

A man in a dark suit is seen from the back, looking towards a large circular graphic. The graphic features a complex maze pattern in the foreground, transitioning into a grid of dots and circuit-like lines in the background. The overall color scheme is dark with a red gradient on the right side.

The Cybersecurity Illusion: The Emperor Has No Clothes

Ponemon Institute Research Report
Sponsored by AttackIQ

Independently Conducted by Ponemon Institute LLC
Published July 2019



The Importance of Understanding the Efficacy of Security Solutions

Presented by Ponemon Institute, July 2019

Part 1. Introduction

An overlooked security risk is not knowing if the technologies deployed are working as promised. In other words, are they protecting the organization from data breaches and cyberattacks? Does the organization have gaps in its IT security infrastructure that allow attackers to penetrate their defenses?

In this report, efficacy refers to both the effectiveness and efficiency of a security strategy, technologies and controls. Following are problems caused by not determining efficacy:

- Uncertainty if attacks against the network are being stopped
- Inability to determine if the organization is getting full value from its technology investments
- Inability to provide senior leadership and the board of directors with a clear picture of the organization's security posture

Sponsored by AttackIQ, Ponemon Institute surveyed 577 IT and IT security practitioners in the United States who are knowledgeable about their organization's IT security strategy and tactics. They are also involved in evaluating or responsible for their organizations' technology investments.

Fifty-three percent of these experts admit they are in the dark about how well the technologies they have are meeting expectations and protecting the network. As a result, only 39 percent of respondents say they are getting full value from their security investments. Further, only 41 percent of respondents say their organizations are effective in determining gaps in coverage and closing those gaps.

Companies surveyed are spending an average of **\$18.4M** annually on cybersecurity, but data breaches still happen.

53%
of IT experts admit they don't know how well the cybersecurity tools they've deployed are working

Figure 1. Problems created by not determining the efficacy of security technologies (Strongly agree and Agree responses combined)



Following are insights from this research.

Most organizations are not using an automated solution to determine gaps in the IT infrastructure. Only 41 percent of respondents say the IT security team is effective in determining gaps in the IT security infrastructure and then closing those gaps. Only 24 percent of respondents say they use an automated solution. Twenty-nine percent of respondents say they use a combination of automated and manual.

Data breaches are likely because of gaps in the IT security infrastructure. Respondents were asked to rate the certainty of reducing the likelihood of a data breach because of the ability of their IT security staff, processes and security solutions on a scale of 1 = no certainty to 10 = high certainty. In both cases, less than half are confident that data breaches can be stopped with their current investments in technology and staff. Sixty-three percent of respondents say they have observed a security control reporting it blocked an attack when it did not.

Companies are spending an average of \$18.4 million annually on cybersecurity, but data breaches still happen because of skilled attackers, complex security infrastructure, and a lack of in-house expertise. The primary reason data breaches still occur is due to the skill of the attackers, according to 70 percent of respondents. This is followed by the complexity (66 percent of respondents) which can be attributed in part because the companies represented in this research have an average of 47 separate security solutions and technologies deployed in their organizations. Sixty-five percent of respondents say the dynamically changing attack surface and lack of adequate security staff with the necessary skills can lead to a data breach.

Staffing and organizational silos prevent the IT security team from responding to a cyberattack. According to the findings, only 25 percent of respondents say the IT security team is able to respond to security incidents within one day. The primary obstacles are created by a shortage of in-house expertise and the lack of timely response and engagement with other departments and functions.

Data breaches still happen because of a lack of visibility into the IT security infrastructure. As discussed previously, 56 percent of respondents say a reason data breaches still occur is because of a lack of visibility into the operations of their security program. While respondents are most confident in having visibility into the organization's applications, endpoints and servers, only 35 percent of respondents say they have a high degree of confidence in visibility into their cloud and IoT devices.

Penetration testing is effective in uncovering security gaps. Fifty-seven percent of respondents say their IT security teams conduct penetration testing. However, almost one-third of respondents (31 percent) say they have no set schedule for penetration testing. Sixty-five percent of respondents say their penetration testing is very effective or effective in uncovering security gaps. Despite the effectiveness in uncovering security gaps, only 17 percent of respondents say they confirm security gaps every time they are found through penetration testing.

IT security teams believe the continuous security validation (CSV) platform effective in finding security gaps and reducing data breach risks. Of the 48 percent of respondents who say their organizations deploy a CSV platform, 68 percent say it is effective in finding security gaps. The ability to identify vulnerabilities quickly is the most important feature in a CSV platform followed by actionable intelligence.

Most organizations will increase their IT security budget in the next 12 months. On average, organizations represented in this study will spend \$18.4 million in 2019. Fifty-eight percent of respondents say their organizations will be increasing their IT security budget by an average of 14 percent. According to respondents, more money will be allocated to improving, managing and maintaining threat detection tools. Incident response plans will receive more funding.

