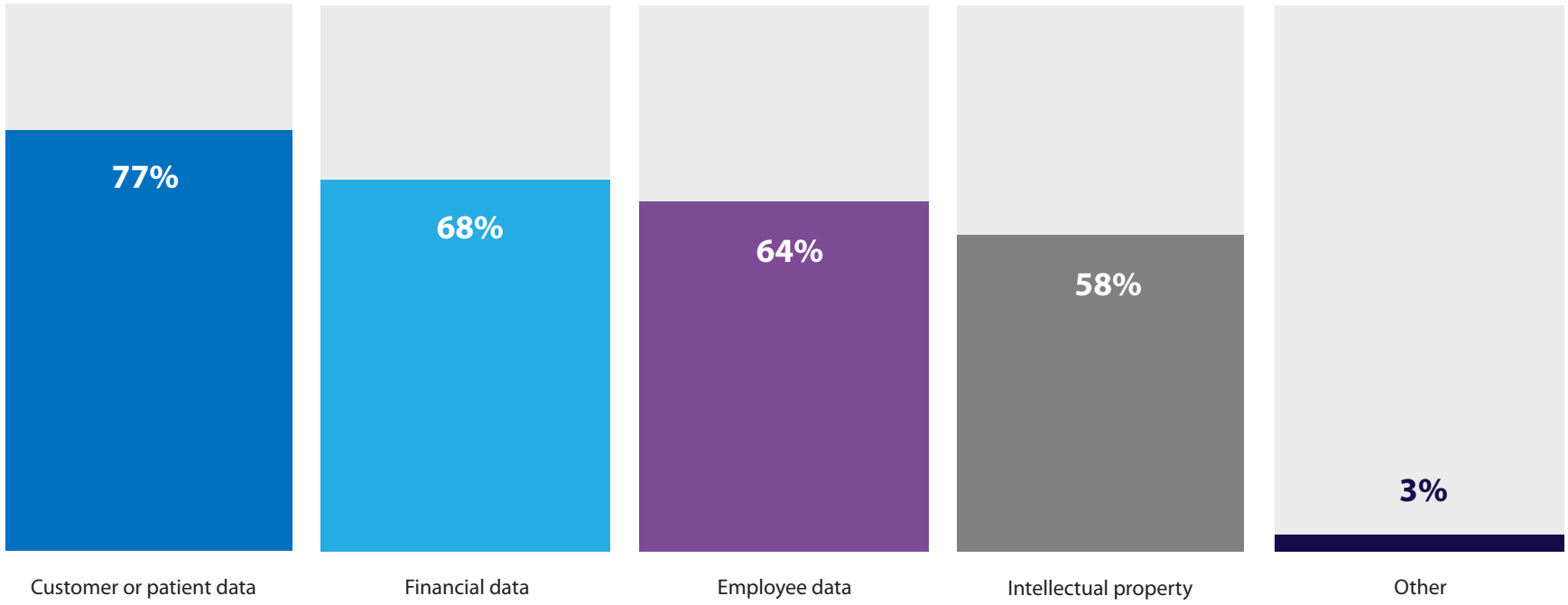
How important is penetration testing to your compliance initiatives?



Compliance and Pen Testing

What type of data is most important for your organization to protect?

Figure 7: Most important types of data to protect



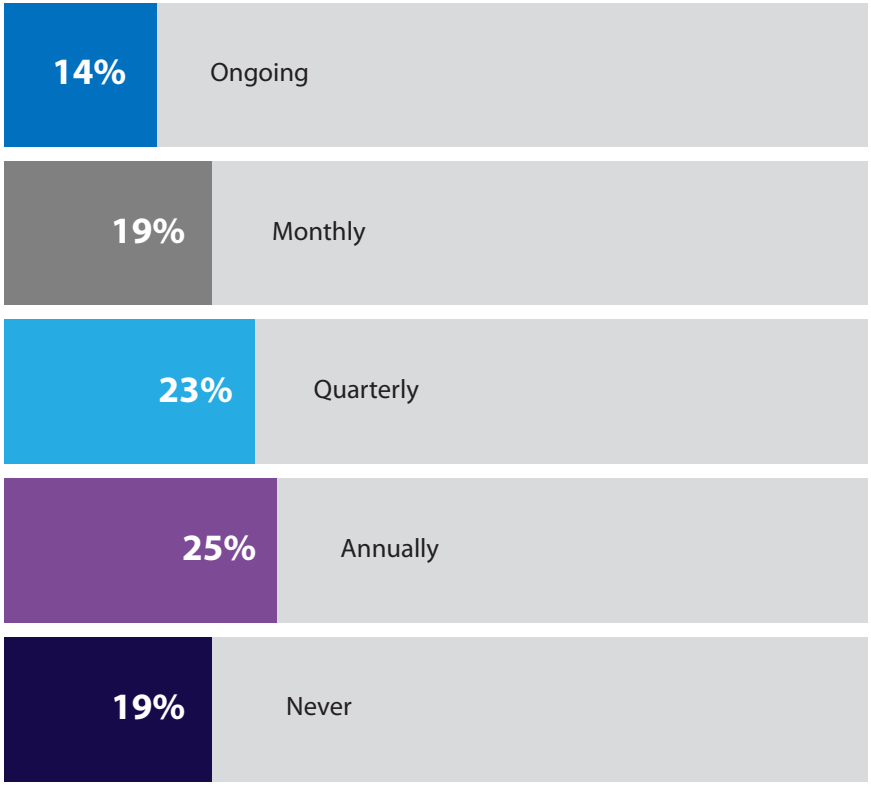
Phishing

Phishing attempts are nearly impossible to block from every inbox and are an incredibly common way for attackers to gain access to employee credentials and an organization's systems. 72% of respondents noted that phishing was a top security concern, indicating that organizations are very aware of the risk that this attack strategy poses (Figure 5).

Phishing simulations can be run to see what type of ploys are tricking employees, and who is susceptible to them. These social engineering pen tests are a valuable tool for education and awareness, which are the primary prevention methods for this type of attack. However, 19% responded that they never conduct phishing simulations, and 25% only conduct them annually, which may indicate a lack of awareness of how helpful frequent phishing simulations are, or a lack of resources (Figure 8).

Figure 8: Frequency of phishing simulations

How often does your organization conduct phishing simulations?



