APRIL 2021

The Failed Practice of Penetration Testing

A SECURITY REPORT FROM CYCOGNITO

CYCOGNITO

Executive Summary

New research commissioned by CyCognito and conducted by Informa Tech shows that while organizations invest significantly in penetration testing, such testing doesn't accurately measure their security posture or breach readiness — the top two stated goals among security and IT professionals. Pen testing limitations mean organizations do not actually test the majority of their attack surface and fail to address huge blind spots that are potentially vulnerable to attack and compromise. The research, from a study surveying enterprises with 3,000 or more employees, found that cost concerns and the challenges associated with the depth, scope, and frequency of penetration tests have hampered the ability of organizations to measure their security posture and prevent breaches. The majority of organizations do penetration tests on 50% or less of their attack surface. Just as locking the front door of a house but leaving the back door and windows unlocked creates an attractive target, attackers will naturally focus on those IT assets organizations leave untested.

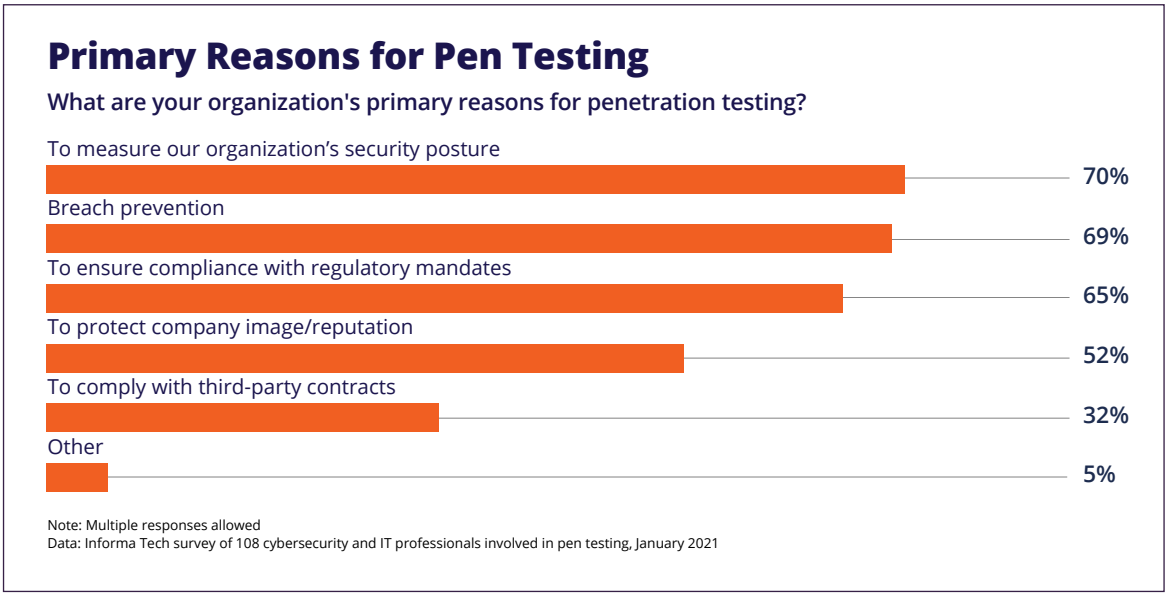
Top 5 Findings:

- **False Assessment of Security Posture and Breach Readiness:** Respondents indicate they depend on penetration tests to fully assess the security of their organizations. The top two drivers behind penetration testing are measuring security posture (70%) and preventing breaches (69%). But those objectives are undermined by the factors noted in the remaining Top 5 Findings.
- **Insufficient Attack Surface Coverage:** Pen tests leave blind spots unaddressed. The top two concerns with penetration testing are: (1) it only provides limited coverage of the attack surface and leaves blind spots (60%), (2) it detects only known assets and not new or unknown ones (47%).
- **Insufficient Cadence:** The majority of organizations don't conduct anywhere near the continuous monitoring that best practices dictate, and some regulations require. Forty-five percent conduct penetration tests just once or twice annually, and 27% do it once a quarter.
- **Testing Takes too Long:** It takes 71% of respondents anywhere from one week to one month to conduct a penetration test. Then, more than 26% have to wait between one to two weeks to get test results, and 13% wait even longer than that.
- **Too Expensive to Use as Needed:** Penetration tests are prohibitively expensive. Seventy-six percent of respondents report penetration testing cost hampers their ability to test more frequently.