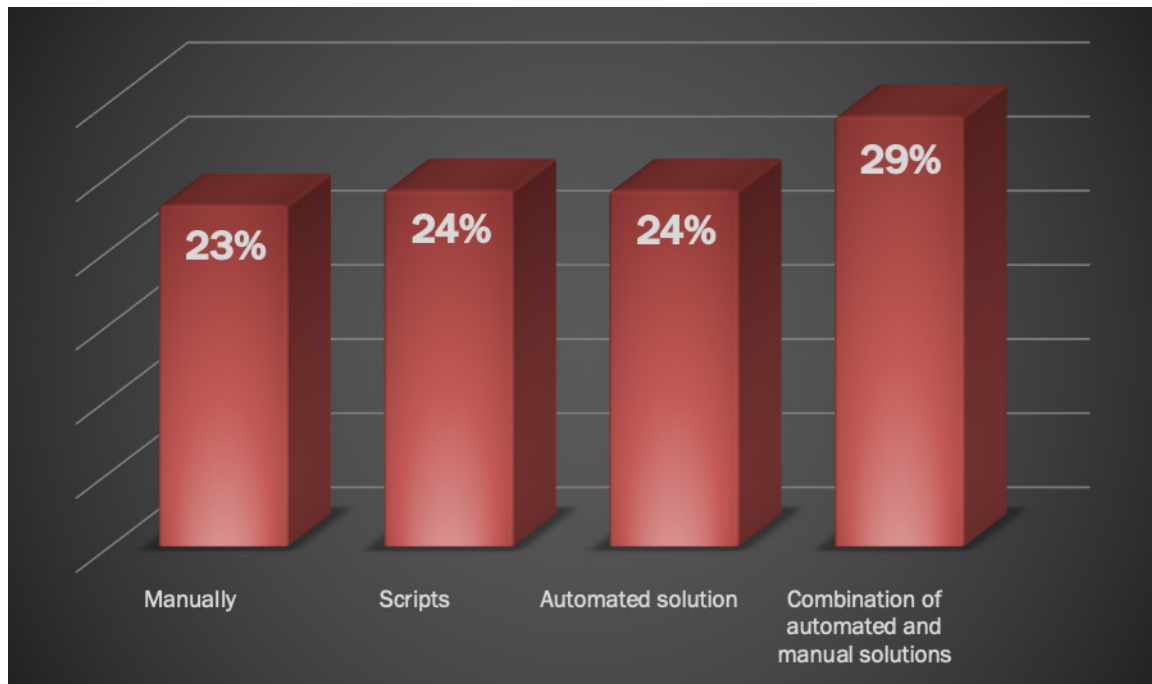
Part 2. Key Findings

In this section, we provide a deeper analysis of the key findings. The complete audited findings are presented in the Appendix of this report. Topics in this research include the following:

- Organizations are at risk because of gaps in the IT security infrastructure
- The efficacy of penetration testing and use of a CSV platform
- Budgets and investments
- Organizations are at risk because of gaps in the IT security infrastructure

Most organizations are not using an automated solution to determine gaps in the IT infrastructure. Only 41 percent of respondents say the IT security team is effective in determining gaps in the IT security infrastructure and then closing those gaps. As shown in Figure 6, only 24 percent of respondents say they use an automated solution. Twenty-nine percent of respondents say they use a combination of automated and manual.

Figure 2. How do you measure gaps in your organization’s IT security infrastructure?

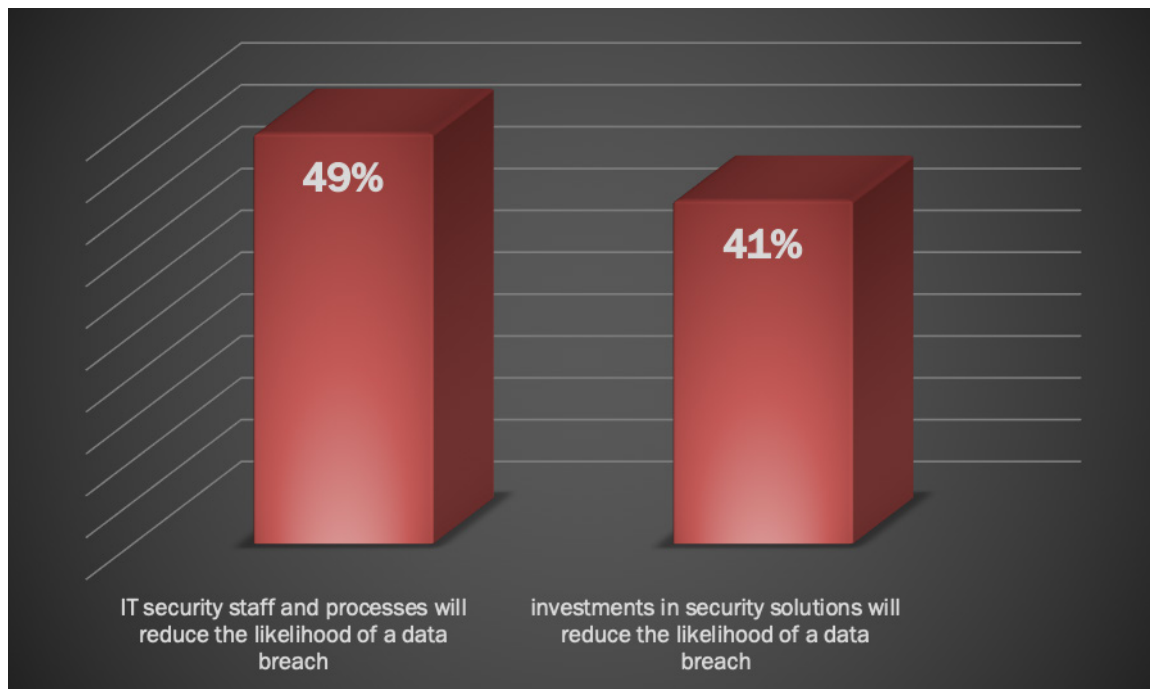


29%

Use a combination of automated and manual solutions to measure gaps in their security