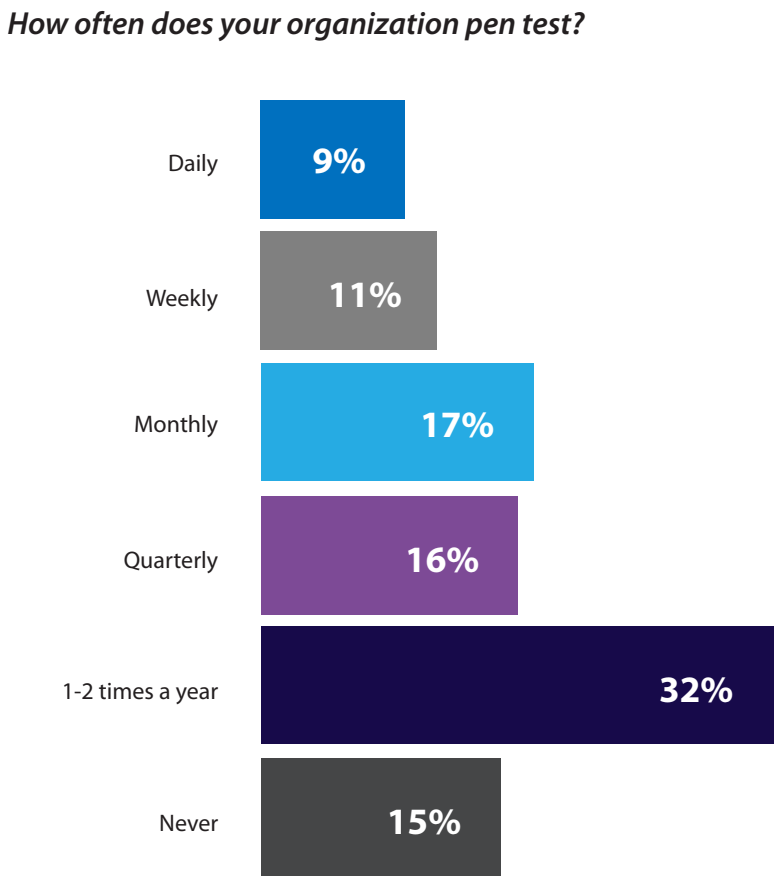
Penetration Testing Frequency

It is promising to see that only a small percentage of respondents (15%) indicated that they never pen test. This indicates that pen testing is viewed as a critical practice that makes an impact in an organization's security posture. Ideally, as long as it done by the right people and with the right tools, pen tests should be run as frequently as possible, particularly when significant changes or updates are made to the infrastructure (Figure 9).

The largest percentage of respondents (32%) test one to two times a year. While this may help sort priorities about security weaknesses, it does indicate a lack of re-testing, which is an important way to validate remediation efforts. Those with internal pen testing teams did report testing more frequently, with 47% reporting monthly or quarterly testing, versus 33% of everyone surveyed. This indicates that testing frequency is most likely heavily influenced by budget and resources.

20% of respondents reported pen testing daily or weekly. Pen testing is typically quite a large undertaking, so there may be a misunderstanding about the difference between a vulnerability scan, which can be run daily or weekly, and a full pen test.

Figure 9: Frequency of penetration testing



In-House Penetration Testing Efforts

While some businesses exclusively enlist the services of a third-party penetration testing team, it is now quite common to build an in-house team, with 42% of respondents working at organizations that have one in place (Figure 10).

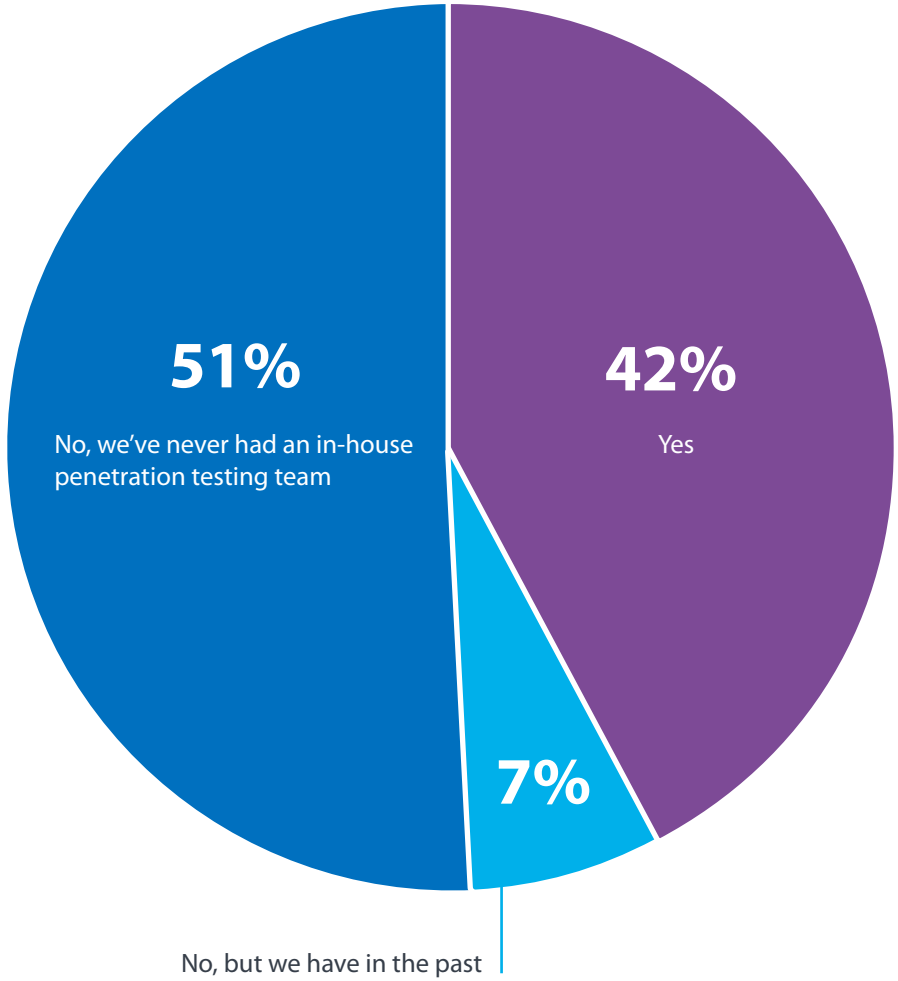
Teams remain relatively small, with 84% of respondents reporting teams of five dedicated team members or fewer (Figure 11). It is also possible that these teams are assisted by personnel that have pen testing tasks as part of their duties, but aren't considered full time team members. Additionally, other organizations may still perform pen testing activities, but don't have teams solely for this purpose.