I. Penetration Tests Are a Failure as a Security Practice

Organizations are primarily conducting penetration tests to measure their security posture (70%) and to prevent breaches (69%) **(Figure 1)**. However, if penetration tests are not scoped properly and do not cover the entire attack surface, they can contribute to a sense of misplaced confidence in an organization's overall security status.

Figure 1



Interestingly, regulatory compliance, a rationale for many enterprise security initiatives, is only the third-highest stated objective for organizations' penetration testing. Sixty-five percent conduct penetration tests to comply with regulations that require periodic assessments of their security posture. Other primary reasons for conducting penetration tests include a desire to protect the organization's image or brand (52%) and to comply with third-party contracts (32%) — an issue that is likely going to gain importance given the recent increase in attacks targeting third-party software and technology providers.

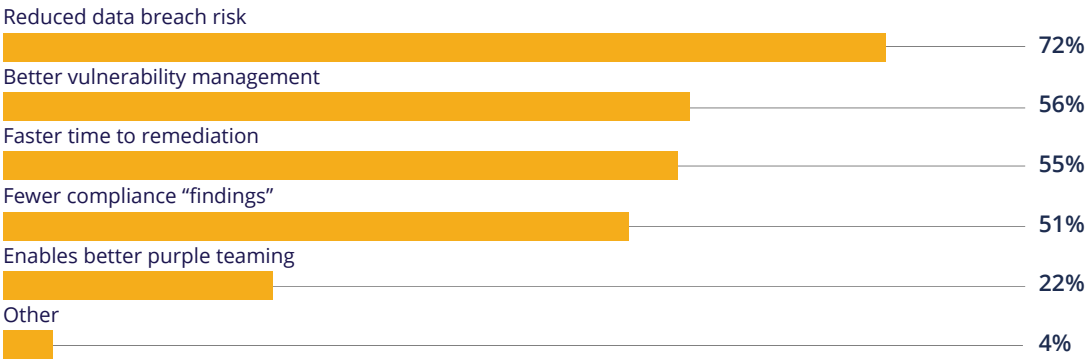
In addition, seventy-two percent of the respondents in the survey say they consider reduced breach risks as the most important metric for measuring ROI on penetration tests, and 56% point to improved vulnerability management **(Figure 2)**. Other popular metrics for measuring ROI include faster time to remediation and fewer compliance issues.

This reliance on pen tests for security begs the question: Are the tests really making organizations any safer, or are they only contributing to a sense of false confidence?

Figure 2

Measuring ROI

How do you measure ROI on your penetration testing investment?



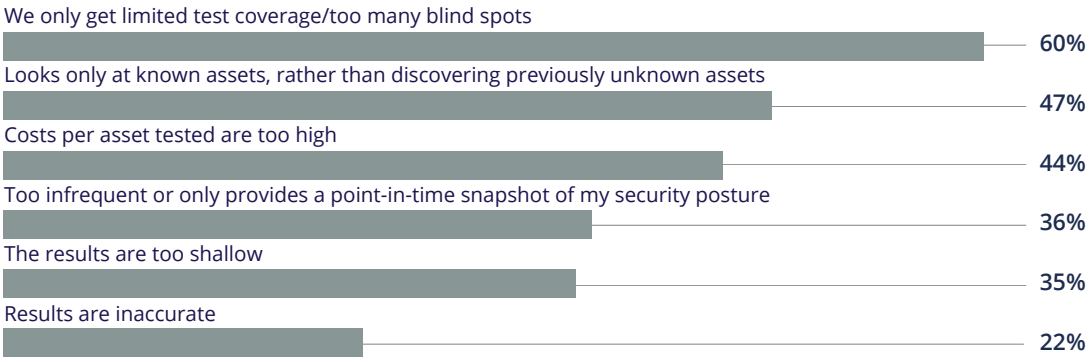
Note: Multiple responses allowed
Data: Informa Tech survey of 108 cybersecurity and IT professionals involved in pen testing, January 2021