Data breaches are likely because of gaps in the IT security infrastructure. Respondents were asked to rate the certainty of reducing the likelihood of a data breach because of the ability of their IT security staff, processes and security solutions on a scale of 1 = no certainty to 10 = high certainty. In both cases, less than half are confident that data breaches can be stopped with their current investments in technology and staff, as shown in Figure 3.

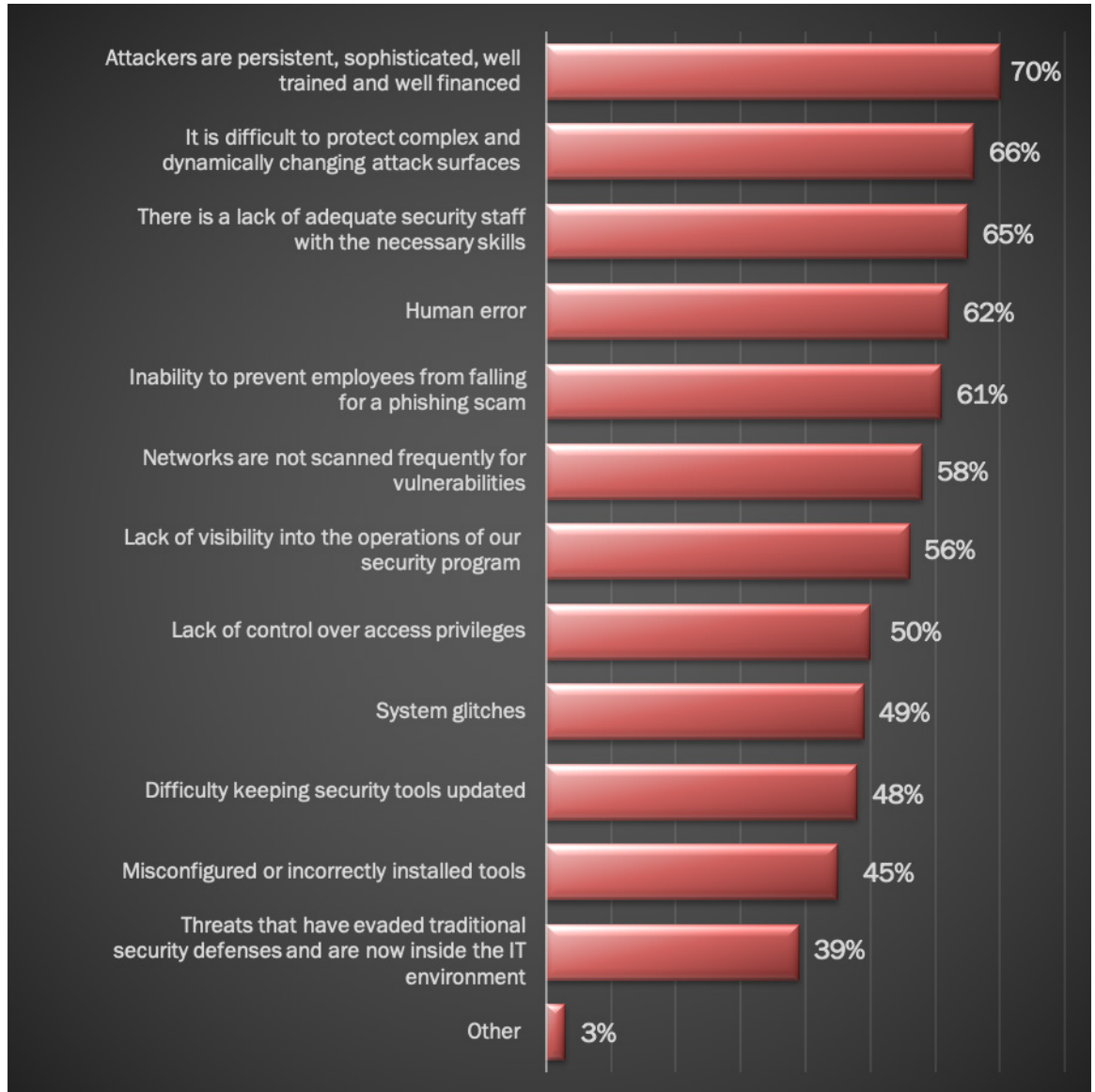
Figure 3. Certainty that investments, staff and processes will reduce the likelihood of a data breach (On a scale from 1 = no certainty to 10 = high certainty, 7+ responses presented)



Data breaches are likely because of gaps in the IT security infrastructure.