Once in place, these teams seem to prove themselves valuable. Only 7% responded that their in-house team is now defunct, perhaps showing that once in place, organizations prefer to keep them intact. In fact, 46% of respondents that have in-house teams noted that they were confident in their security posture versus the only 29% of those that did not have an internal team (Figure 12).

It is also worth noting that 61% of those that reported they did not have an internal team were in an organization with fewer than 500 employees, and represented 70% of those reporting that they didn't have enough need. Smaller organizations may not be able to justify the resources required to have an in-house team. Their needs may be adequately met by third party services, since their IT infrastructures aren't as large, so testing is not such a time consuming effort (Figure 13).

Figure 10: In-house penetration testing

Do you have an in-house penetration testing team?



In-House Penetration Testing Efforts

Figure 11: In-house pen testing team size

How many dedicated team members does your in-house penetration testing team have?

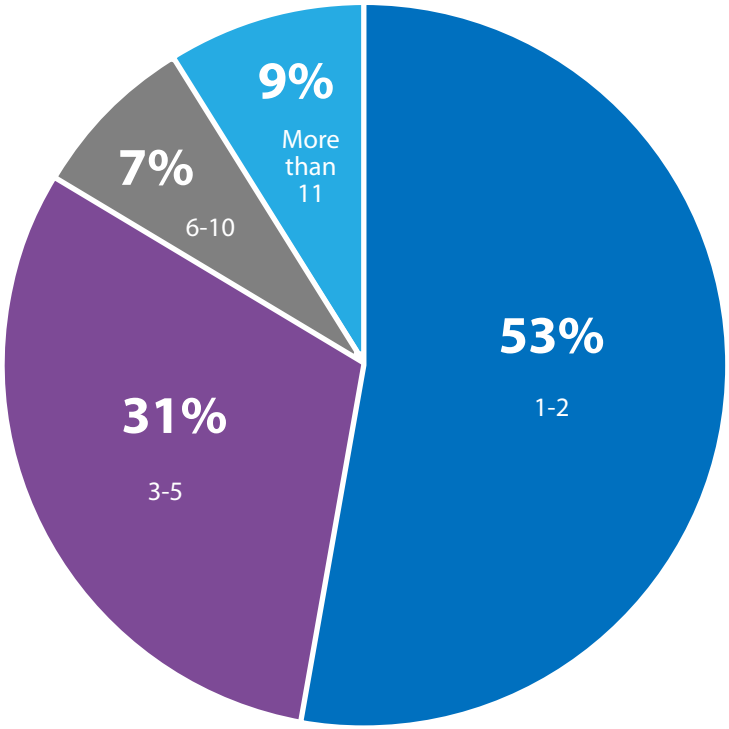
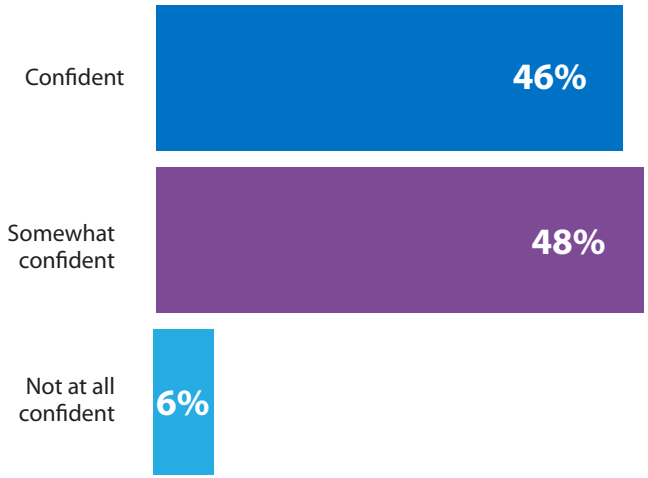


Figure 12: Confidence in security posture

(respondents with internal teams only)

