Ponemon INSTITUTE

The State of Breach and Attack Simulation and the Need for Continuous Security Validation: A Study of US and UK Organizations

Research sponsored by Cymulate

Independently Conducted by Ponemon Institute LLC

November 2020

© 2020 Ponemon Institute Research Report

The State of Breach and Attack Simulation and the Need for Continuous Security Validation: A Study of US and UK Organizations

Prepared by Ponemon Institute, November 2020

Part 1. Introduction

The purpose of the research, sponsored by Cymulate, is to better understand how the rapidly evolving threat landscape and the frequency of changes in the IT architecture and in security are creating new challenges. The research focuses on the testing and validation of security controls in this extremely dynamic environment. We also seek to understand the issues organizations have in their ability to detect and remediate threats through assessments and testing of security controls.

Although change has always been a constant in both IT and cybersecurity, COVID-19 has accelerated business digitization and security adaptations. Seventy-nine percent of respondents say that they have had to modify security policies to accommodate working from home.

Sixty-two percent of respondents say their organizations had to acquire new security technologies to protect WFH, and yet 62 percent of respondents say their organizations did not validate these newly deployed security controls.

Ponemon Institute surveyed 1,016 IT and IT security practitioners in the United States and United Kingdom who are familiar with their organizations' testing and evaluation of security controls. An average of 13 individuals staff the security team in organizations represented in this research.

Following are key takeaways from the research.

- Sixty-one percent of respondents say the benefit of continuous security validation or frequent security testing is the ability to identify security gaps due to changes in the IT architecture followed by 59 percent of respondents who say it is the ability to identify security gaps caused by human error and misconfigurations.
- Sixty percent of respondents say their organizations are making frequent changes to security controls; daily (27 percent of respondents) and weekly (33 percent of respondents). Sixty-seven percent of respondents say that it is very important to test that the changes applied to the security controls have not created security gaps such as software bugs or vulnerabilities, misconfigurations and human error.
- Seventy percent of respondents say it is important to validate the effectiveness of security controls against new threats and hacker techniques and tactics.

The following findings are based on a deeper analysis of the research.

Vigilance in testing the effectiveness of security controls increases confidence that security controls are working as they are supposed to.

- Organizations that self-reported their organization is vigilant in testing the effectiveness of their security controls (38 percent respondents) have a much higher level of confidence that their organization's security controls are working as they are supposed to. Of the 22 percent of respondents who rate their level of confidence as high, almost half (47 percent) of respondents say they are vigilant in their effectiveness testing.

High confidence in security controls increases the security posture in an evolving threat landscape.

- Organizations that have a high level of confidence that their organization's security controls are working as they are supposed to are applying changes to security controls (e.g., configuration setting, software or signature update policy rules, etc.) daily or weekly.

- These organizations have a much lower percentage of security controls that fail pen testing and/or attack simulation within each cycle. Specifically, 25 percent of respondents with high confidence say less than 10 percent of security controls fail pen testing and/or attack simulation.

Part 2. Key findings

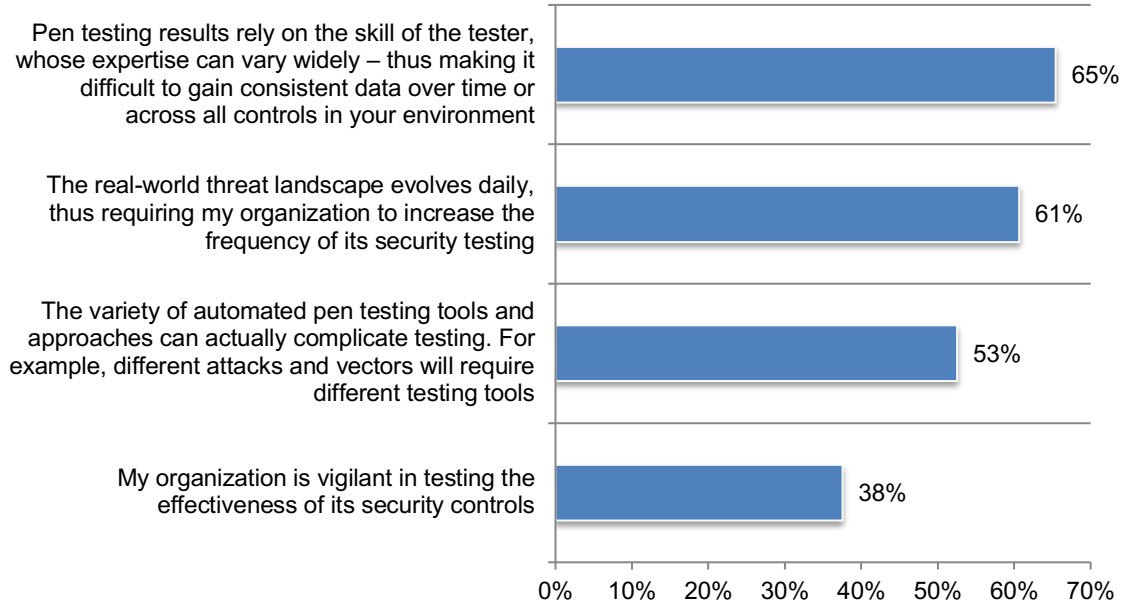
In this section, we present an analysis of the research results. The complete audited findings are presented in the Appendix of this report. The report is organized according to the following topics.

- The impact of current approaches to the testing of security controls on an organization's security posture
- Security control validation and Breach and Attack Simulation (BAS)
- Steps taken to address possible security risks due to COVID-19
- Perceptions about the effectiveness of Managed Security Service Providers (MSSPs)
- Differences between organizations in the US and UK

A lack of vigilance in testing, security complexity, the variety of automated pen testing tools and approaches, and variation in the skills of the pen testers are obstacles for organizations to overcome. Only 39 percent of respondents rate the effectiveness of their organizations' approach to testing security controls as very effective or effective.

According to Figure 1, 61 percent of respondents believe frequent testing is critical in an ever-changing threat landscape, however, only 38 percent of respondents say their organization is vigilant in testing the effectiveness of its security controls. What may deter the frequency of testing is that more than half (53 percent) of respondents say the variety of automated pen testing tools and approaches can actually complicate testing. For example, different attacks and vectors will require different testing tools. Pen testing results rely upon the skill of the tester, whose expertise can vary widely—thus making it difficult to gain consistent data over time or across all controls in their environment, according to 65 percent of respondents.

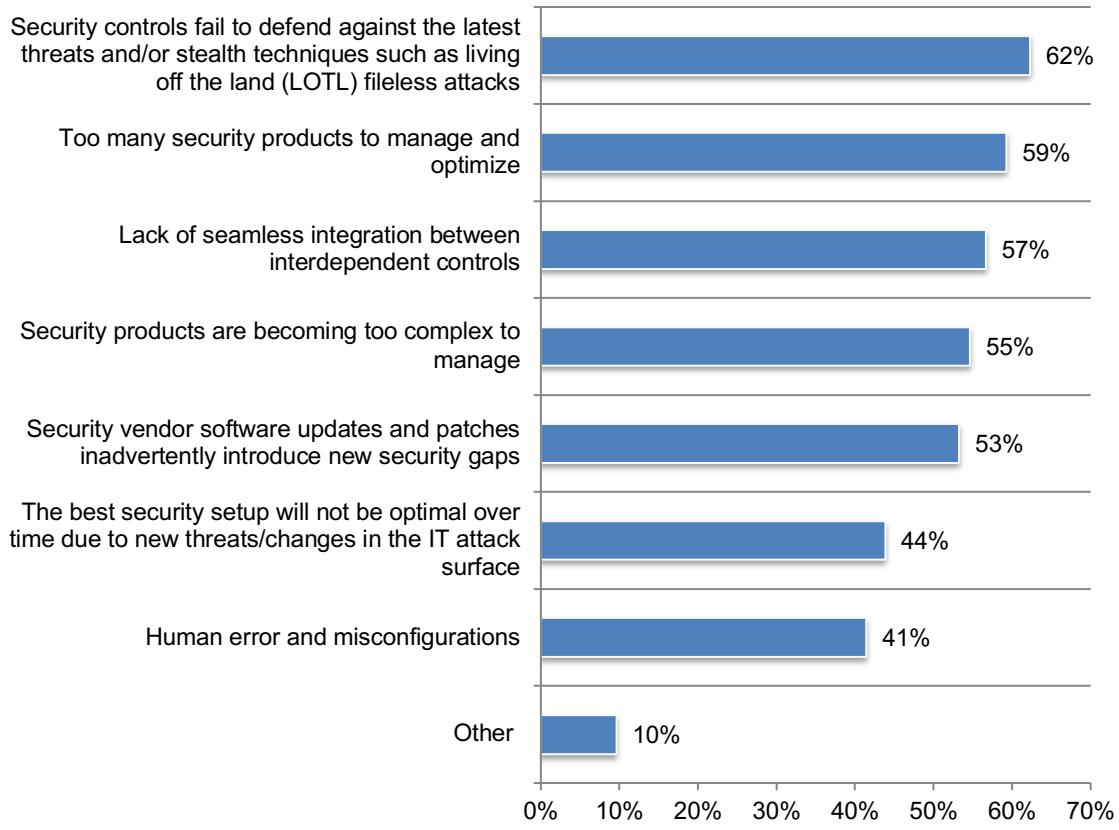
Figure 1. Perceptions about organization's approaches to testing security controls.
Strongly agree and Agree responses combined



The impact of current approaches to testing of security controls on an organization's security posture

Failing to defend against threats and complexity are the primary reasons security controls are ineffective. Only 22 percent of respondents say they are highly confident that their organizations' security controls are working as they are supposed to. Figure 2 presents the reasons for organizations' disappointment in the ability of security controls to keep up with changes in the IT security architecture and the evolving threat landscape. The biggest failure, according to 62 percent of respondents, is that controls are not effective in defending against the latest threats and/or stealth techniques such as living off the land (LoTL) fileless attacks followed by complexity. Specifically, too many security products are complex to manage and optimize (59 and 55 percent of respondents). Other issues are the lack of seamless integration between interdependent controls (57 percent of respondents) and security vendor software updates and patches inadvertently introduce new security gaps (53 percent of respondents).

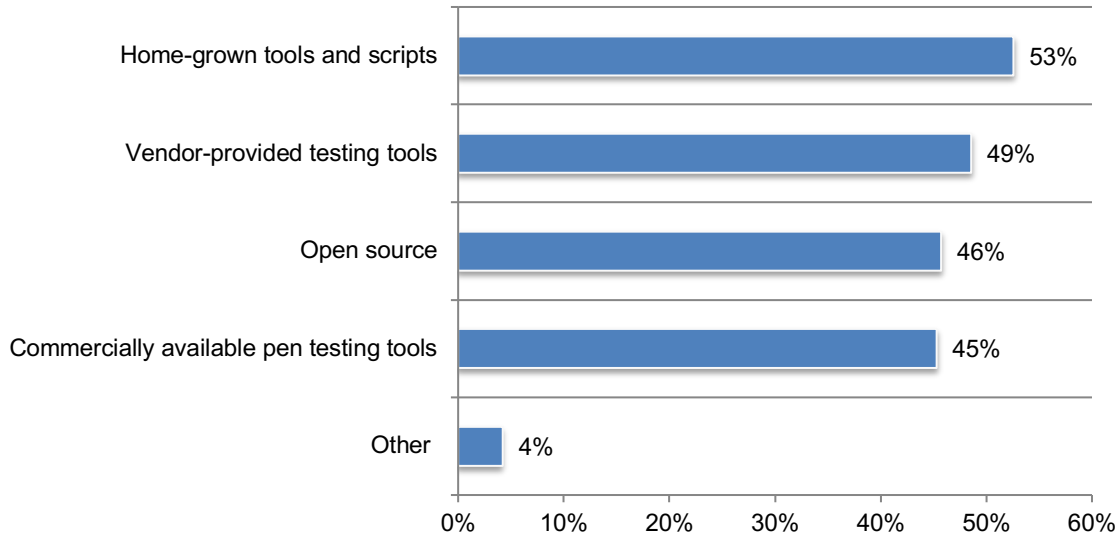
Figure 2. Why security controls do not work as they should
More than one response permitted



Most organizations are testing their security controls without success. While 61 percent of respondents say their organizations validate the effectiveness of their security controls, only 29 percent of these respondents rate their testing methods as highly effective.