Companies are spending an average of \$18.4 million annually on cybersecurity, but data breaches still happen. Figure 4 presents a long list of reasons why organizations continue to have data breaches. The primary reason is the skill of the attackers, according to 70 percent of respondents. This is followed by the complexity and dynamically changing attack surface and lack of adequate security staff with the necessary skills, 66 percent and 65 percent of respondents, respectively.

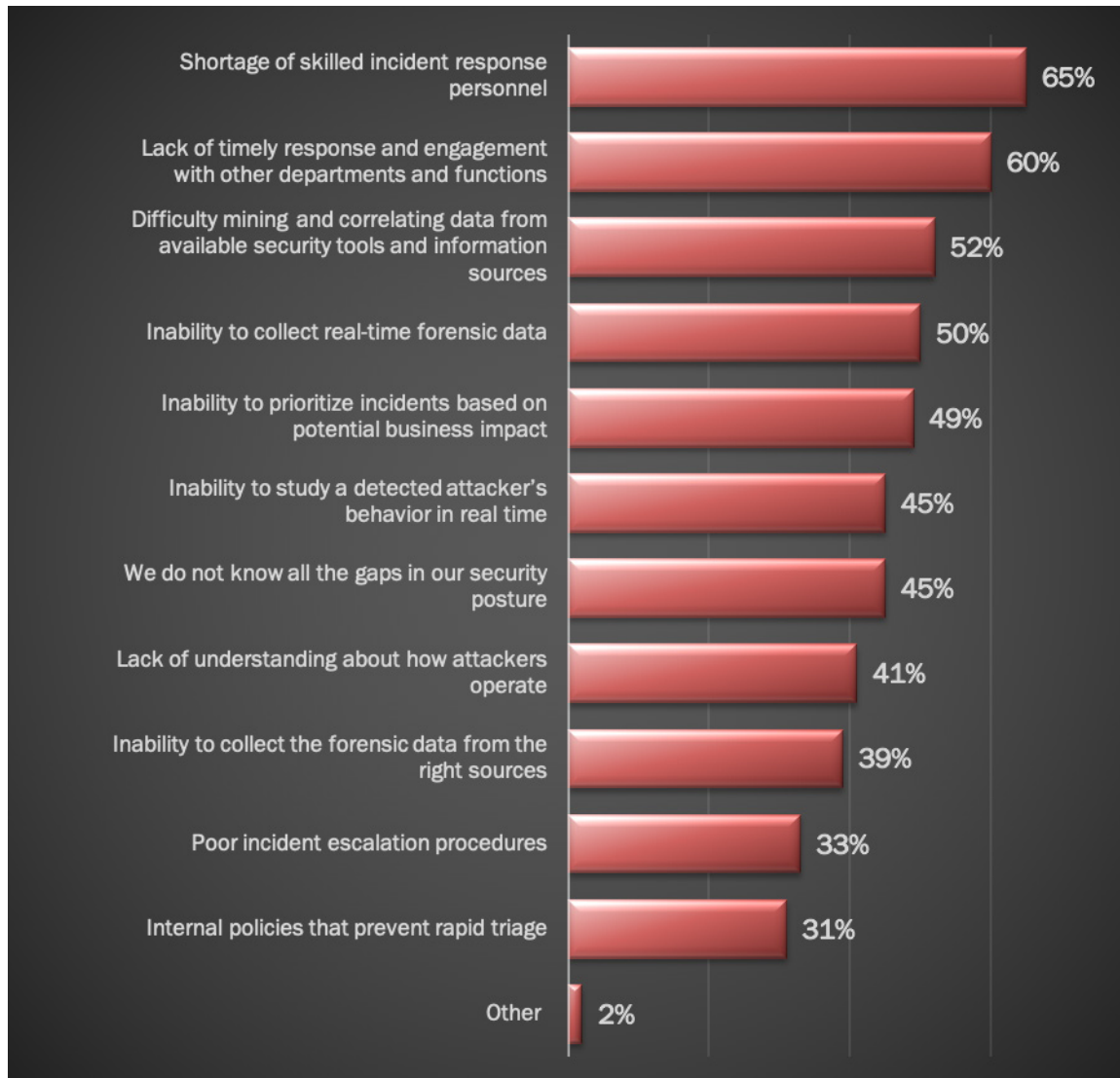
Figure 4. Why data breaches still happen despite investments in cybersecurity technologies
 (More than one response permitted)



only
25%
 of respondents say the IT security team is able to respond to security incidents within one day.

Staffing and organizational silos prevent the IT security team from responding to a cyberattack. According to the findings, only 25 percent of respondents say the IT security team is able to respond to security incidents within one day. The primary obstacles are created by a shortage of in-house expertise and the lack of timely response and engagement with other departments and functions, as shown in Figure 5.