Survey data shows that IT and security professionals are concerned about a variety of issues pertaining to their organization's penetration-testing processes. Sixty percent, for instance, are worried that current penetration tests cover only a portion of their attack surface and have left them with too many blind spots (**Figure 3**). Nearly half (47%) are concerned that their penetration tests look at only known assets and don't discover new or unknown ones, and 44% say the cost per asset tested is too high. More than one-third (36%) believe they are, at best, getting a point-in-time assessment of their security status because penetration tests are too infrequent. Snapshot security assessments, while sometimes sufficient for meeting compliance requirements, do not provide insight on an environment's current security status or exposure to new threats.

Figure 3

Pen Testing Concerns

What are your biggest concerns with your current penetration testing?



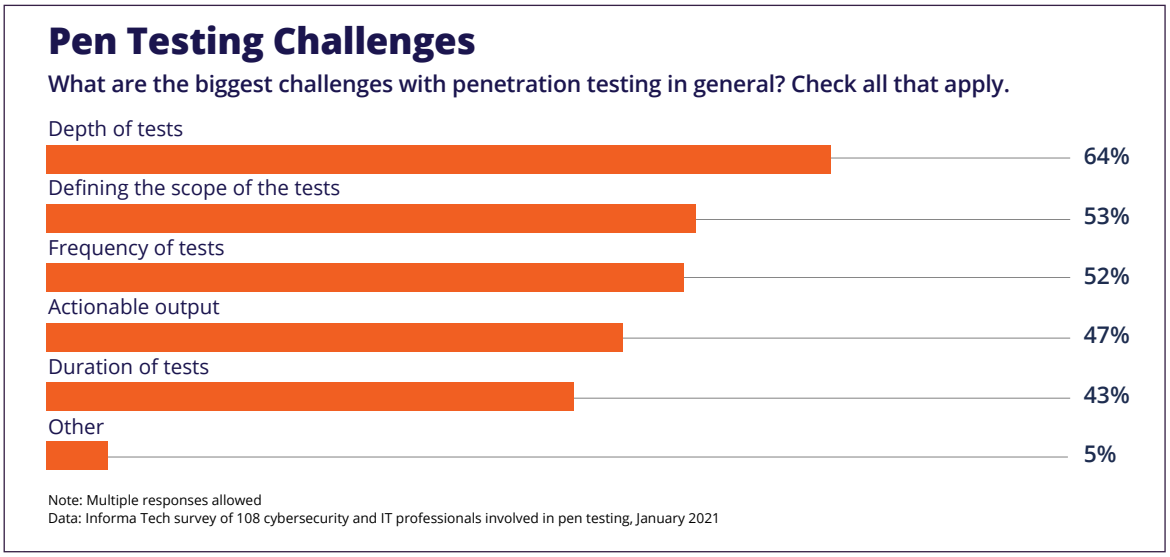
Note: Multiple responses allowed
Data: Informa Tech survey of 108 cybersecurity and IT professionals involved in pen testing, January 2021

The causes for the respondents' concerns about penetration tests are not hard to find. Our survey shows that huge gaps continue to exist in the frequency, scope, and depth with which they are conducted. In addition, the costs associated with the exercise are holding back many enterprises from conducting security assessments that are broader in scope and more frequent in nature.

Ia. Limited Coverage

Let's consider challenges with scope and depth. Sixty-four percent say the biggest challenge with penetration tests is making them inclusive — or deep — enough to cover all assets at risk **(Figure 4)**.