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

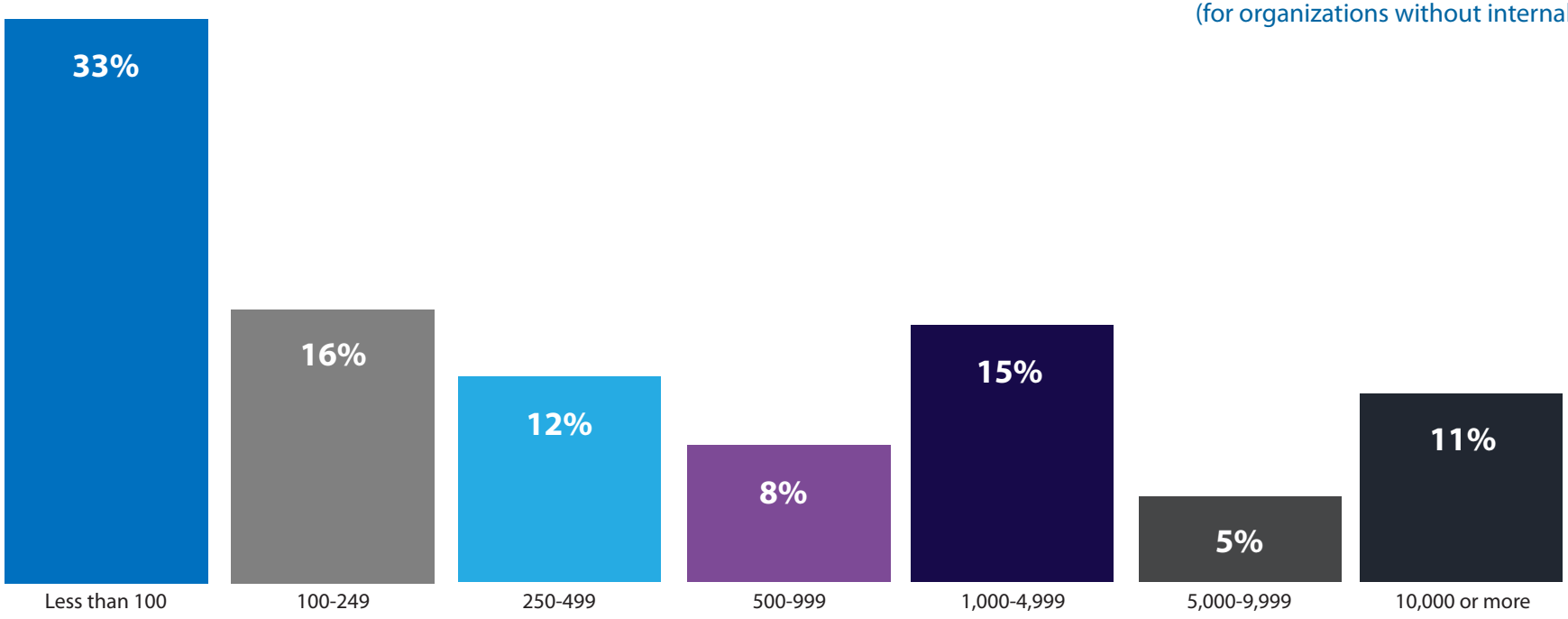


In-House Penetration Testing Efforts

How many employees does your organization have?

Figure 13: Number of employees

(for organizations without internal teams)



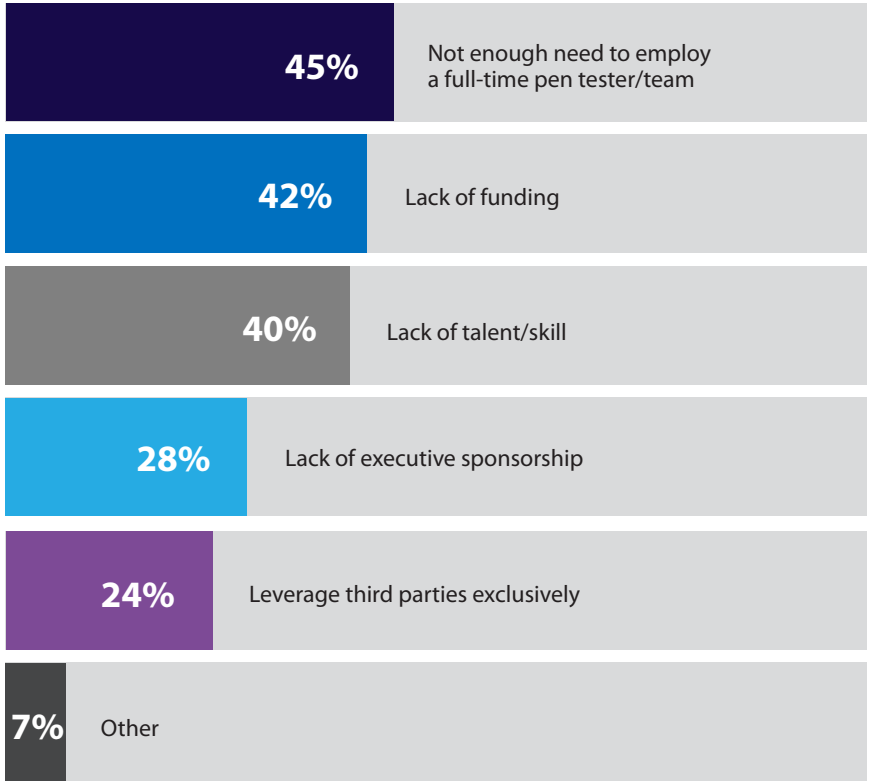
In-House Penetration Testing Staffing Challenges

There are many reasons cited for not having an in-house penetration testing team. 40% cited lack of talent and 42% cited lack of funding, which aligns with the ongoing skills shortage in the cybersecurity field (Figure 14). There are not enough experienced pen testers to go around, and those that are can be very expensive. This is further reflected by the fact that 49% of respondents reported that their staff has three years or fewer of experience with pen testing (Figure 15).

60% indicated that technology plays an influence in whether or not they have an in-house team, demonstrating the vital the role pen testing tools can play for in-house pen testing teams (Figure 16). Some tools can help combat the talent obstacle, as they function not only as a way to streamline and enhance pen testing efforts, but also as a way to standardize testing and enable comparing results.

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

Why doesn't your organization have an in-house penetration testing team?



In-House Penetration Testing Staffing Challenges

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

What is the average number of years of experience your in-house team has with penetration testing?

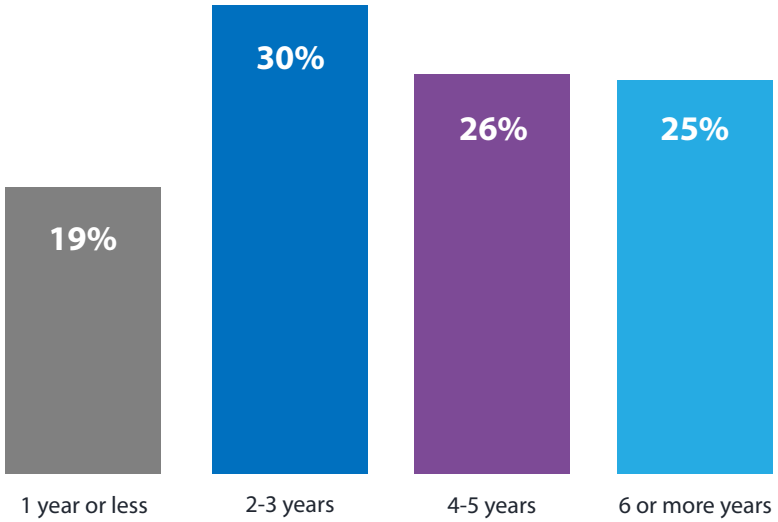
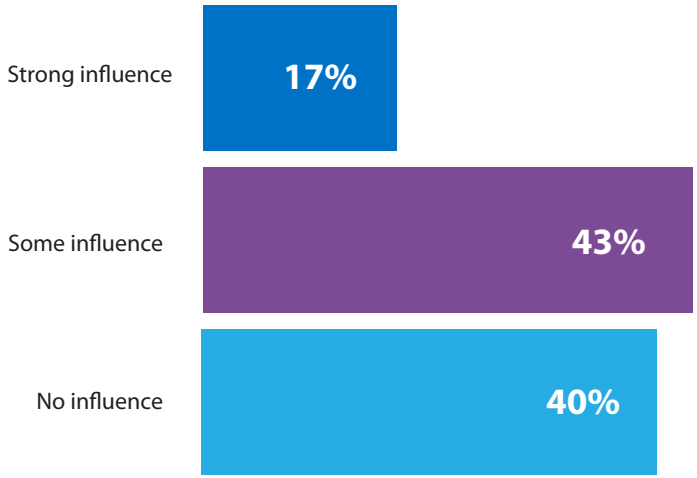


Figure 16: Influence of pen testing technology

How does penetration testing technology influence your organization's decision to have an in-house penetration testing function?