Figure 5. Obstacles to the ability to effectively respond to cyberattacks (More than one response permitted)

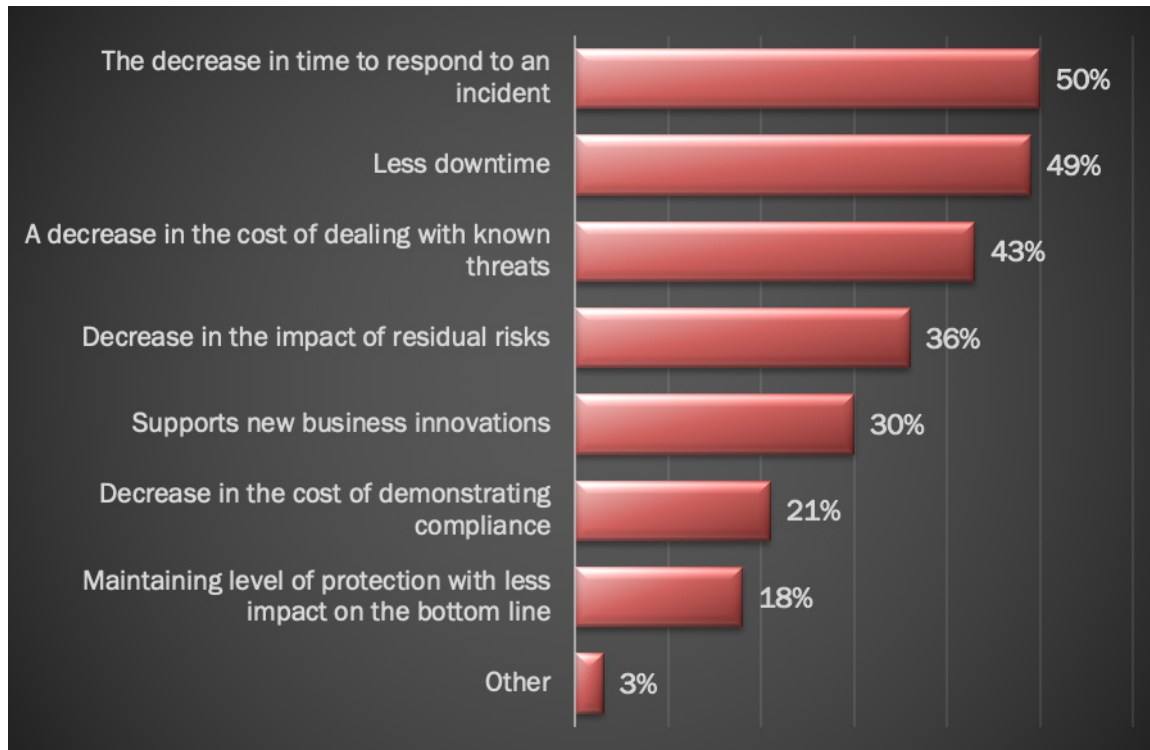


50%
of respondents are trying to determine the efficacy of their organization's security program

One reason for not having an effective and efficient security program is the inability to respond quickly to a cyberattack. According to Figure 6, 50 percent of respondents are trying to determine the efficacy of their organization's security program, based on the decrease in time to respond to an incident. Only 36 percent of respondents say they measure the decrease in the impact of residual risks.

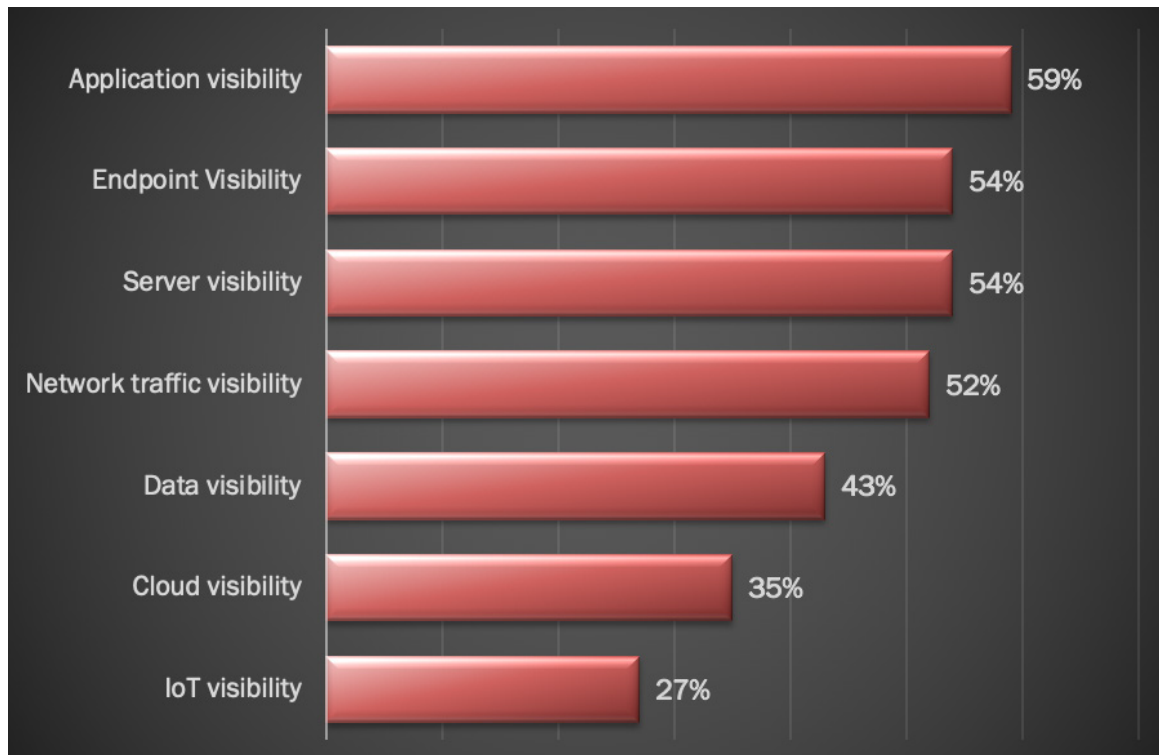
63%
of respondents
said they have
observed a
security control
reporting it
blocked an
attack when it
actually failed to
do so