Figure 3 presents the tools used to test security controls. More than half (53 percent) of respondents say their organizations use home-grown tools and scripts and almost half (49 percent) of respondents say their organizations use vendor-provided testing tools.

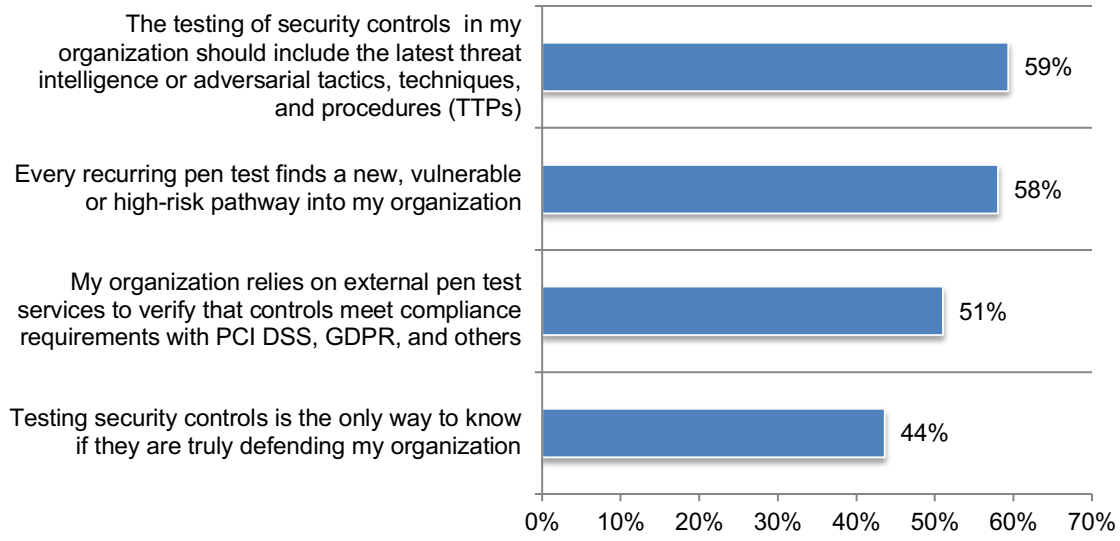
Figure 3. What tools/techniques does your organization use to test security controls?
More than one response permitted



Organizations are looking for alternatives to understand the effectiveness of their security controls. As shown in Figure 4, only 44 percent of respondents say testing of security controls is the only way to know if they are truly defending their organizations, indicating that organizations are looking for additional methods to understand the effectiveness of security controls.

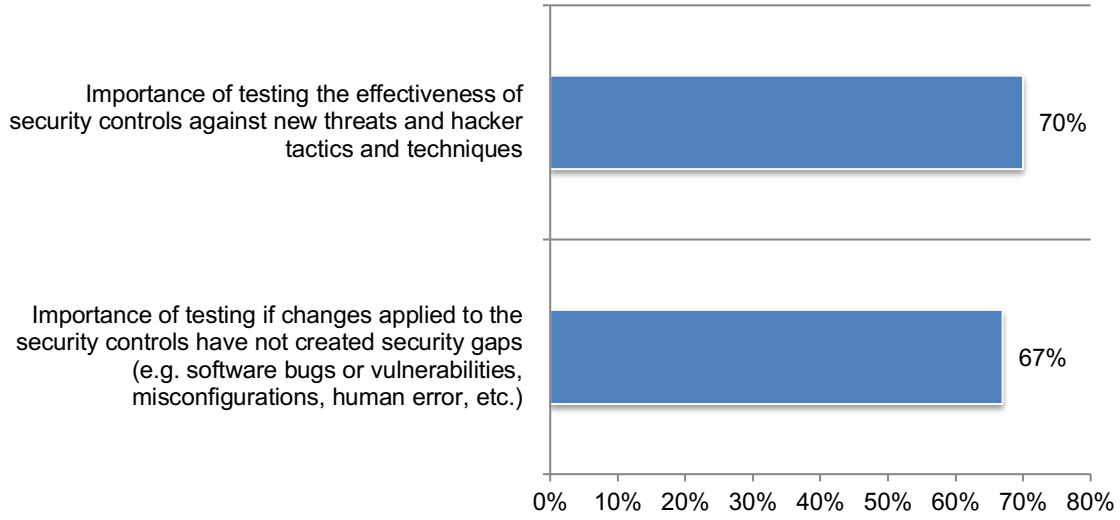
Testing approaches should include the latest threat intelligence or adversarial tactics, techniques and procedures (TTPs), according to 59 percent of respondents. More than half (51 percent) of respondents say their organizations rely on external pen test services to verify that security controls meet compliance requirements. Every recurring pen test finds a new, vulnerable or high-risk pathway into their organizations, according to 58 percent of respondents.

Figure 4. Perceptions about the testing of security controls
Strongly agree and Agree responses combined



According to Figure 5, when asked to rate the importance of testing the effectiveness of security controls against new threats and hacker tactics and techniques on a scale of 1 = not important to 10 = very important, 70 percent of respondents rate it as very important (7+ responses on the scale of 1 to 10). On the 10-point scale, 67 percent of respondents say it is important or very important to test that changes applied to the security controls have not created security gaps (7+ responses).

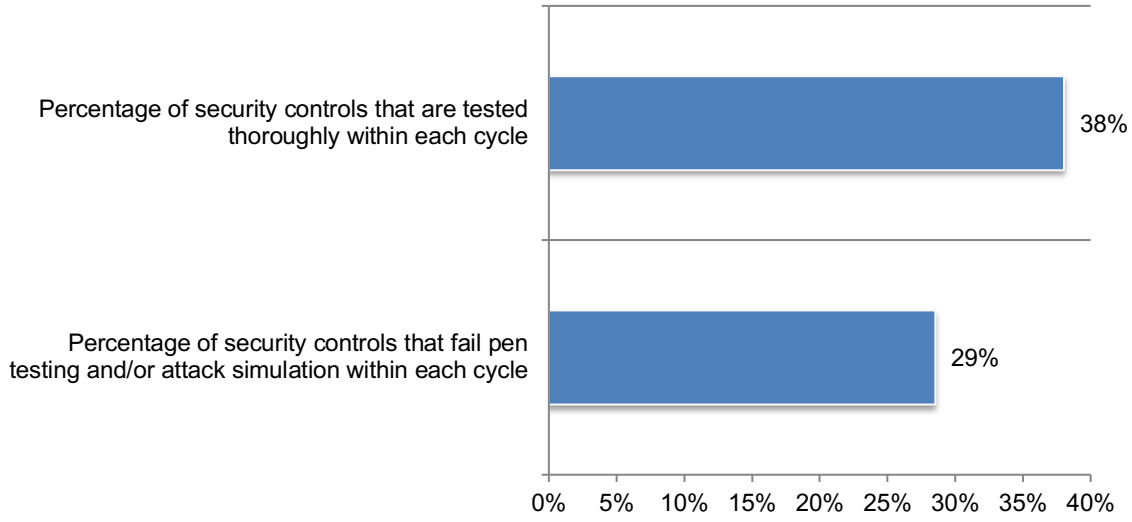
Figure 5. The importance of techniques used to test changes in security controls and effectiveness in testing against new threats
On a scale from 1=not important to 10=very important, 7+ responses presented



Testing of security controls is infrequent. Only 22 percent of respondents say their organizations test daily or weekly. However, as discussed previously, more frequent security testing should be required because the real-world threat landscape evolves daily, according to 61 percent of respondents.

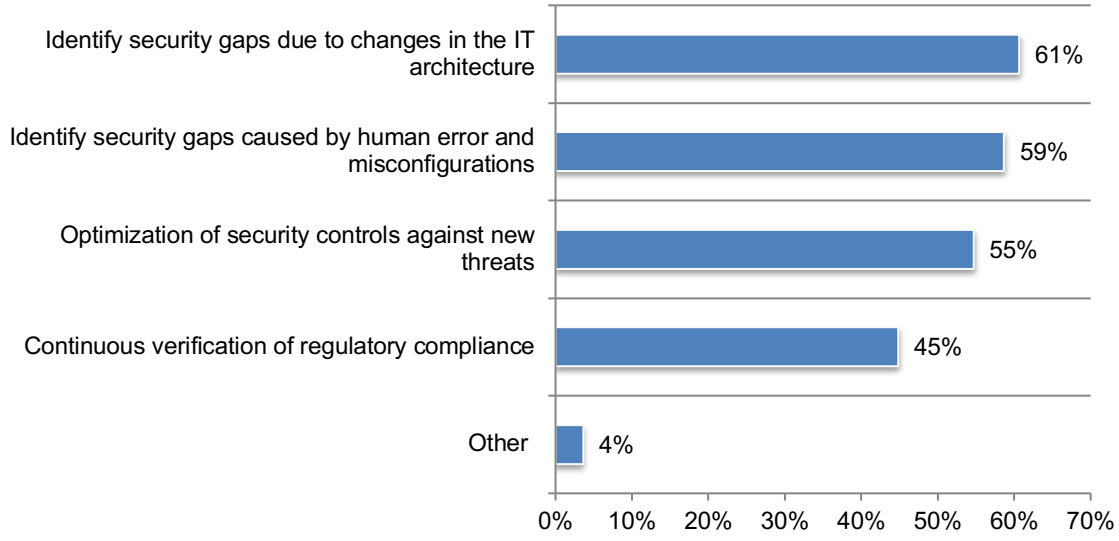
As shown in Figure 6, only an average of 38 percent of security controls are tested thoroughly within each cycle. An average of 29 percent of security controls fail pen testing and/or attack simulations within each cycle, which exposes the organization to attacks against high risk threat vectors.