Purple Teams

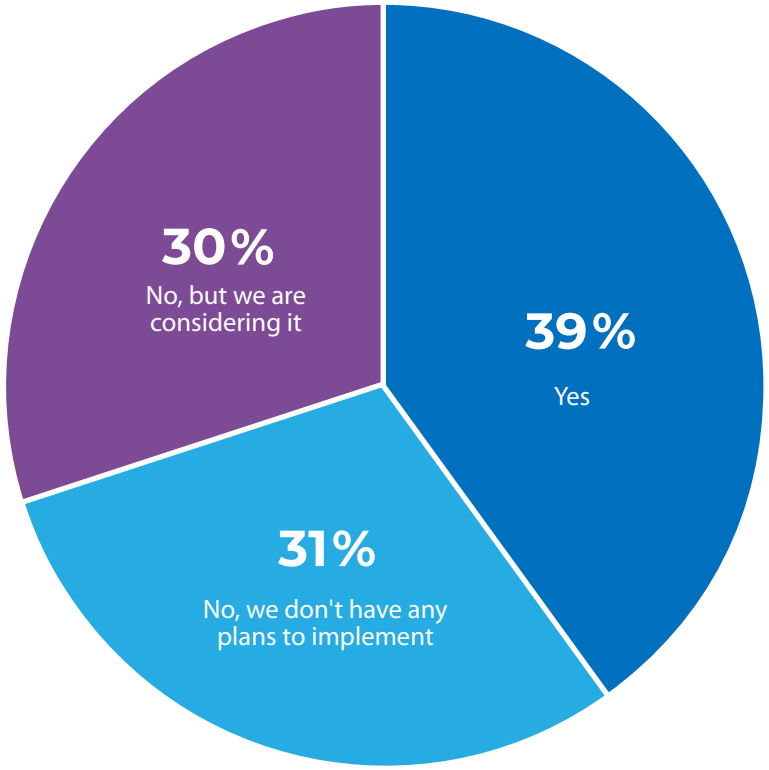
Purple teaming, which focuses on aligning the efforts of both red and blue teams, creates a communicative joint team that shares the goal of improving security. 39% of respondents reported that they have already implemented the approach (Figure 17).

Considering the amount of resources—time, money, and personnel—needed to institute this approach, this number is surprisingly high. Respondents may only be using purple teams for small engagements.

These responses imply that the idea of purple teaming is becoming more widely accepted as best practice, and that it is not a disagreement on strategy, but rather the amount of effort needed to implement a comprehensive purple team exercise that is the main inhibiting factor. This move towards purple teams, even for small engagements, is positive, since purple teams are more collaborative and make testing efforts even more effective with unified, cohesive plans, goals, and strategies.

Figure 17: Utilization of a purple team approach

Do you utilize a purple team approach (red and blue teams working together) in your pen-testing strategy?



Penetration Testing Tools

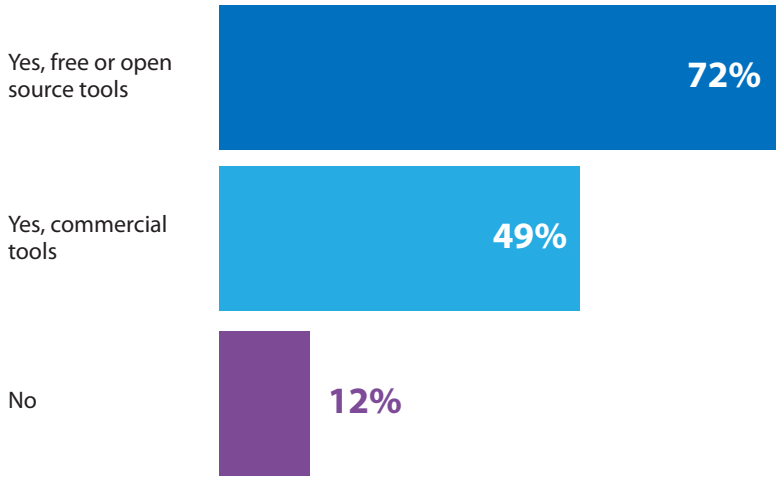
Nearly all respondents indicated that they use penetration testing tools of some kind, and 72% of respondents noted that they used free and/or open source tools (Figure 18). This falls in line with the common practice of multiple tools that meet different needs. For example, commercial testing tools, used by nearly 50% of respondents, can provide commercial-grade exploits that open source tools may not be able to offer. Using a combination of both open source and commercial tools aligns with the 62% of respondents that indicated cost as an important consideration (Figure 19).

Using a variety of tools also appears to be a practical solution given how important features were noted to be when evaluating a tool (83%), and the wide range of features respondents consider important when looking for in a pen testing tool (Figure 19).

Among the most desired features were templates/automation capabilities, an extensive threat library, and multi-vector testing capabilities. Reporting was the most popular, with 69% of respondents listing it as an important feature (Figure 20). This may be due to compliance needs, which often require extensive documentation to prove adherence to certain regulations and industry practices. Reporting is also an arduous, time-consuming task, so good reporting functionality can streamline things considerably.