Figure 6. How do you measure the efficacy of your organization’s security program? (More than one response permitted)



Data breaches still happen because of a lack of visibility into the IT security infrastructure. As discussed previously, 56 percent of respondents say a reason data breaches still occur is because of a lack of visibility into the operations of their security program. Respondents were asked to rate their organizations’ confidence in having visibility into various areas of their IT security infrastructure on a scale of 1 = no confidence to 10 = high confidence. Figure 7 presents the high confidence responses. The most confidence is the visibility into the organization’s applications, endpoints and servers. Only 35 percent of respondents say they have a high degree of confidence in visibility into their cloud and IoT devices.

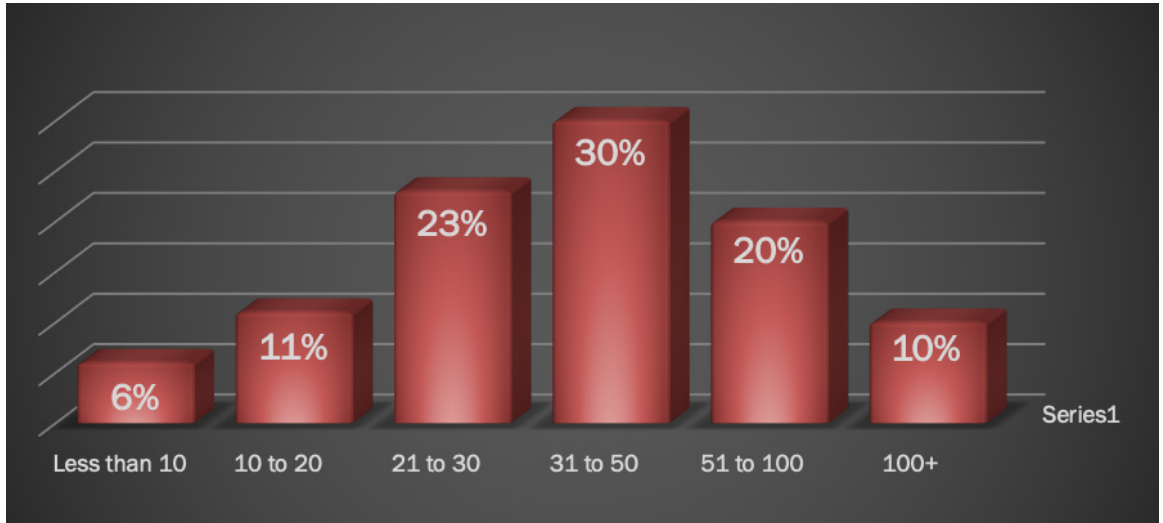
Figure 7. Confidence in having visibility into the IT security infrastructure (On a scale from 1 = low confidence to 10 = high confidence, 7+ responses presented)



Complexity can prevent companies from preventing data breaches.

Complexity can be the enemy of security. According to the findings, complexity can prevent companies from preventing data breaches. As shown in Figure 8, an average of almost 47 separate security solutions and technologies are deployed in respondents' organizations.

Figure 8. How many separate security solutions and technologies does your organization deploy today? (Extrapolated value = 46.7)