Figure 6. Failures in testing
Extrapolated values presented



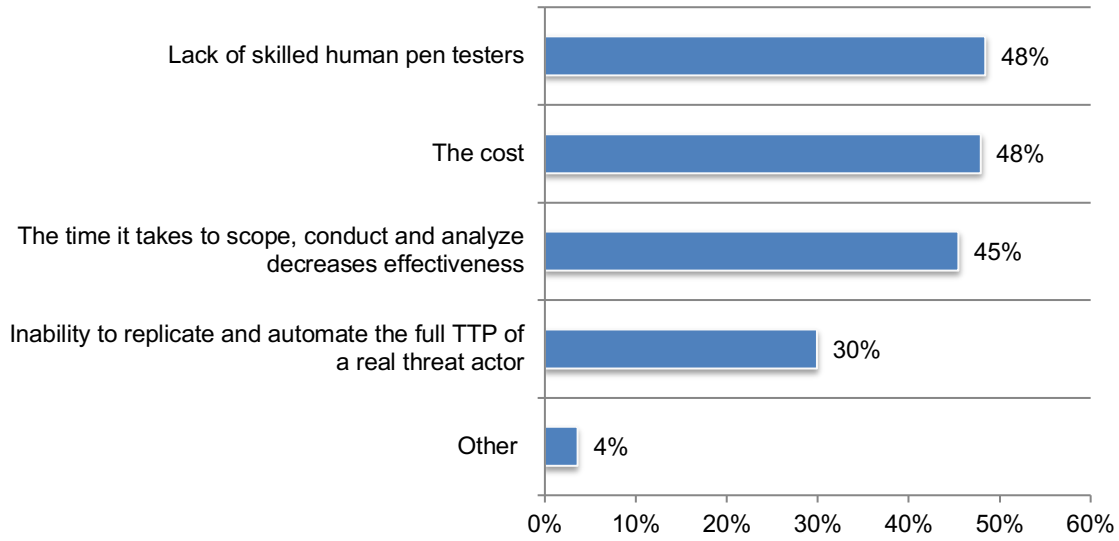
Continuous and frequent security validation would mitigate the risks caused by changes in the IT architecture. The perceived benefits of frequent security testing are primarily to identify security gaps due to changes in the IT architecture (61 percent of respondents), identify security gaps due to human error and misconfigurations (59 percent of respondents) and optimize security controls against new threats (55 percent of respondents), as shown in Figure 7.

Figure 7. What are the perceived benefits of continuous security validation or frequent security testing?
More than one response permitted



Cost and lack of in-house expertise are the main barriers to effective pen testing in organizations. As shown in Figure 8, cost and lack of skilled human pen testers are the main barriers to having effective pen testing. As discussed previously, pen testing results rely on the skill of the tester, whose expertise can vary widely—thus making it difficult to gain consistent data over time or across all controls in the organization's environment, according to 65 percent of respondents.

Figure 8. What are the main barriers to effective pen testing in organizations?
More than one response permitted

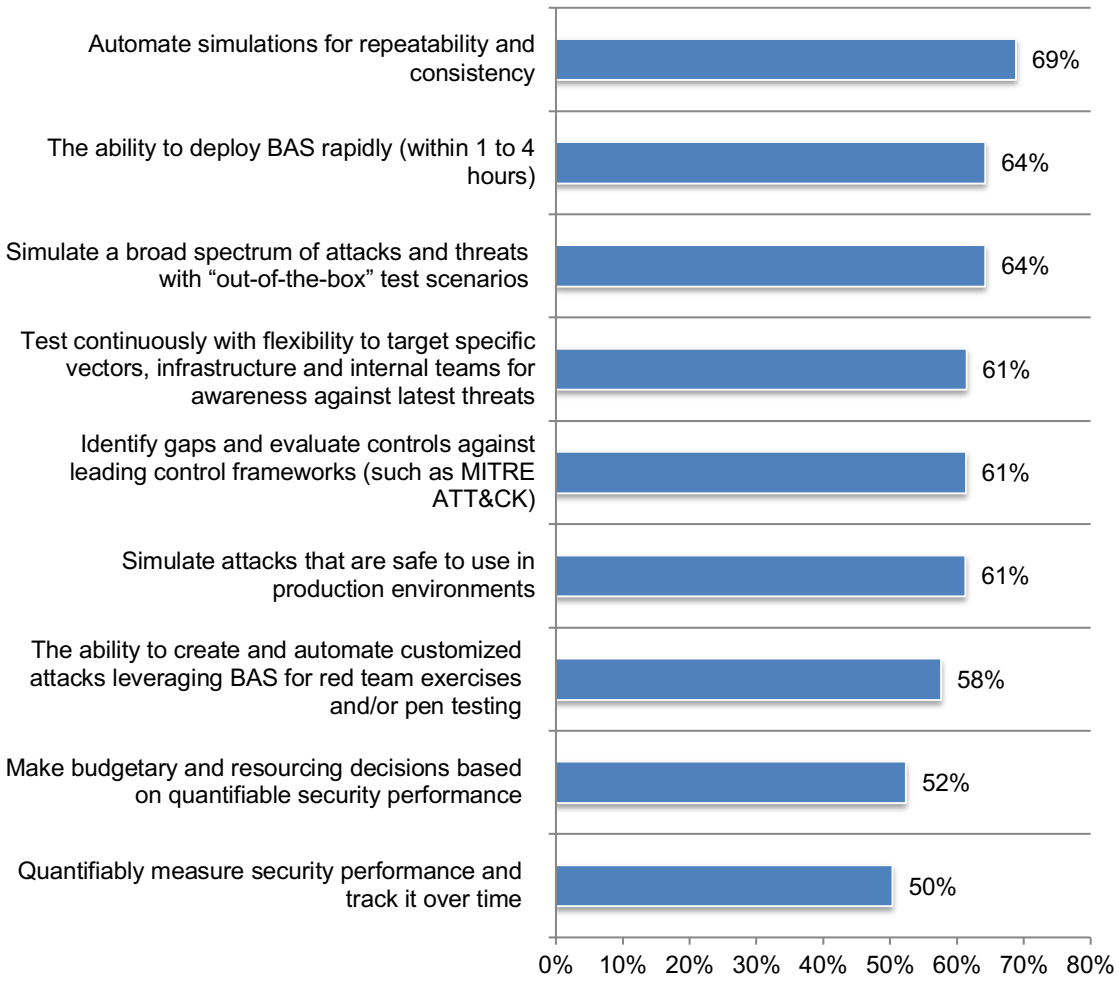


Security Control Validation with Breach and Attack Simulation (BAS)

Breach and attack simulation allow organizations to validate the effectiveness of their security controls continually and consistently against real world attacks. It automates a broad spectrum of attacks over multiple attack vectors against the enterprise infrastructure. The results of these life-like attacks identify security gaps and misconfigurations, providing detailed remediation guidance. Adversarial simulations are also used in purple team exercises to stress test incident detection and response capabilities. Using BAS removes the risks to production environments inherent with other testing approaches.

Thirty-seven percent of respondents say their organizations currently use BAS and 40 percent of these respondents plan to acquire BAS within 12 months. Of these respondents, 43 percent prefer a cloud-based BAS deployment and 39 percent of respondents prefer it to be on-premises. Eighteen percent of respondents have no preference. Organizations with BAS consider the following nine features of BAS as the most important. As shown in Figure 9, the top three features are automated simulations for repeatability and consistency (69 percent of respondents), the ability to deploy BAS rapidly (within 1 to 4 hours) (64 percent of respondents) and the simulation of a broad spectrum of attacks and threats with "out-of-the-box" test scenarios (64 percent of respondents).

Figure 9. The most important features for a BAS
Very important and Important responses combined



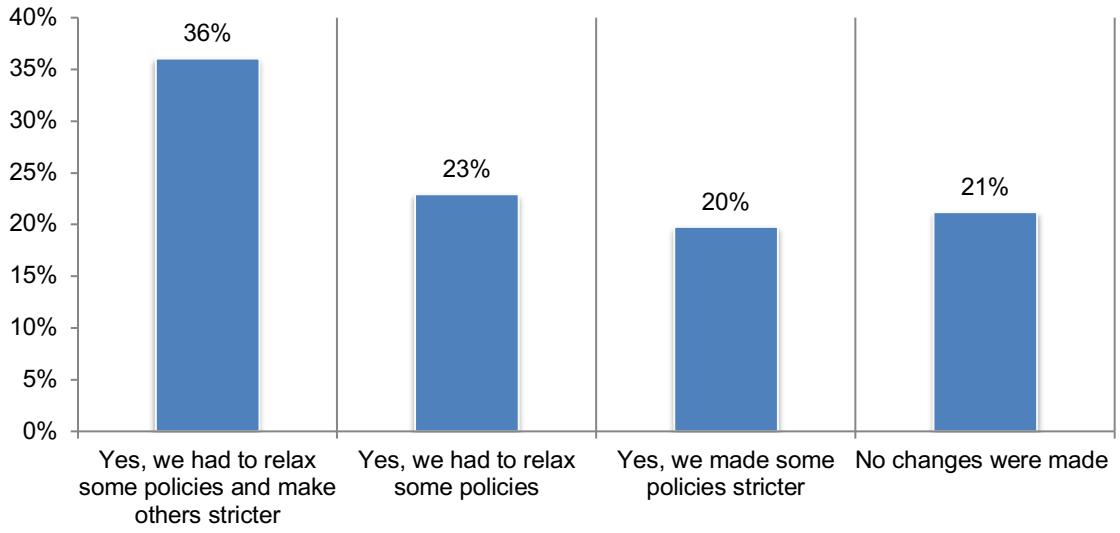
Steps taken to address security risks due to COVID-19

COVID-19 has worsened the threat landscape for many organizations. Security risks created by COVID-19 include a lack of physical and cybersecurity in the teleworker's workspace and phishing and social engineering scams directed at remote workers.

To ensure a secure remote workforce, organizations are investing in new security products and services but not making security policies stricter. Sixty-two percent of respondents say their organizations have acquired new security products and/or services to protect the rapid expansion of a remote workforce caused by COVID-19.

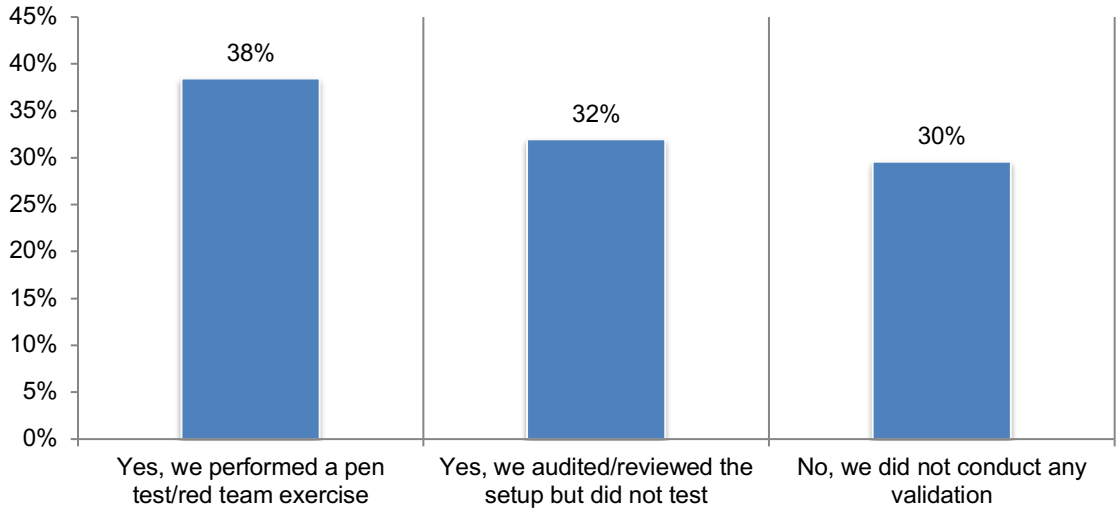
However, as shown in Figure 10, only 20 percent of respondents say their organizations made security policies stricter because of remote working. Thirty-six percent of respondents say their organizations relaxed some policies and made others stricter.