Figure 18: Active use of penetration testing software

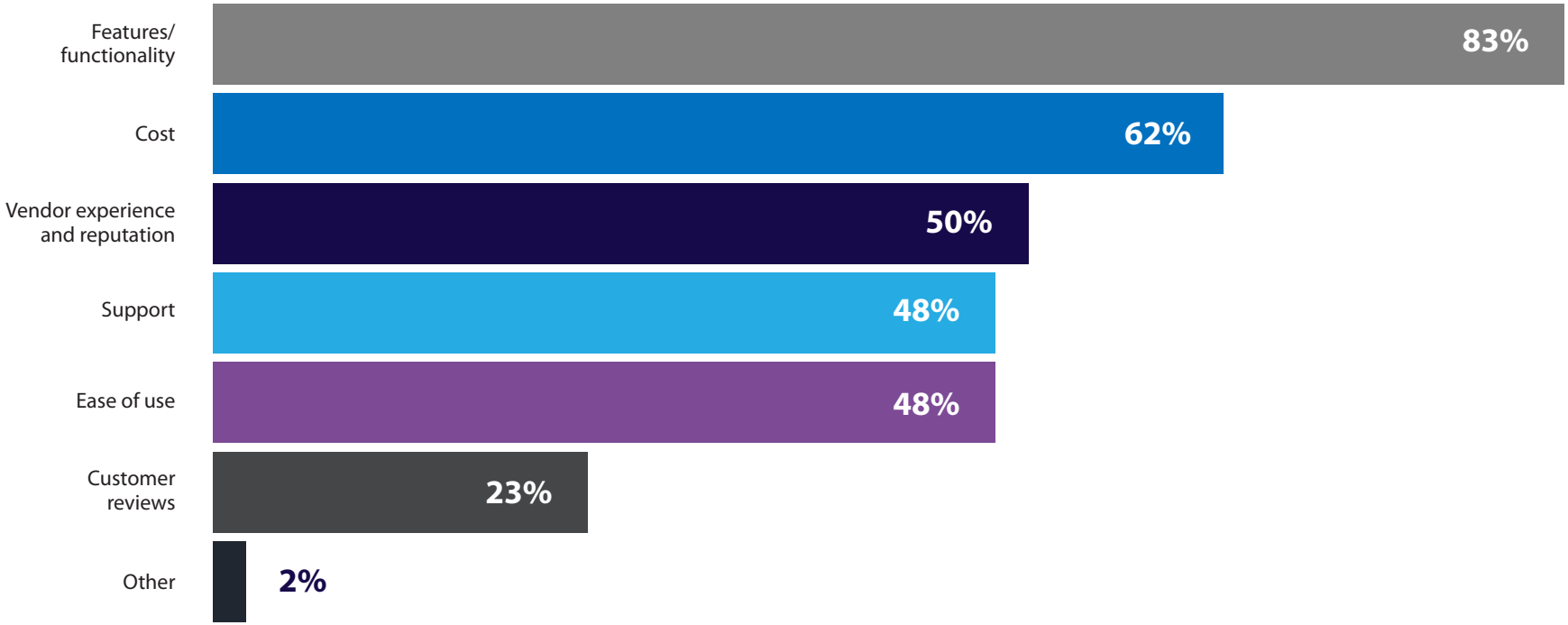
Does your organization actively use penetration testing software or tools?



Penetration Testing Tools

Figure 19: Most important criteria for evaluating pen testing software

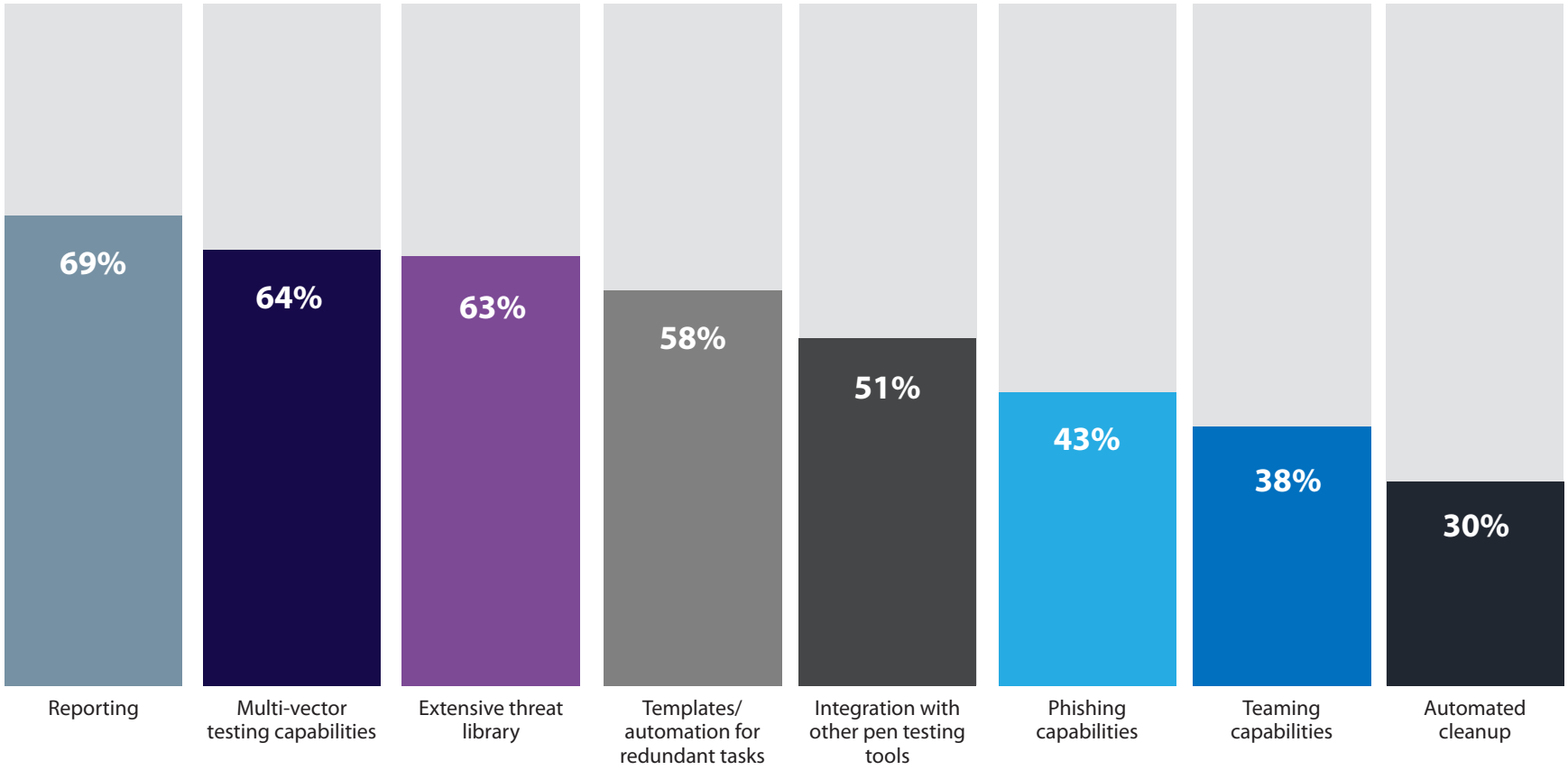
What criteria do you consider most important when evaluating penetration testing software?