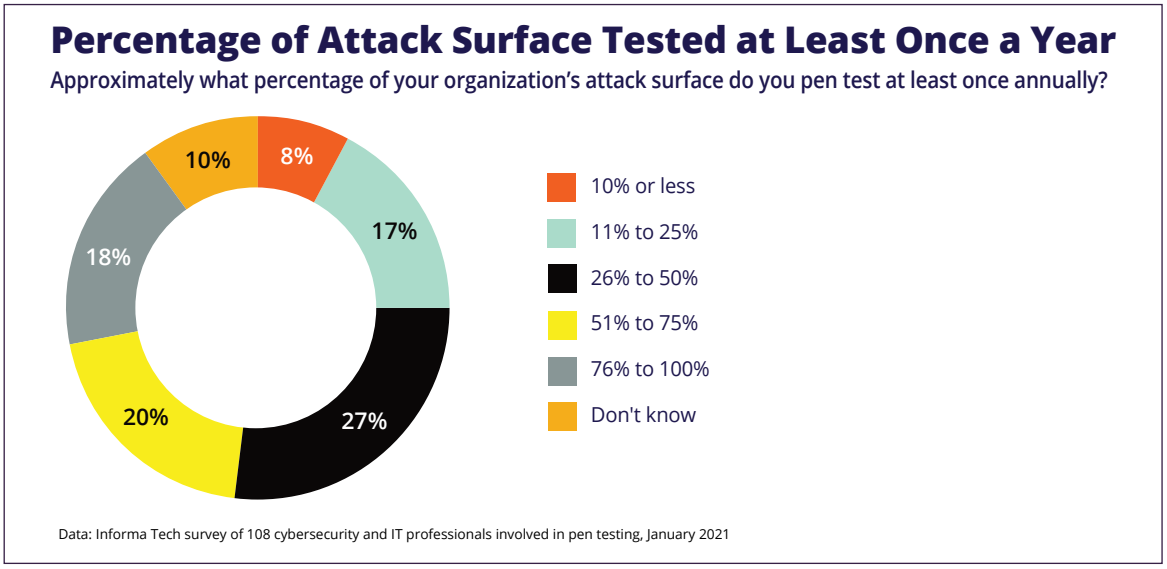
Figure 4



More than seven in ten organizations (72%) currently conduct penetration tests on just 75% or less of their organization's entire attack surface — leaving them essentially blind to exposures on the remaining 25% **(Figure 5)**. For many organizations, the exposure is much greater. When we break the 72% down, it shows 44% of organizations test between 10% and 50% of their attack surface and 8% test a mere 10% or less. This means more than half of organizations test 50% or less of their attack surface. For these organizations, it would appear that their investments in penetration testing are being largely undermined by their continuing vulnerability to — and lack of visibility over — threats on large, untested portions of their attack surface. Eighty-three percent say they test 10,000 assets or fewer and of that, 58% report covering less than 1,000 Internet-connected assets per penetration test — a troubling finding given that survey respondents come from large organizations with 3,000 or more employees, and those organizations undoubtedly have tens or hundreds of thousands of Internet-exposed assets.

A plurality of organizations (48%) is doing penetration testing on their web apps, IT infrastructure, and third-party/supply-chain ecosystem. However, the extent and scope of this testing is far from comprehensive. More than one-third (37%) are primarily or only assessing the security posture of their IT infrastructure, and 10% describe their organizations as conducting penetration tests on their web applications alone. Only 4% say they primarily use penetration tests to assess the security of third parties, indicating that organizations generally don't view penetration testing as a viable means to assess potential exposure to third-party risk.