Figure 10. Did your organization change or relax security policies to accommodate remote working?



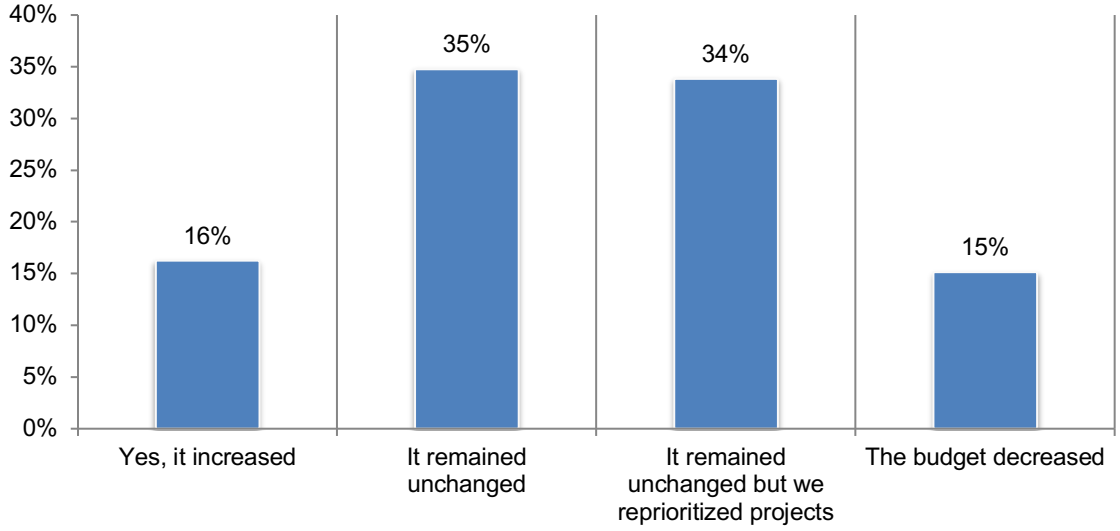
Many organizations are not testing the controls to ensure they protect remote working. Only 38 percent of respondents performed a pen test to validate the effectiveness of the security controls that protect remote working. Thirty percent of respondents say their organizations did not conduct any validation and 32 percent of respondents say their organizations reviewed the controls but did not test.

Figure 11. Did your organization validate the effectiveness of the security controls that protect remote working?



Despite the need to invest in new security products and services, few organizations (16 percent of respondents) increased their IT security budget. Thirty-five percent of respondents say the budget remained unchanged and 34 percent of respondents say the budget remained unchanged, but projects were reprioritized.

Figure 12. Did your IT security budget change to address the unique security circumstances created by the pandemic?

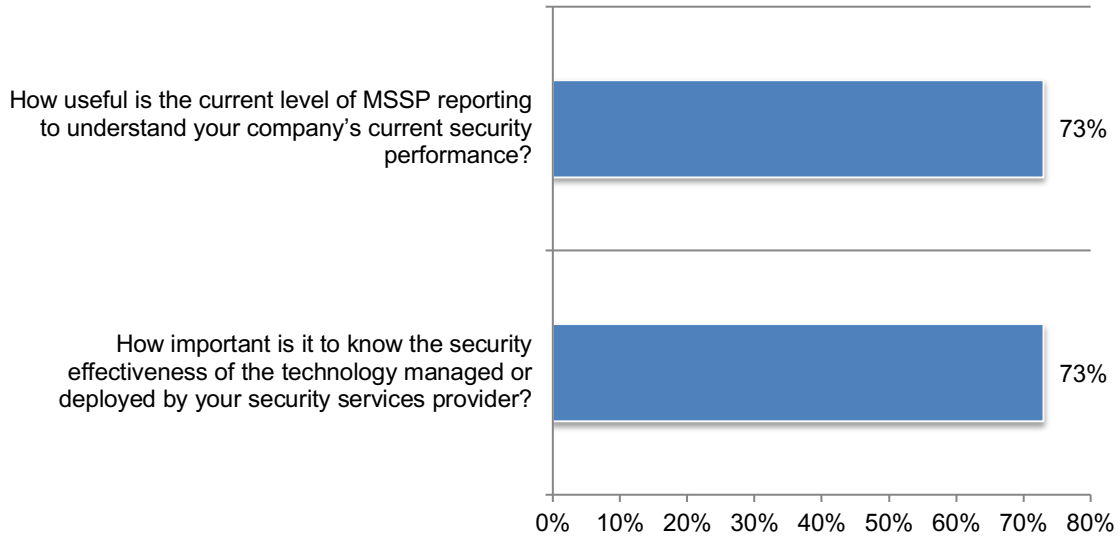


Perceptions about the effectiveness of Managed Security Services Providers (MSSPs)

Most organizations believe their MSSPs are doing a good job. Forty percent of respondents say their organizations have engaged an MSSP for part of their security infrastructure (19 percent) or for all of their security infrastructure (21 percent). Of these respondents, 79 percent of respondents are satisfied (35 percent) or very satisfied (44 percent) with their MSSP.

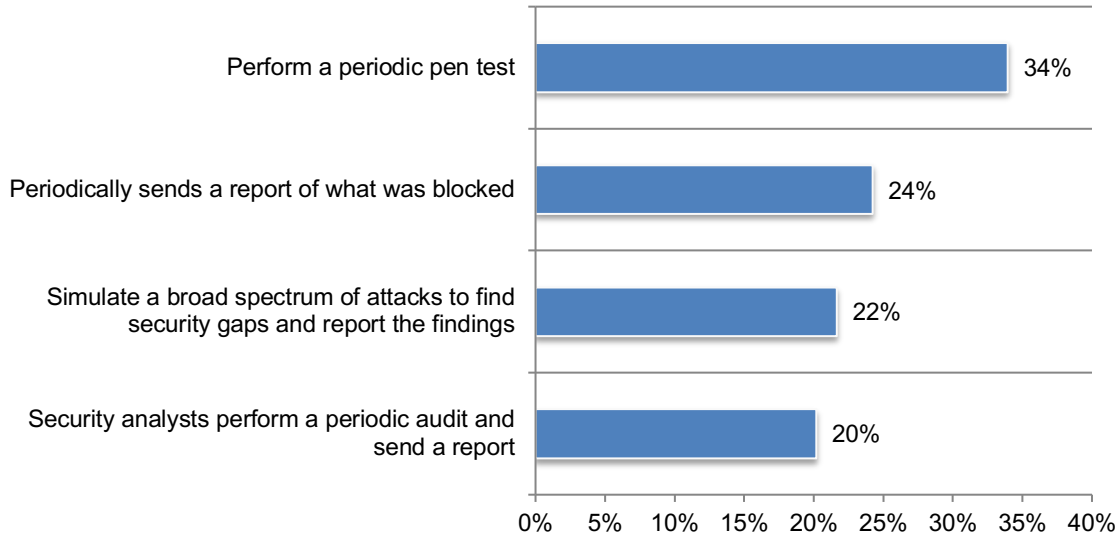
As shown in Figure 13, when asked to rate the importance of knowing the security effectiveness of the technology managed or deployed by the MSSP on a scale of 1 = not important to 10 = very important, 73 percent of respondents say it is important or very important. Similarly, when asked to rate the usefulness of their MSSPs' level of reporting about their organizations' security performance from 1 = not useful to 10 = very useful, 73 percent say such reporting is very useful.

Figure 13. How important is it to know the effectiveness of the MSSPs' technology and to understand your company's current security performance?
On a scale from 1 = not useful to 10 = very useful
On a scale from 1 = not important to 10 = very important, 7+ responses presented



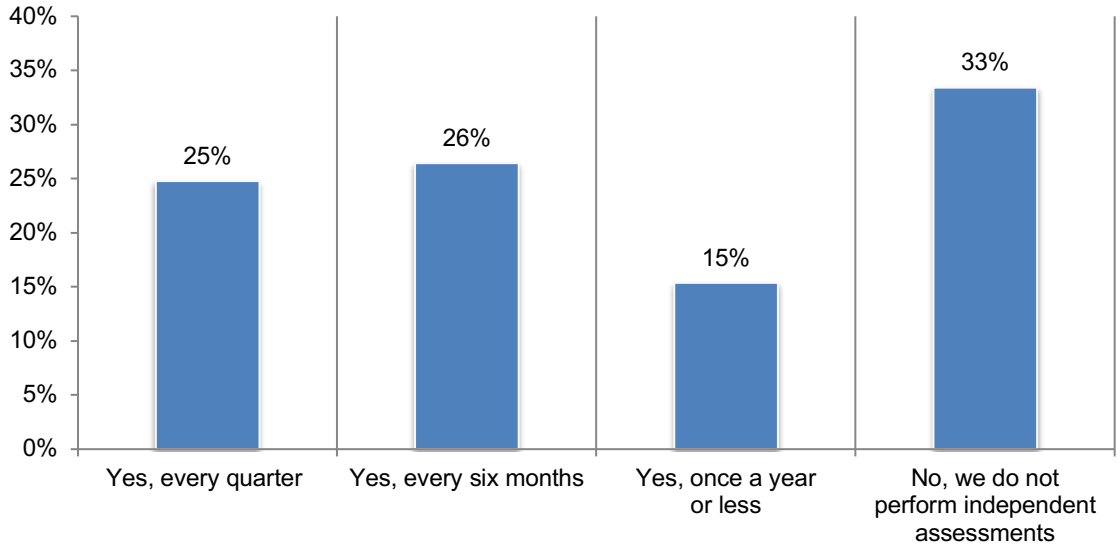
More than a third (34 percent) of respondents say their MSSPs perform a periodic pen test to assure their organization of the quality of the services they provide. However, only 22 percent of respondents say their MSSPs simulate a broad spectrum of attacks to find security gaps and report findings, as shown in Figure 14.

Figure 14. How does your MSSP assure your organization of the quality of the services they provide?
More than one response permitted



Fifty-one percent of respondents say their organizations conduct independent assessments to verify that their MSSPs is protecting their organizations effectively every quarter (25 percent of respondents) or every six months (26 percent of respondents).

Figure 15. Does your organization perform any form of independent assessments to verify that its MSSP providing effective protection?

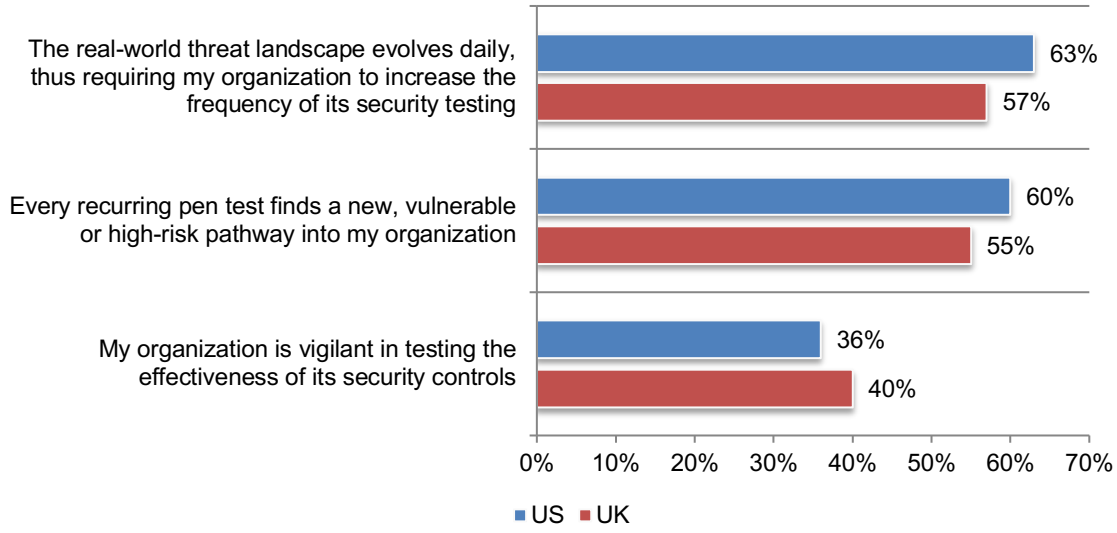


Differences between the United States and United Kingdom

In this section, we provide an analysis of the differences in responses between the United States (621 respondents) and the United Kingdom (395 respondents).