Penetration Testing Tools

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

Figure 20: Most important features in pen testing software

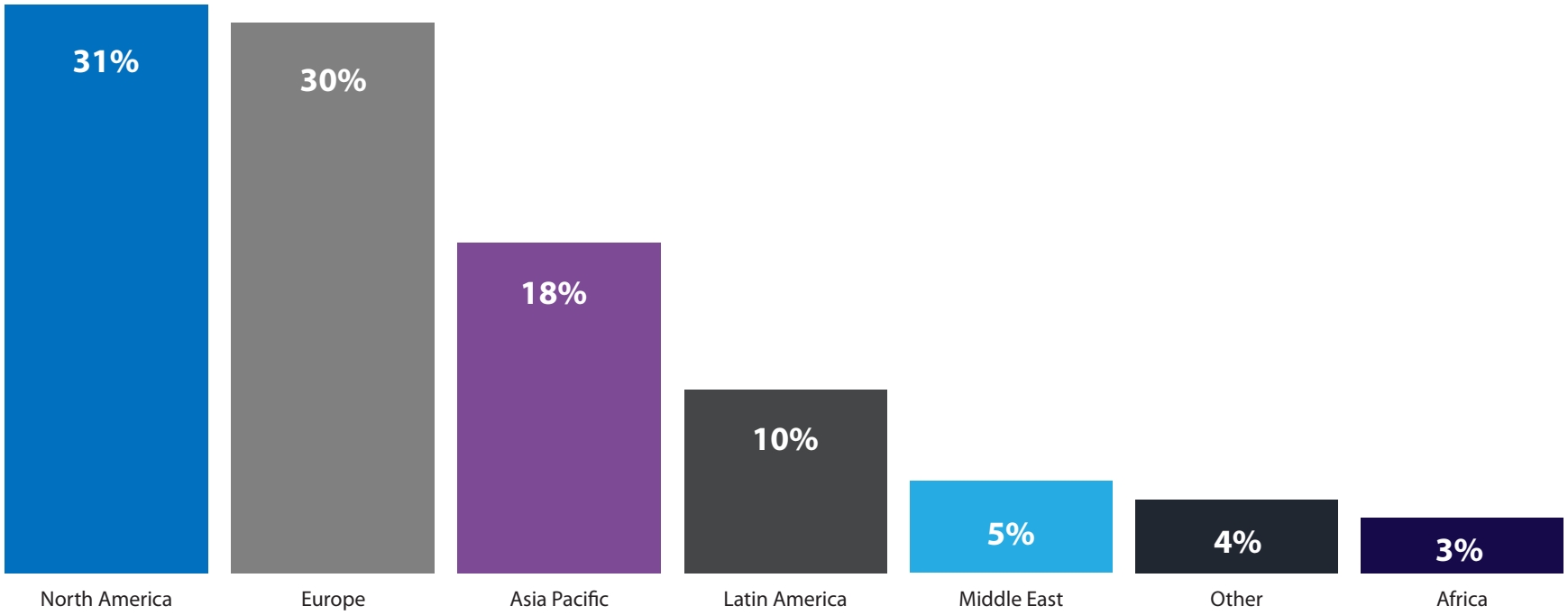


Demographics

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.

Figure 21: Regions

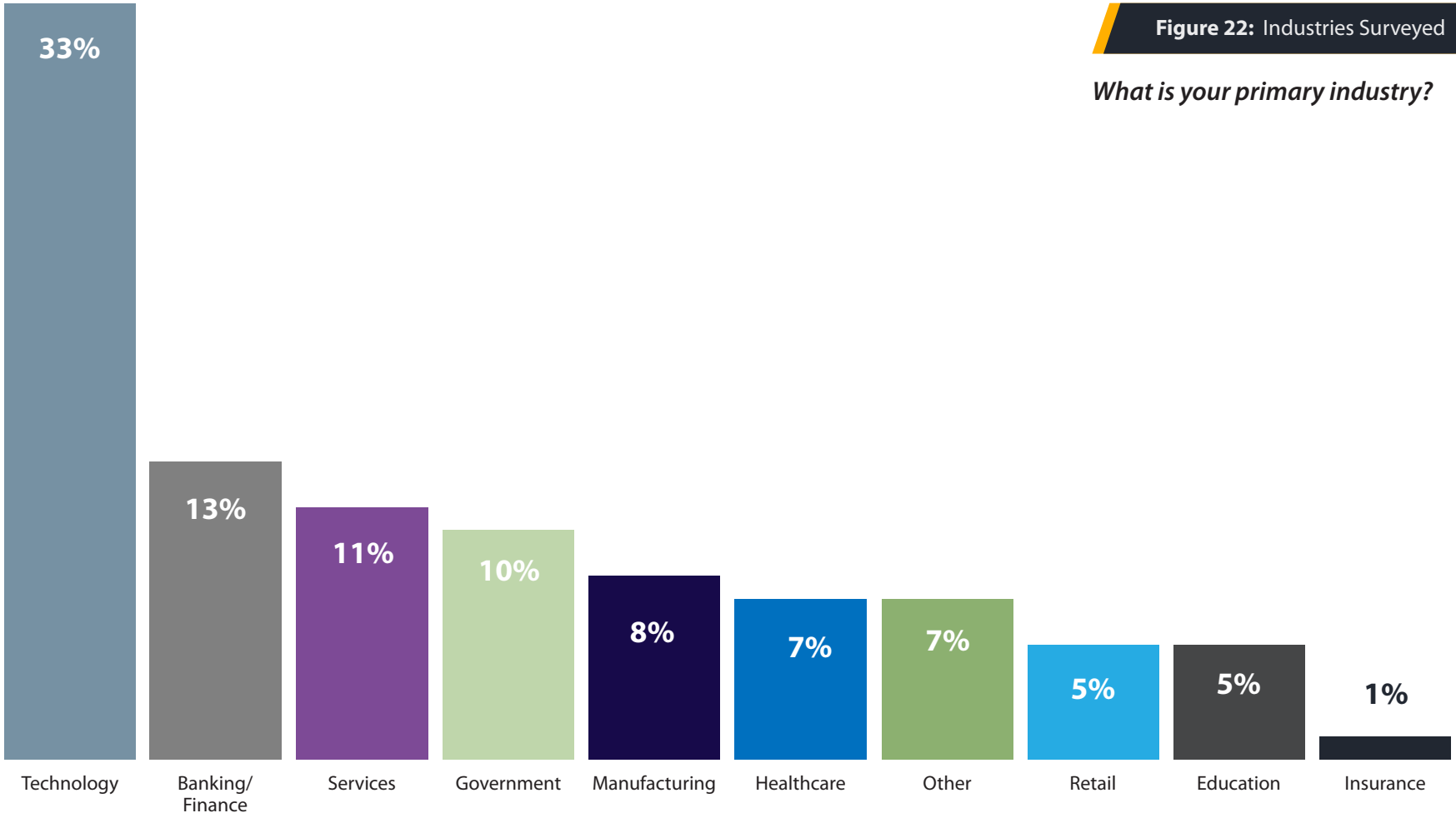
In which region is your organization headquartered?