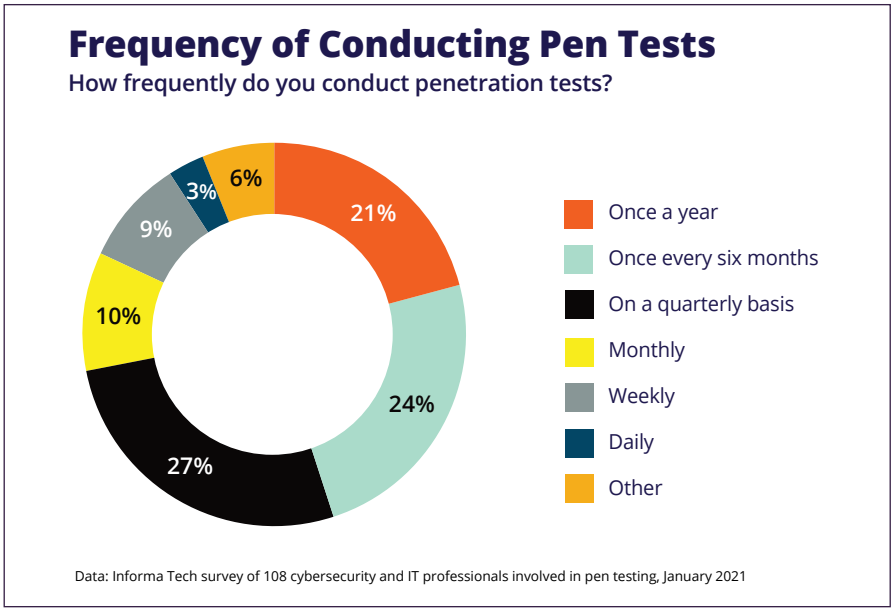
Figure 5



Ib. Infrequent

Frequency of testing is another major issue, with 52% identifying it as one of their biggest challenges. Our data shows a majority of organizations are conducting nowhere near the continuous monitoring that best practices dictate — and which some regulations require. Forty-five percent conduct penetration tests just once or twice annually, and 27% do it once a quarter **(Figure 6)**. Of the remaining organizations, 22% conduct penetration tests more frequently: 10% are doing it on a monthly basis, 9% weekly, and 3% daily. Six percent indicated an "other" response and described the frequency of their penetration tests as every other year, when new systems are introduced, prior to contracting with a third-party, or for other reasons.

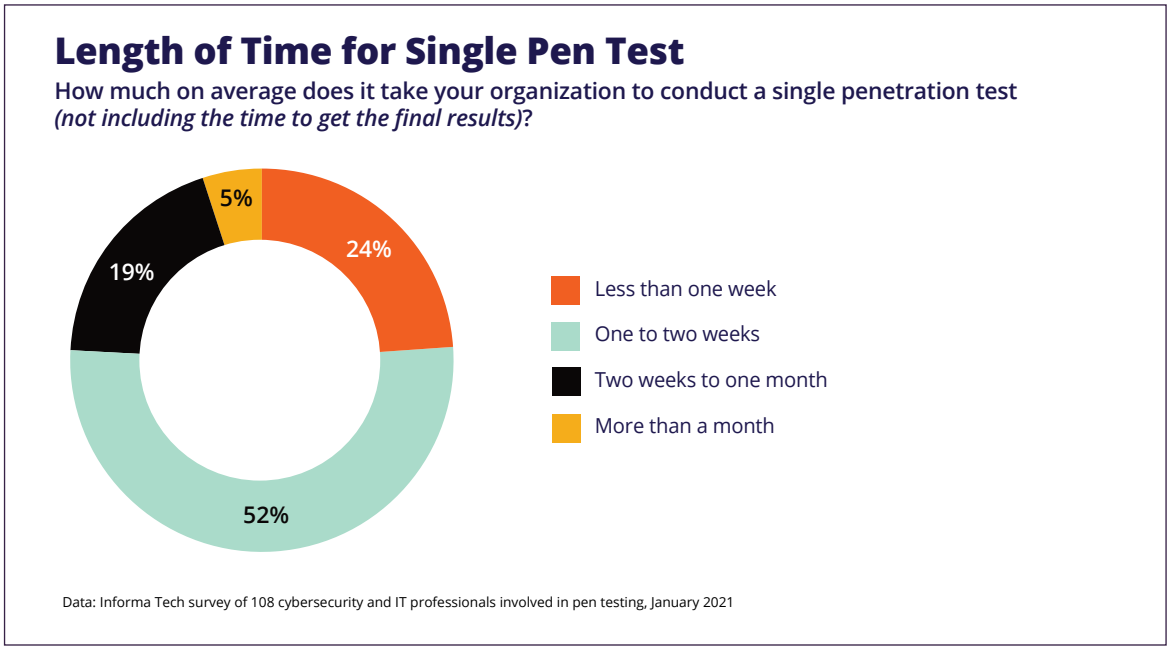
Figure 6



Ic. Lengthy Time to Get Results

Both the time needed for conducting penetration tests and the time involved in getting results present major challenges as well. Between conducting a test and receiving the results, a substantial number of organizations require at least one month for a single penetration test. Testing alone takes weeks. Seventy-one percent report taking from one week to one month to conduct a single penetration test (**Figure 7**). For 5%, it takes more than a month. Getting test results also takes too long. More than one-quarter (26%) have to wait between one and two weeks, and 13% wait even longer than that.