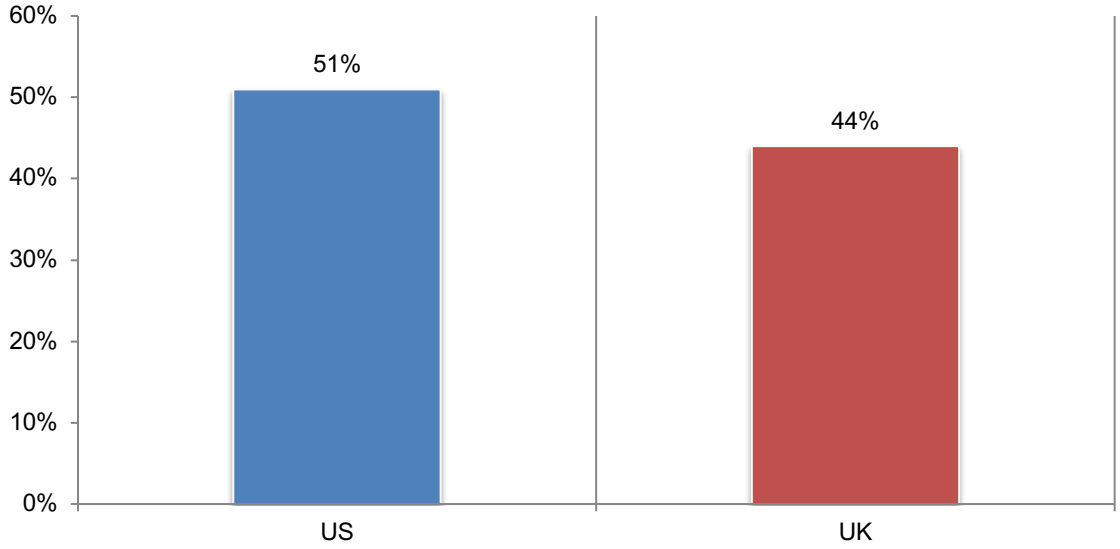
US organizations have a larger security team than UK organizations. US organizations have an average of 15 individuals vs. 10 individuals in UK organizations to staff their security teams. US respondents are more likely to agree that the real-world threat landscape evolves daily requiring an increase in the frequency of security testing (63 percent of US respondents vs. 57 percent of UK respondents), as shown in Figure 16.

Figure 16. Perceptions about security control validation
Strongly agree and Agree responses combined



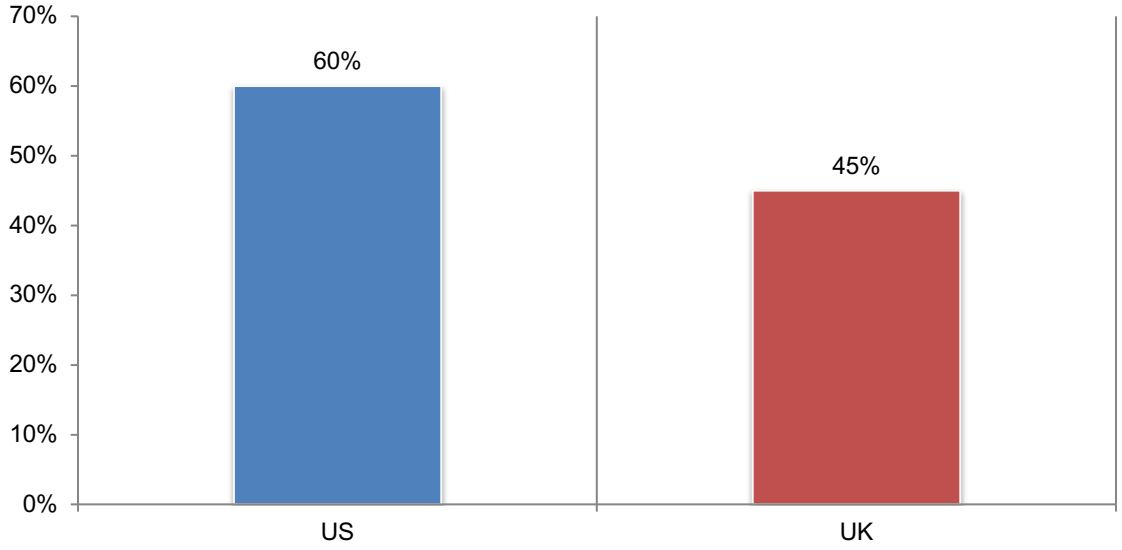
US respondents have more confidence that their security controls are working as they should. Fifty-one percent of US respondents vs. 44 percent of UK respondents are very confident in the effectiveness of their security controls, as shown in Figure 17.

Figure 17. How confident are you that your organizations security controls are working as they are supposed to?
On a scale from 1 = no confidence to 10 = high confidence, 7 + responses presented



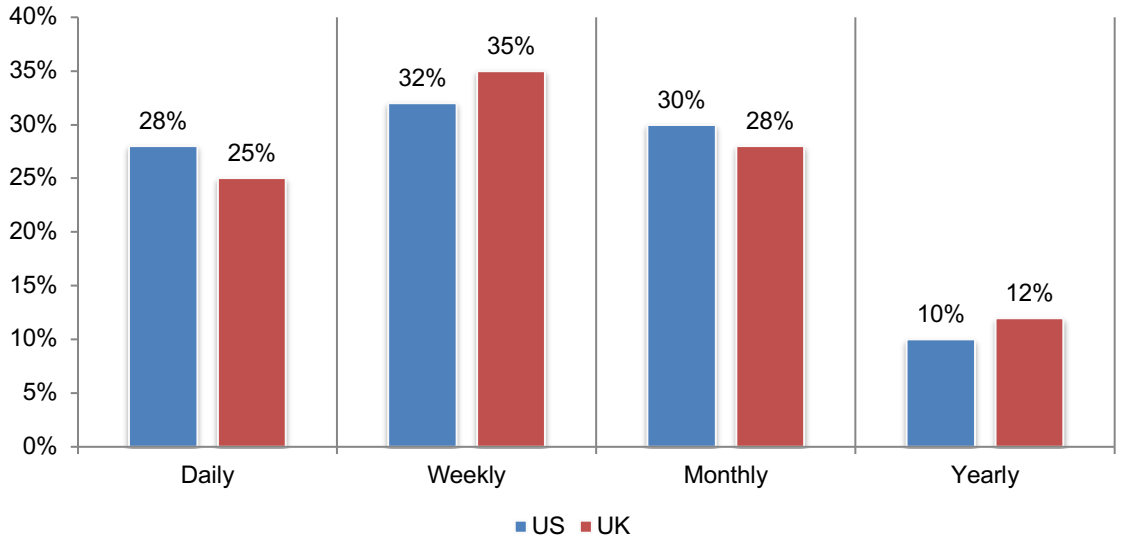
The most salient difference between the US and UK is in respondents' perception of the effectiveness of their organizations' security control validation methods. Sixty-three percent of US organizations and 58 percent of UK respondents test the effectiveness of their organizations' security controls. Of these respondents, 60 percent of US respondents say their security control validation methods are effective or very effective (7+ responses on the 10-point scale) vs. 45 percent of respondents in the UK.

Figure 18. How effective are your organization's security control testing methods?
On a scale from 1 = not effective to 10 = very effective, 7+ responses presented



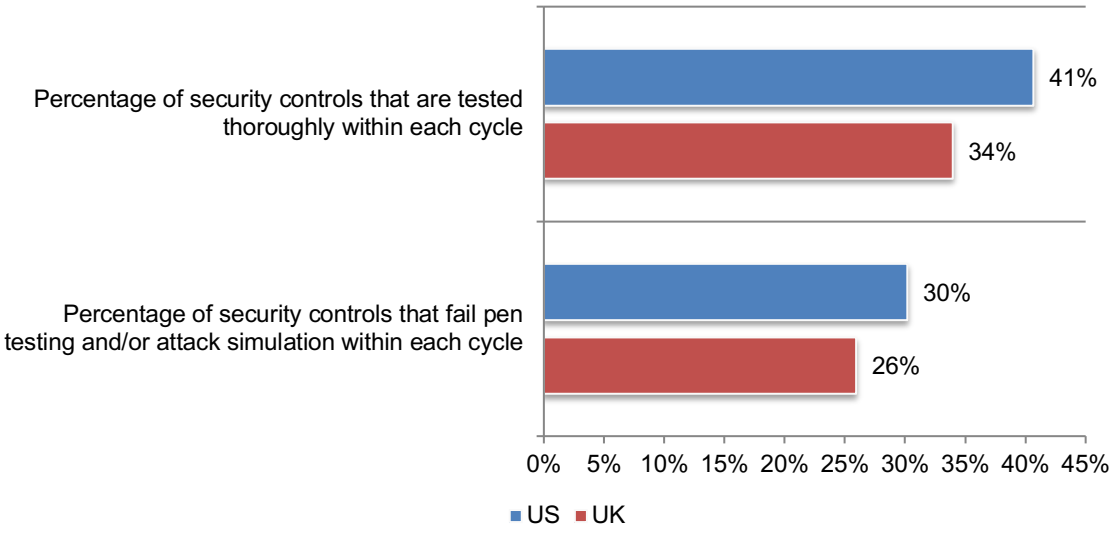
Sixty percent of respondents in both the US and UK apply changes daily or weekly to security controls such as configuration setting, software or signature update policy rules, as shown in Figure 19.

Figure 19. How frequently are changes applied to security controls?