Demographics

Figure 22: Industries Surveyed

What is your primary industry?



Demographics

Figure 23: Job levels surveyed

What is your job level?

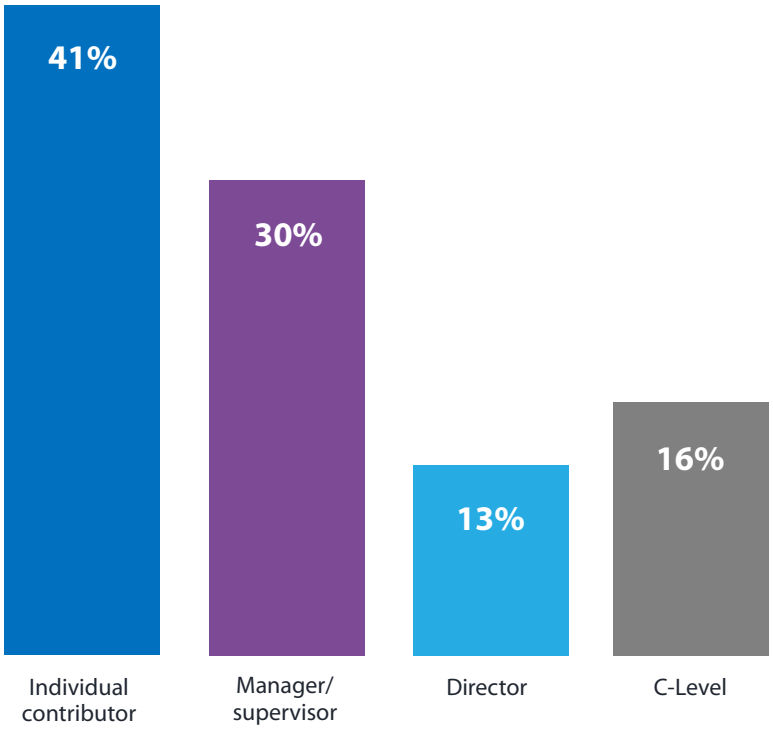
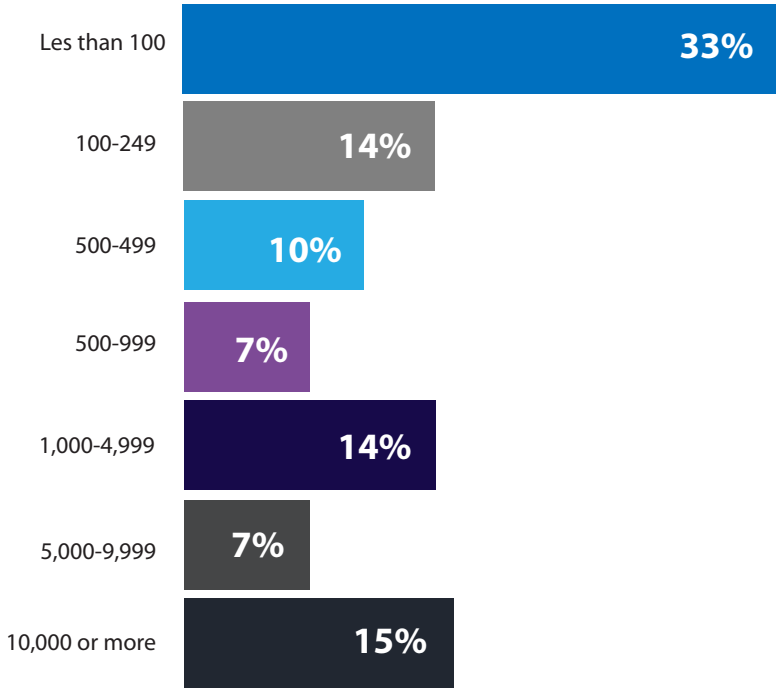


Figure 24: Size of organizations surveyed

How many employees does your organization have?



Conclusion

Without penetration testing, how do you know if you're at risk? As scary as it can be to find out that you have dangerous security weaknesses, the only way to eliminate them is to know they are there in the first place. Penetration testing remains the best way to keep ahead of adversaries by allowing you to uncover vulnerabilities before they can.

The goal of this survey was to provide visibility into how cybersecurity professionals are utilizing pen testing. The results revealed the wide range of ways that people pen test, indicating that any organization can tailor a program to suit their needs and available resources. Third party services are a great option for smaller organizations who may not yet be able to have someone internal dedicated full time, but they are also ideal for larger organizations with in-house teams who need external validation or simply a second pair of eyes. In-house teams can take many different shapes—small, large, experienced, novice. Tools are also versatile, and organizations typically use more than one to get all the features they want and need. There are any number of combinations of tools that can be paired together to create a unique suite that ensures a team can imitate any type of attacker.

Though pen testing programs are not without their challenges, the amount of options available enable security teams to tweak and adjust things as needed to get the most out of their efforts. Having such flexibility in how an organization can put together a pen testing program will allow the practice of pen testing to continue to thrive as long as threat actors continue to attack.

www.coresecurity.com

coresecurity
by HelpSystems

About Core Security

Core Security provides organizations with critical, actionable insight about who, how, and what is vulnerable in their IT environment. With our layered security approach and robust threat-aware, identity & access, network security, and vulnerability management solutions, security teams can efficiently manage security risks across the enterprise.

© HelpSystems, LLC. All trademarks and registered trademarks are the property of their respective owners.

cs-gd-0621-79d