Figure 7



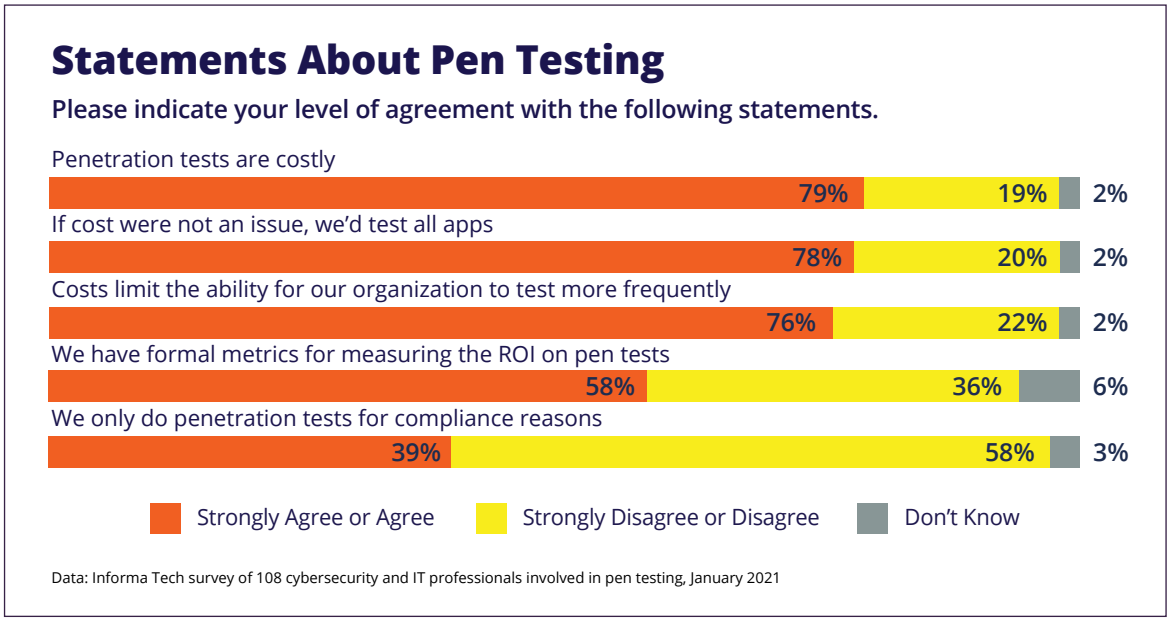
Id. Validation and Remediation Delays

Once organizations have their penetration-testing results, they are challenged to use them effectively because the identified issues take too long to triage, are not relevant, and take too long to remediate. Forty-seven percent have a hard time getting actionable output from the tests, and 70% "agreed" or "strongly agreed" that the triage process — or the process of sorting out what's a true positive and what's a false positive along with ordering vulnerabilities by severity — takes too long. Sixty-five percent identify the tests as surfacing too many vulnerabilities, and three-quarters say remediating the identified risks takes too long. All these issues represent a major weakness at a time when threats are evolving faster than ever and adversaries are constantly looking for new and unknown vulnerabilities to exploit.

Ie. Expensive

Many organizations want to improve the depth and frequency of their penetration tests, but cost considerations are holding them back. Some 79% of respondents report penetration tests as being too costly, and almost the same number (76%) describe cost as hampering their ability to test more frequently (**Figure 8**). Seventy-eight percent would increase the depth of their penetration tests to cover all assets if cost were not a factor.