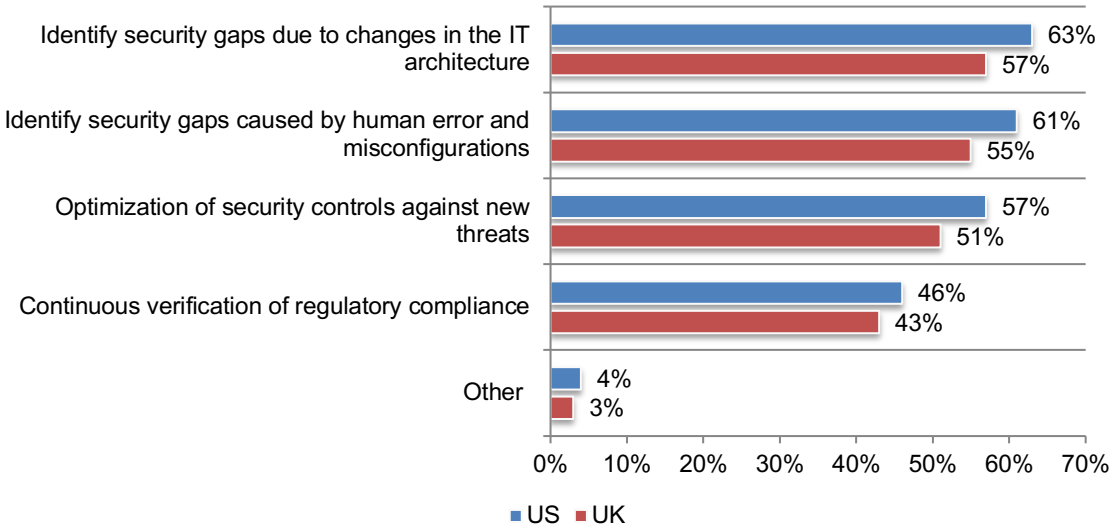
US organizations are more likely to test security controls thoroughly within each cycle. As shown in Figure 20, 41 percent of US respondents vs. 34 percent of UK respondents say their organizations test security controls thoroughly within each cycle. US organizations have a slightly higher percentage of security controls that fail pen testing and/or attack simulation within each testing cycle.

Figure 20. What percentage of security controls are tested within each cycle and what percentage of security controls fail pen testing and/or attack simulation within each cycle
Extrapolated values presented



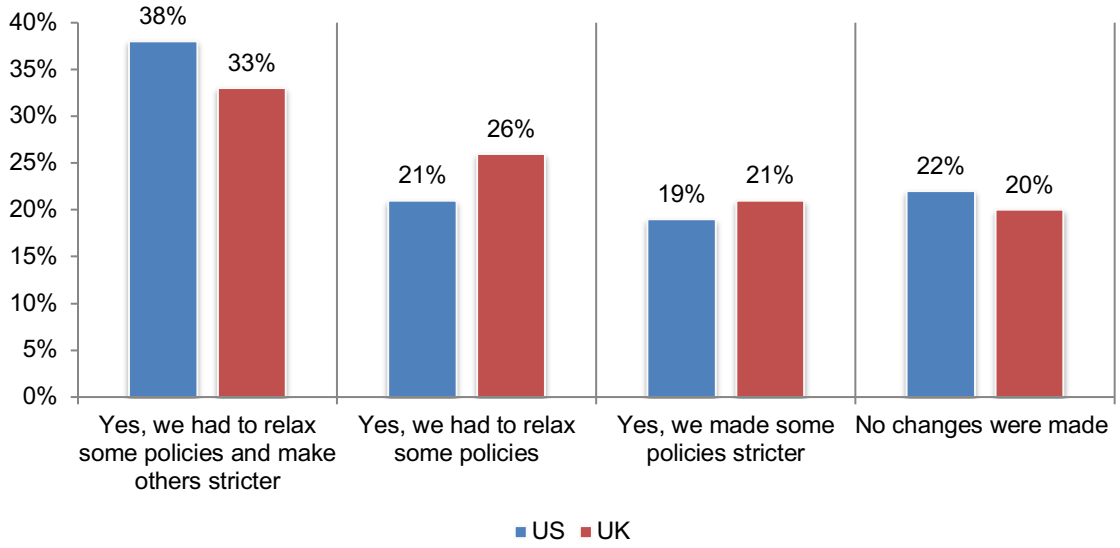
US organizations are more likely to recognize the benefits of continuous security validation or frequent security testing. As shown in Figure 21, 63 percent of US respondents vs. 57 percent of UK respondents say the number one benefit is the ability to identify security gaps due to changes in the IT architecture. The number two benefit is the ability to identify security gaps caused by human error and misconfigurations (61 percent of US respondents vs. 55 percent of UK respondents).

Figure 21. What are the perceived benefits of continuous security validation or frequent security testing?
More than one response permitted



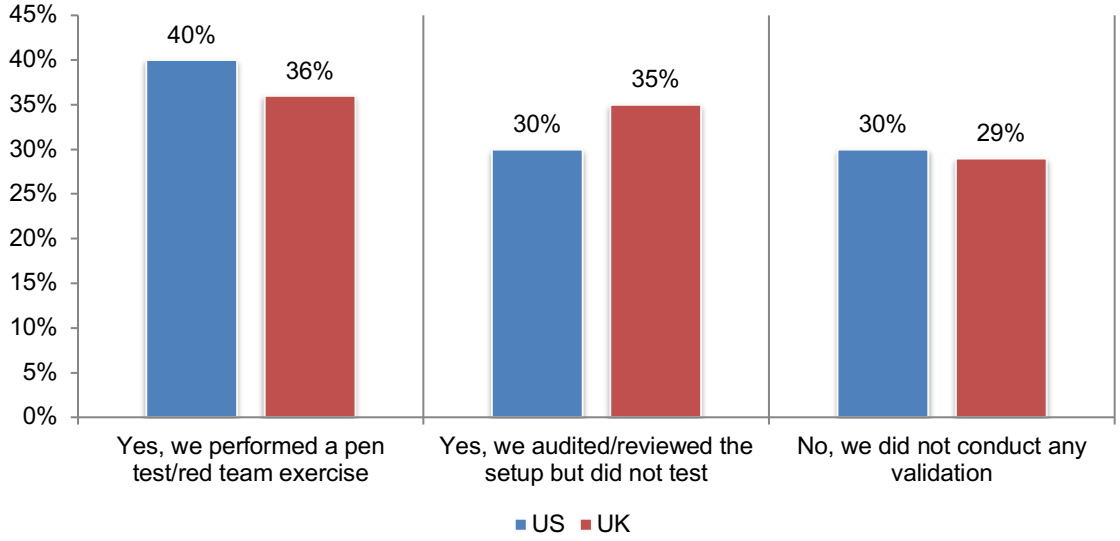
COVID-19 has impacted the security posture of both US and UK organizations. To secure the remote workforce, 63 percent of US respondents and 60 percent of UK respondents say their organizations acquired new security products and/or services to protect the rapid expansion of a remote workforce caused by COVID-19. As shown in Figure 22, most organizations did make changes to their security policies. Thirty-eight percent of US respondents and 33 percent of UK respondents say it was a combination of relaxing some policies and making others stricter.

Figure 22. Did you change or relax security policies to accommodate remote working?



Most organizations in both countries have not tested or validated the security controls that protect remote working. Understandably, organizations were not prepared to have the majority of their workforce working remotely. As shown in Figure 23, 40 percent of US organizations and 36 percent of UK respondents did a pen test to validate the effectiveness of security controls that protect remote working. However, 30 percent of US respondents and 29 percent of UK respondents did not conduct any validation.

Figure 23. Did your organization validate the effectiveness of the security controls that protect remote working?



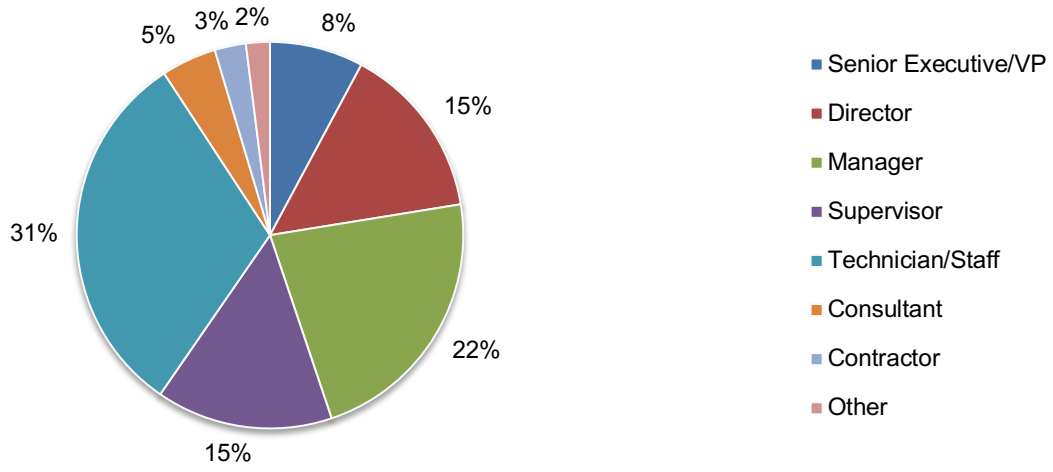
Part 3. Methods

A sampling frame of 26,250 IT or IT security practitioners located in the United States and the United Kingdom, and who are familiar with their organizations' validation and evaluation of security controls were selected as participants in the research. Table 1 shows that there were 1,108 total returned surveys. Screening and reliability checks led to the removal of 92 surveys. Our final sample consisted of 1,016 surveys, a 3.9 percent response.

Table 1. Sample response	US	UK
Sampling frame	16,450	9,800
Total returns	673	435
Rejected or screened surveys	52	40
Final sample	621	395
Response rate	3.8%	4.0%

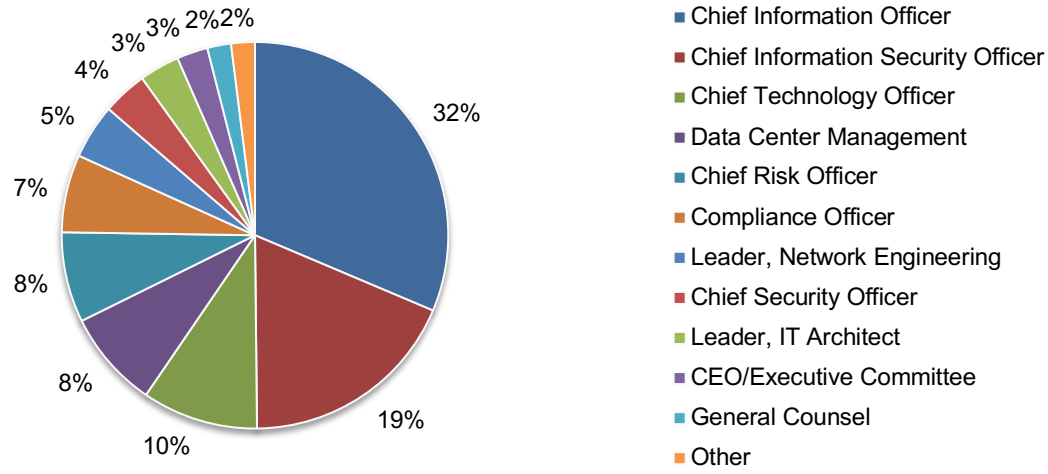
Pie Chart 1 reports the IT security respondents' organizational level within participating organizations. By design, more than half (60 percent) of these respondents are at or above the supervisory levels. Thirty-one percent of these respondents report their position level as technician/staff.