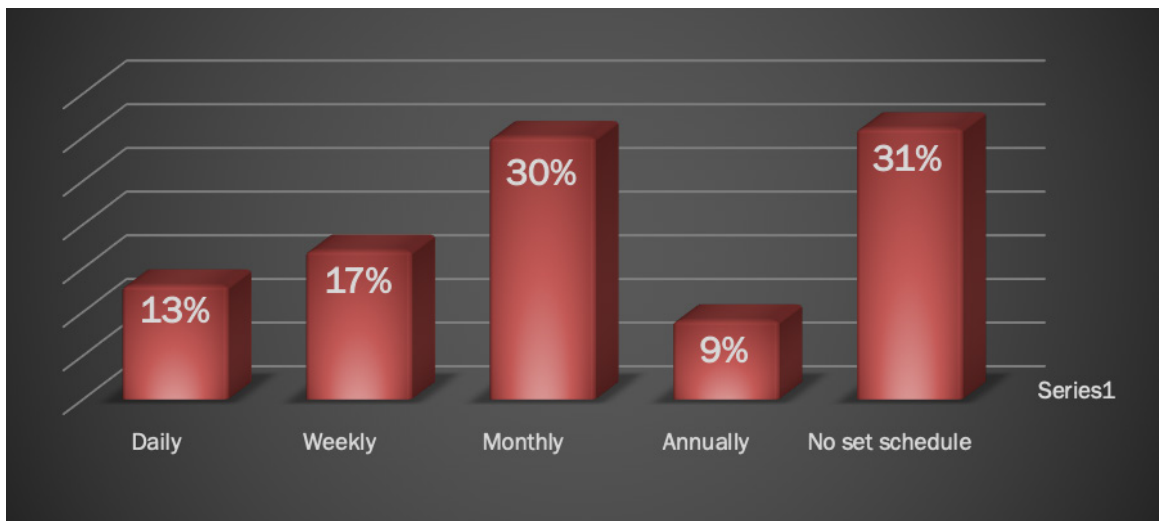


An average of almost **47** separate security solutions and technologies are deployed in respondents' organizations.

The Efficacy of Penetration Testing and use of a CSV Platform

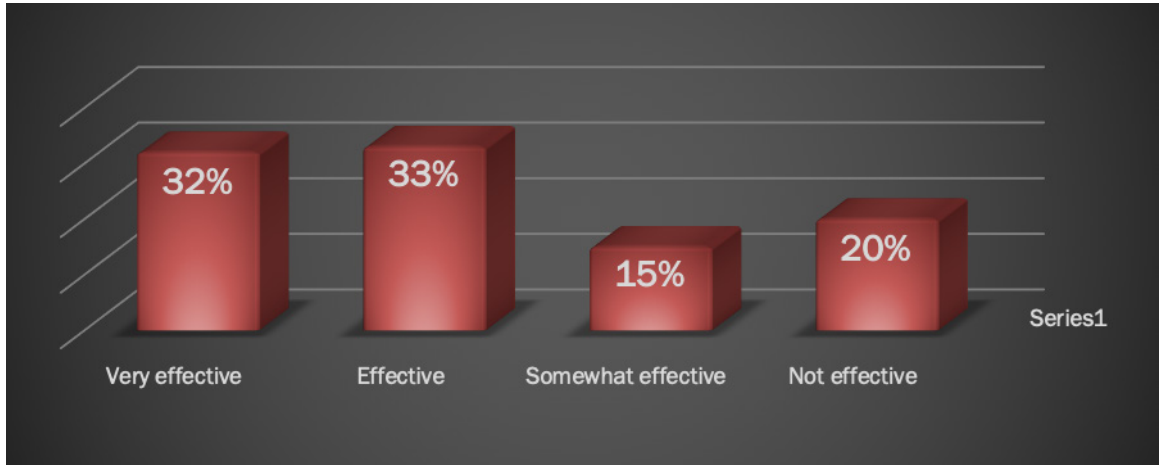
Penetration testing is effective in uncovering security gaps. Fifty-seven percent of respondents say their IT security teams conduct penetration testing. However, as shown in Figure 9, almost one-third of respondents (31 percent) say they have no set schedule for penetration testing.

Figure 9. How often does your organization conduct penetration testing?



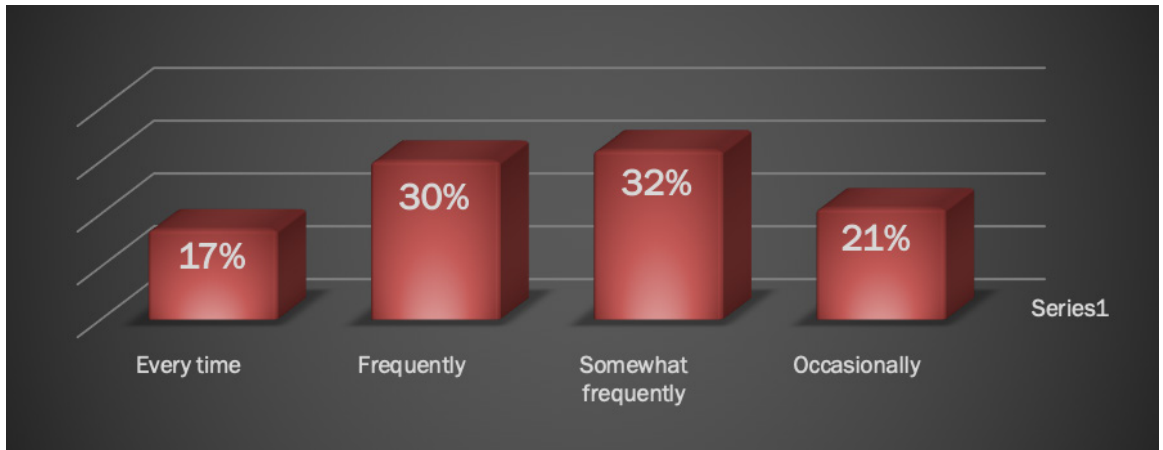
As shown in Figure 10, 65 percent of respondents say their penetration testing is very effective or effective in uncovering security gaps.

Figure 10. How effective is penetration testing in uncovering security gaps?



Despite the effectiveness in uncovering security gaps, only 17 percent of respondents say they confirm security gaps every time they are found. As shown in Figure 11, 53 percent say they confirm only somewhat frequently or occasionally.