Figure 8



Looking into cost, we find that survey data shows that some 12% of organizations currently spend more than $1 million annually conducting these tests, and another 8% spend between $500,000 and $1 million. Another 30% describe their organizations as spending between $100,000 and $500,000 annually on penetration tests, and 35% — or more than one in three — spend up to $100,000 per year on the exercise. However, for all of this investment in penetration testing, there are still major concerns with its viability for measuring security posture and preventing breaches.

II. Is There Still Value to Pen Testing?

Given all of the drawbacks to penetration testing, it's still important to note that there is a place for it. Pen testing is still a valid way to surface some vulnerabilities in specific, scoped portions of an attack surface at a single point in time. Penetration tests also have the benefit of being executed by skilled security professionals who bring human creativity to complex challenges; they can surface deep issues that automation is still unable to identify reliably. Many security teams use legacy pen testing to satisfy compliance requirements around web app/software releases or M&A.

When penetration testing is required, it is best used in addition to, not in place of, other security practices. In a world of continuous development and continuous integration, legacy pen tests used alone leave too much of an organization's attack surface exposed. It also does not provide a true picture of security posture and overall readiness or effectiveness of an organization's security.

III. Recommendations

The new research confirms that traditional penetration tests alone are no longer sufficient to protect organizations against current and emergent threats. What's required is an approach to risk detection that is more comprehensive, frequent, and cost-effective than the penetration tests that organizations currently conduct. The approach needs to enable continuous discovery of all attacker-exposed assets across the organization and in closely related environments such as those belonging to subsidiaries, partners, suppliers, and cloud service providers.

For maximum effectiveness, organizations need to employ the methodologies and techniques that attackers use to find and probe all Internet-exposed assets for risks that can be exploited. To accelerate the time it takes to get results, organizations will want to triage risks based on business impact, purpose, and ownership of assets so that IT and security teams can focus remediation efforts on the most critical risks and know who, in their large organizations, to consult with on risk reduction. Finally, organizations will benefit from finding ways to automatically validate fixes to reduce validation timeframes and delays.

IV. Conclusion

Many organizations are conducting penetration tests to detect and mitigate threats yet remain dangerously vulnerable. CyCognito's research shows that when using penetration testing as a security practice organizations lack visibility over their Internet-exposed assets, resulting in blind spots that are vulnerable to exploits and compromise.

Prohibitive testing costs are preventing organizations from conducting penetration tests broadly or frequently enough to cover the entire attack surface or at a level deep enough to test all assets and applications that are at risk.

Because penetration tests are not being conducted on a continuous basis, many organizations are getting only a limited point-in-time assessment of their security status and would be well served to seek out solutions that address penetration-testing shortfalls.

V. Methodology

CyCognito commissioned Informa Tech to research the current state of penetration-testing practices at enterprise organizations with 3,000 or more employees. The survey queried 108 IT and security managers involved in penetration testing on their reasons and processes for conducting these tests, the ROI, and the challenges associated with conducting them on a regular basis. The survey was conducted online in December 2020 and January 2021. Respondents were recruited via emailed invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database. Informa Tech was responsible for all survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

The survey only included respondents who identify themselves as being involved in determining the need for penetration tests and in selecting, purchasing, or using the results of penetration-testing technologies at organizations with 3,000 or more employees.

Thirty-eight percent of the respondents are from organizations that employed 20,000 or more employees, and 21% work at organizations with between 10,000 and 19,999 employees. The remaining 41% are employed at organizations with between 3,000 and 9,999 workers.

The survey queried respondents with job titles that include cybersecurity/information security director, IT director/head, chief security officer (CSO/CISO), and cybersecurity/information security manager. Other titles include CIO/CTO, security architect, threat intelligence director, and chief privacy officer. Respondents represent organizations from more than 16 industry verticals such as banking/financial services, government, technology, education, healthcare, and manufacturing.

About CyCognito

CyCognito was founded by offensive security experts whose deep understanding of attacker techniques led them to create a totally new approach to risk assessment. CyCognito's mission is to help organizations identify and eliminate critical security risk that is often unknown to them — the attackers' paths of least resistance.

Learn more at **CyCognito.com**