Pie Chart 1. Position level within the organization
(Sample = 1,016)



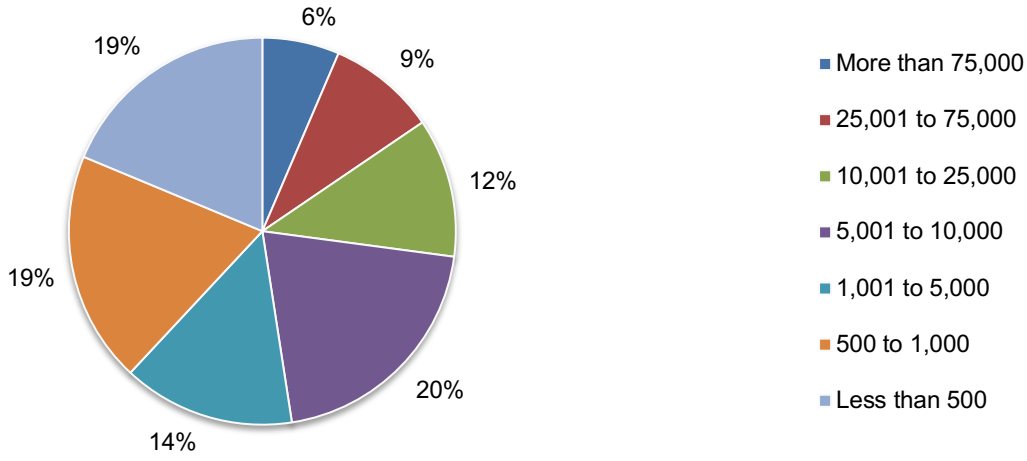
Pie Chart 2 identifies the primary person to whom the IT security respondent reports. Thirty-two percent of respondents identified the chief information officer as the person to whom they report. Another 19 percent indicated they report directly to the chief information security officer and 10 percent of these respondents report to the chief technology officer.

Pie Chart 2. Distribution of respondents according to reporting channel
(Sample = 1,016)



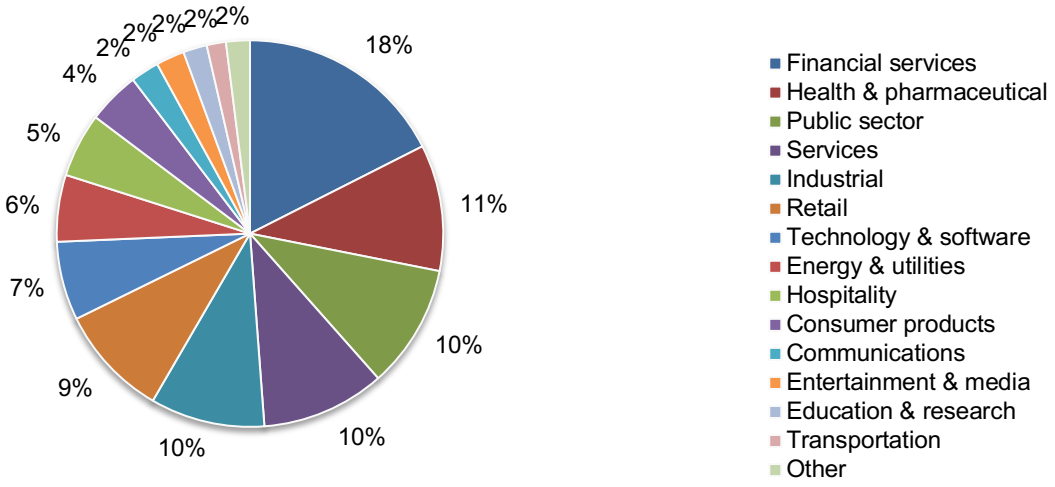
According to Pie Chart 3, more than half (61 percent) of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 3. Distribution of respondents according to full-time global headcount
(Sample = 1,016)



Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceutical (11 percent of respondents), public sector (10 percent of respondents), services (10 percent of respondents), industrial (10 percent of respondents), and retail (9 percent of respondents).

Pie Chart 4. Distribution of respondents according to primary industry classification
(Sample = 1,016)



Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on two samples of survey returns. We sent surveys to a representative sample of IT and IT security and Individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that Individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of IT and IT security practitioners in various organizations the United States and the United Kingdom. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period. Similarly, the accuracy is based on contact information and the degree to which the list is representative of Individuals.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in August 2020.

Survey response	US	UK	Total
Total sampling frame	16,450	9,800	26,250
Total returns	673	435	1,108
Rejected surveys	52	40	92
Final sample	621	395	1,016
Response rate	3.8%	4.0%	3.9%

Part 1. Screening questions

S1. What percentage of your role within your organization is dedicated to the testing and evaluation of security controls?	US	UK	Total
None (stop)	0%	0%	0%
Less than 10%	4%	5%	4%
10% to 25%	19%	23%	21%
26% to 50%	30%	36%	32%
51% to 75%	32%	28%	30%
76% to 100%	15%	8%	12%
Total	100%	100%	100%
Extrapolated value	48%	42%	46%

S2. How familiar are you with your organization's approaches to security control testing?	US	UK	Total
Very familiar	41%	39%	40%
Familiar	40%	35%	38%
Somewhat familiar	19%	26%	22%
No knowledge (stop)	0%	0%	0%
Total	100%	100%	100%

S3. Do you have any responsibility in managing the IT security function within your organization?	US	UK	Total
Yes, full responsibility	34%	32%	33%
Yes, some responsibility	50%	47%	49%
Yes, minimum responsibility	16%	21%	18%
No responsibility (stop)	0%	0%	0%
Total	100%	100%	100%

Part 2. Perceptions of security testing

Q1. How would you rate the effectiveness of your organization's approach to testing security controls?	US	UK	Total
Very effective	16%	18%	17%
Effective	21%	23%	22%
Somewhat effective	23%	25%	24%
Not effective	26%	23%	25%
Ineffective	14%	11%	13%
Total	100%	100%	100%

Attributions: Please rate the following statements about the security control testing approaches within your organization using the agreement scale provided below each item. Strongly Agree and Agree response.	US	UK	Total
Q2a. My organization is vigilant in testing the effectiveness of its security controls.	36%	40%	38%
Q2b. Testing security controls is the only way to know if they are truly defending my organization.	44%	43%	44%
Q2c. The testing of security controls in my organization should include the latest threat intelligence or adversarial tactics, techniques, and procedures (TTPs).	59%	60%	59%
Q2d. My organization relies on external pen test services to verify that controls meet compliance requirements with PCI DSS, GDPR, and others.	53%	48%	51%
Q2e. The real-world threat landscape evolves daily, thus requiring my organization to increase the frequency of its security testing.	63%	57%	61%
Q2f. Every recurring pen test finds a new, vulnerable or high-risk pathway into my organization.	60%	55%	58%
Q2g. Pen testing results rely on the skill of the tester, whose expertise can vary widely – thus making it difficult to gain consistent data over time or across all controls in your environment.	67%	63%	65%
Q2h. The variety of automated pen testing tools and approaches can actually complicate testing. For example, different attacks and vectors will require different testing tools.	51%	55%	53%

Part 3. The state of security testing

Q3. Please rate your level of confidence that your organization's security controls are working as they are supposed to from 1 = no confidence to 10 = high confidence.	US	UK	Total
1 0r 2	8%	15%	11%
3 or 4	15%	16%	15%
5 or 6	26%	25%	26%
7 or 8	30%	20%	26%
9 or 10	21%	24%	22%
Total	100%	100%	100%
Extrapolated value	6.32	5.94	6.17

Q4. What are the main reasons security controls do not work as they are supposed to? Please select all that apply.	US	UK	Total
Lack of seamless integration between interdependent controls	59%	53%	57%
The best security setup will not be optimal over time due to new threats and/or changes in the IT attack surface	45%	42%	44%
Security vendor software updates and patches inadvertently introduce new security gaps	56%	49%	53%
Human error and misconfigurations	43%	39%	41%
Too many security products to manage and optimize	62%	55%	59%
Security products are becoming too complex to manage	57%	51%	55%
My organization's security controls fail to defend against the latest threats and/or stealth techniques such as living off the land (LOTL) fileless attacks	65%	58%	62%
Other (please specify)	10%	9%	10%
Total	397%	356%	381%

Q5. Does your organization incorporate a blue team / red team simulation in order to test its readiness to prevent and contain cyberattacks?	US	UK	Total
Yes, we use a blue team	24%	21%	23%
Yes, we use a red team	24%	35%	28%
Yes, we use both	32%	26%	30%
No, we do not use either	20%	18%	19%
Total	100%	100%	100%

Q6. How many individuals staff your organization's security team?	US	UK	Total
1 to 5	33%	40%	36%
6 to 10	35%	39%	37%
11 to 25	14%	12%	13%
26 to 50	11%	8%	10%
More than 50	7%	1%	5%
Total	100%	100%	100%
Extrapolated value	14.62	10.06	12.85

Q7. What portion of your IT security's budget is allocated to security testing?	US	UK	Total
Less than 1%	2%	5%	3%
1% to 5%	12%	21%	15%
6% to 10%	19%	21%	20%
11% to 25%	25%	30%	27%
26% to 50%	29%	13%	23%
More than 50%	13%	10%	12%
Total	100%	100%	100%
Extrapolated value	25%	19%	23%

Q8. Does your organization have an in-house, IT infrastructure pen-tester/red team?	US	UK	Total
Yes	52%	46%	50%
No	48%	54%	50%
Total	100%	100%	100%

Q9a. Does your organization test the effectiveness of its security controls?	US	UK	Total
Yes	63%	58%	61%
No (please skip to Q10)	37%	42%	39%
Total	100%	100%	100%

Q9b. If yes, how effective are your organization's security control testing methods, from 1=not effective to 10=very effective.	US	UK	Total
1 0r 2	5%	11%	7%
3 or 4	12%	18%	14%
5 or 6	23%	26%	24%
7 or 8	26%	23%	25%
9 or 10	34%	22%	29%
Total	100%	100%	100%
Extrapolated value	6.94	6.04	6.59

Q9c. If yes, what tools/technologies does your organization use to test security controls? Please select all that apply.	US	UK	Total
Vendor-provided testing tools	54%	40%	49%
Commercially available pen testing tools	48%	41%	45%
Open source	43%	50%	46%
Home-grown tools and scripts	51%	55%	53%
Other (please specify)	5%	3%	4%
Total	201%	189%	196%

Q10. What are the perceived benefits of continuous security validation or frequent security testing? Please check all that apply.	US	UK	Total
Continuous verification of regulatory compliance	46%	43%	45%
Optimization of security controls against new threats	57%	51%	55%
Identify security gaps due to changes in the IT architecture	63%	57%	61%
Identify security gaps caused by human error and misconfigurations	61%	55%	59%
Other (please specify)	4%	3%	4%
Total	231%	209%	222%

Q11. How frequently are changes applied to security controls (e.g. configuration setting, software or signature update policy rules, etc.)?	US	UK	Total
Daily	28%	25%	27%
Weekly	32%	35%	33%
Monthly	30%	28%	29%
Yearly	10%	12%	11%
Total	100%	100%	100%

Q12. How important is it to test that changes applied to the security controls have not created security gaps (e.g. software bugs or vulnerabilities, misconfigurations, human error, etc.) from 1=not important to 10=very important.	US	UK	Total
1 0r 2	4%	3%	4%
3 or 4	5%	6%	5%
5 or 6	24%	26%	25%
7 or 8	27%	26%	27%
9 or 10	40%	39%	40%
Total	100%	100%	100%
Extrapolated value	7.38	7.34	7.36

Q13. How important is it to test the effectiveness of security controls against new threats and hacker tactics and techniques from 1=not important to 10=very important?	US	UK	Total
1 0r 2	0%	2%	1%
3 or 4	6%	7%	6%
5 or 6	25%	19%	23%
7 or 8	35%	33%	34%
9 or 10	34%	39%	36%
Total	100%	100%	100%
Extrapolated value	7.44	7.50	7.46

Q14. There are two broadly defined approaches to answering the question, “can an attacker get into my organization’s enterprise systems and IT infrastructure?” What best defines your approach?	US	UK	Total
The use of pen-testing teams to attempt to breach your organizations’ defenses	44%	48%	46%
The use of systems that test the effectiveness of each security control	32%	32%	32%
A combination of both approaches	24%	20%	22%
Total	100%	100%	100%

Q15. What best defines the security control (security infrastructure) testing cycle deployed within your organization?	US	UK	Total
Only when an incident or breach occurs	21%	17%	19%
Daily	14%	10%	12%
Weekly	9%	11%	10%
Monthly	6%	8%	7%
Quarterly	8%	9%	8%
Semi-yearly	6%	8%	7%
Yearly	8%	7%	8%
More than yearly	5%	4%	5%
We don’t have a control testing cycle	23%	26%	24%
Total	100%	100%	100%

Q16. What percentage of security controls are tested thoroughly within each cycle?	US	UK	Total
Less than 10%	10%	16%	12%
10% to 25%	20%	27%	23%
26% to 50%	32%	33%	32%
51% to 75%	35%	17%	28%
76% to 100%	3%	6%	4%
Total	100%	99%	100%
Extrapolated value	41%	34%	38%

Q17. What percentage of security controls fail pen testing and/or attack simulation within each cycle?	US	UK	Total
Less than 10%	24%	26%	25%
10% to 25%	32%	35%	33%
26% to 50%	23%	27%	25%
51% to 75%	15%	9%	13%
76% to 100%	6%	3%	5%
Total	100%	100%	100%
Extrapolated value	30%	26%	29%

Q18. What are the main barriers to effective pen testing in your organization? Please selected all that apply.	US	UK	Total
Inability to replicate and automate the full TTP of a real threat actor	33%	25%	30%
Lack of skilled human pen testers	50%	46%	48%
The time it takes to scope, conduct and analyze decreases effectiveness	47%	43%	45%
The cost	51%	43%	48%
Other (please specify)	4%	3%	4%
Total	185%	160%	175%

Part 4. Breach attack simulation (BAS)

Q19a. Does your organization's security control testing utilize BAS, or does it plan to utilize BAS?	US	UK	Total
Yes, we utilize BAS	39%	35%	37%
Yes, we plan to acquire BAS within 12 months	40%	39%	40%
No, we have no plans to acquire BAS within 12 months (please skip to Q22)	21%	26%	23%
Total	100%	100%	100%

Q19b. If yes, what are the most important features of your BAS approach? Please use the 5-point importance scale to rate the importance of each feature. Very Important and Important responses combined.	US	UK	Total
Q19b-1. Simulate attacks that are safe to use in production environments	64%	57%	61%
Q19b-2. Simulate a broad spectrum of attacks and threats with “out-of-the-box” test scenarios	67%	60%	64%
Q19b-3. Test continuously with flexibility to target specific vectors, infrastructure and internal teams for awareness against latest threats	63%	59%	61%
Q19b-4. Automate simulations for repeatability and consistency	70%	67%	69%
Q19b-5. Conduct testing at any time interval – hourly, daily, week or ad hoc	47%	50%	48%
Q19b-6. Identify gaps and evaluate controls against leading control frameworks (such as MITRE ATT&CK)	66%	54%	61%
Q19b-7. Remediate exposure using actionable insights	48%	44%	46%
Q19b-8. Quantifiably measure security performance and track it over time	50%	51%	50%
Q19b-9. Continuously verify regulatory compliance	45%	42%	44%
Q19b-10. Make budgetary and resourcing decisions based on quantifiable security performance	52%	53%	52%
Q19b-11. Test security products before procurement	55%	43%	50%
Q19b-12. Communicate our security performance transparently to upper management	51%	46%	49%
Q19b-13. The ability to create and automate customized attacks leveraging BAS for red team exercises and/or pen testing	58%	57%	58%
Q19b-14. The ability to deploy BAS rapidly (within 1 to 4 hours)	67%	60%	64%

Q20. Does your organization have a BAS deployment preference?	US	UK	Total
Our organization prefers cloud-based	45%	40%	43%
Our organization prefers on-premises	38%	41%	39%
Our organization has no preference	17%	19%	18%
Total	100%	100%	100%

Q21. Does your organization prefer a method for the execution of attack-simulations?	US	UK	Total
Our organization prefers to run individual (atomic) executions	36%	44%	39%
Our organization prefers to run a sequence of chained attack commands	33%	30%	32%
Our organization requires both methods	14%	15%	14%
Our organization has no preference	17%	11%	15%
Total	100%	100%	100%

Part 5. Coronavirus questions

Q22. Did you acquire new security products and/or services to protect the rapid expansion of a remote workforce caused by the Covid-19 pandemic?	US	UK	Total
Yes	63%	60%	62%
No	37%	40%	38%
Total	100%	100%	100%

Q23a. Did you change or relax security policies to accommodate remote working?	US	UK	Total
Yes, we had to relax some policies and make others stricter	38%	33%	36%
Yes, we had to relax some policies	21%	26%	23%
Yes, we made some policies stricter	19%	21%	20%
No changes were made	22%	20%	21%
Total	100%	100%	100%

Q24. Did your organization validate the effectiveness of the security controls that protect remote working?	US	UK	Total
Yes, we performed a pen test/red team exercise	40%	36%	38%
Yes, we audited/reviewed the setup but did not test	30%	35%	32%
No, we did not conduct any validation	30%	29%	30%
Total	100%	100%	100%

Q25. Did your IT security budget change to address the unique security circumstances created by the pandemic?	US	UK	Total
Yes, it increased	17%	15%	16%
It remained unchanged	34%	36%	35%
It remained unchanged but we reprioritized projects	35%	32%	34%
The budget decreased	14%	17%	15%
Total	100%	100%	100%

Part 6. MSSP questions

Q26. Does your company engage an MSSP or MDR?	US	UK	Total
No, and we have no plans to in the next 12 months (please skip to Part 7)	27%	31%	29%
No, but we plan to within the next 12 months (please skip to Part 7)	33%	29%	31%
Yes, for a part of our security infrastructure	17%	22%	19%
Yes, for all of our security infrastructure	23%	18%	21%
Total	100%	100%	100%

Q27. How important is it to know the security effectiveness of the technology managed or deployed by your security services provider from a scale of 1 = not important to 10 = very important?	US	UK	Total
1 0r 2	1%	3%	2%
3 or 4	5%	6%	5%
5 or 6	22%	17%	20%
7 or 8	32%	36%	34%
9 or 10	40%	38%	39%
Total	100%	100%	100%
Extrapolated value	7.60	7.50	7.56

Q28. How useful is the current level of MSSP reporting to understand your company's current security performance from scale of 1 = not useful to 10 = very useful?	US	UK	Total
1 0r 2	2%	1%	2%
3 or 4	7%	8%	7%
5 or 6	18%	20%	19%
7 or 8	35%	34%	35%
9 or 10	38%	37%	38%
Total	100%	100%	100%
Extrapolated value	7.50	7.46	7.48

Q29. How satisfied is your organization with the security services provided by your organization's MSSP on a scale from 1 = not satisfied to 10 = very satisfied?	US	UK	Total
1 0r 2	2%	3%	2%
3 or 4	6%	7%	6%
5 or 6	12%	14%	13%
7 or 8	34%	36%	35%
9 or 10	46%	40%	44%
Total	100%	100%	100%
Extrapolated value	7.82	7.56	7.72

Q30. How does your MSSP assure you of the quality of the services they provide? Please select all that apply.	US	UK	Total
Perform a periodic pen test	32%	37%	34%
Periodically sends a report of what was blocked	25%	23%	24%
Security analysts perform a periodic audit and send a report	19%	22%	20%
Simulate a broad spectrum of attacks to find security gaps and report the findings	24%	18%	22%
Total	100%	100%	100%

Q31. Do you perform any form of independent assessments to verify that your MSSP is protecting your organizations effectively?	US	UK	Total
Yes, every quarter	24%	26%	25%
Yes, every six months	28%	24%	26%
Yes, once a year or less	15%	16%	15%
No, we do not perform independent assessments	33%	34%	33%
Total	100%	100%	100%

Part 7. Your role and organization

D1. What organizational level best describes your current position?	US	UK	Total
Senior Executive/VP	9%	6%	8%
Director	15%	14%	15%
Manager	22%	23%	22%
Supervisor	14%	16%	15%
Technician/Staff	30%	33%	31%
Consultant	5%	4%	5%
Contractor	3%	2%	3%
Other (please specify)	2%	2%	2%
Total	100%	100%	100%

D2. Check the primary person you or your IT security leader reports to within the organization.	US	UK	Total
CEO/Executive Committee	3%	2%	3%
Chief Financial Officer	1%	0%	1%
Chief Information Officer	32%	31%	32%
Chief Information Security Officer	19%	18%	19%
Chief Risk Officer	8%	7%	8%
Chief Security Officer	3%	5%	4%
Chief Technology Officer	9%	11%	10%
Compliance Officer	5%	9%	7%
Data Center Management	9%	7%	8%
General Counsel	2%	2%	2%
Leader, IT Architect	3%	4%	3%
Leader, Network Engineering	5%	4%	5%
Other (please specify)	1%	0%	1%
Total	100%	100%	100%

D3. What is the worldwide headcount of your organization?	US	UK	Total
Less than 500	16%	23%	19%
500 to 1,000	17%	23%	19%
1,001 to 5,000	14%	15%	14%
5,001 to 10,000	22%	18%	20%
10,001 to 25,000	12%	11%	12%
25,001 to 75,000	11%	6%	9%
More than 75,000	8%	4%	6%
Total	100%	100%	100%

D4. What industry best describes your organization's industry focus?	US	UK	Total
Agriculture & food services	1%	0%	1%
Communications	2%	3%	2%
Consumer products	4%	5%	4%
Defense & aerospace	1%	0%	1%
Education & research	2%	2%	2%
Energy & utilities	6%	5%	6%
Entertainment & media	2%	3%	2%
Financial services	18%	17%	18%
Health & pharmaceutical	11%	10%	11%
Hospitality	5%	6%	5%
Industrial	10%	9%	10%
Public sector	10%	11%	10%
Retail	9%	10%	9%
Services	10%	11%	10%
Technology & software	7%	6%	7%
Transportation	2%	1%	2%
Other (please specify)	0%	1%	0%
Total	100%	100%	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from Individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

About Cymulate

Used by organizations to continuously assess their security posture across the full kill chain, uncover security gaps and misconfigurations, and remediate issues effectively, Cymulate provides visibility and KPIs to know how secure you are and to plan and allocate resources effectively.

The Cymulate platform is SaaS-based, making it simple to deploy literally within minutes. It provides out-of-the-box, comprehensive assessments that are updated daily with the latest attack techniques and threats. This enables security teams to test and optimize the efficacy of their security controls against the evolving threats landscape. Cymulate operationalizes the MITRE ATT&CK framework end-to-end, from reconnaissance through to impact and uses the framework extensively to map assessments and results to it.

Cymulate Purple team module enables full customization for security teams to create assessments unique to their security policy and environments and simulate adversarial behavior to exercise incident response playbooks. Cymulate provides the visibility for security professionals to know and control the dynamic environment they operate in.

Run a simple attack simulation to find your security gaps - https://cymulate.com/free-trial/ or Schedule a 30 minutes demo - https://cymulate.com/schedule-a-demo/.