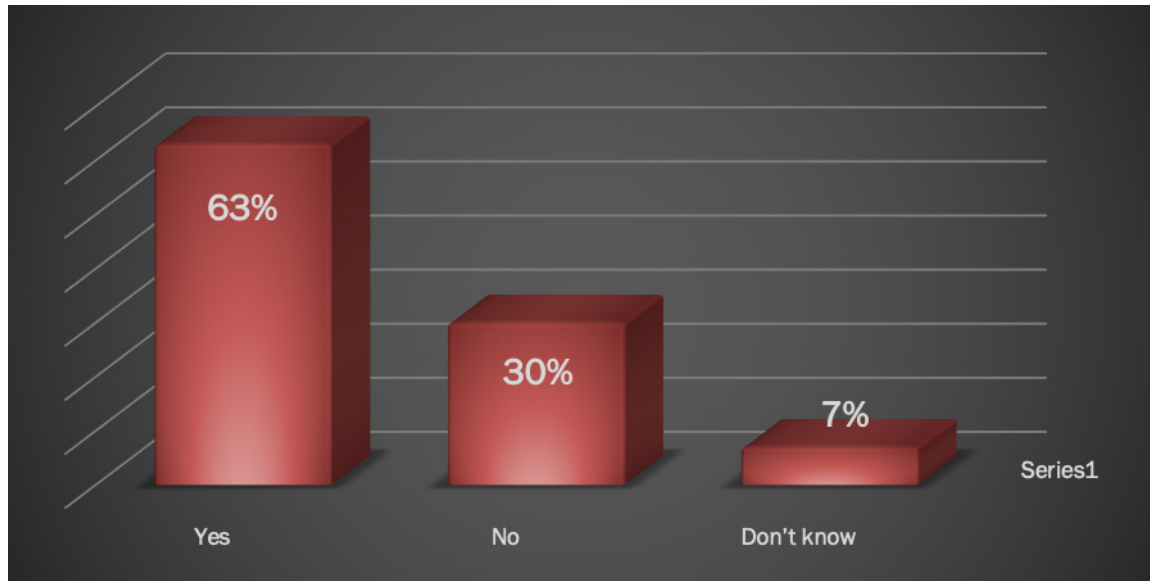
Figure 11. How often do you confirm security gaps found by penetration testing?



As discussed previously, IT security teams are uncertain if technologies are working as they should. As shown in Figure 12, 63 percent of respondents say they have observed a security control reporting it blocked an attack when it did not.

65%
of
respondents
found that
**penetration
testing**
was
very effective
or effective.

Figure 12. Have you ever observed a security control reporting it blocked an attack when it did not?

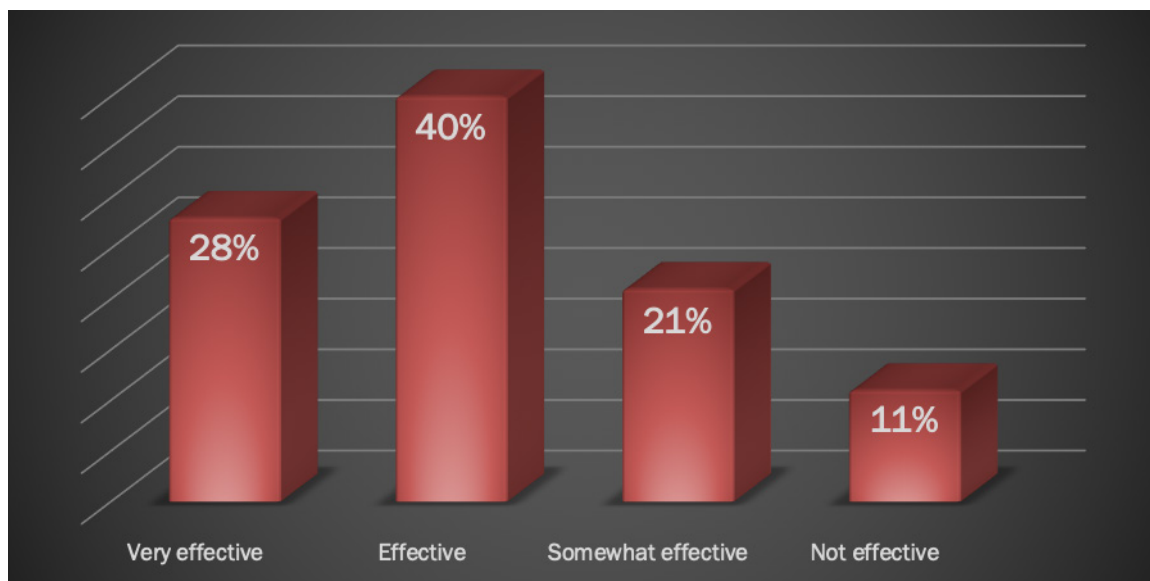


63%
of
respondents
observed
a security
control
reporting it
**blocked an
attack when it
did not.**

In this section, we discuss the CSV platform that enables organizations to test the efficacy of their security solution and determine how well security solutions are performing. It identifies gaps in coverage and misconfiguration to prioritize remediation efforts. Almost half of respondents (48 percent) deploy a CSV platform using attack simulations.

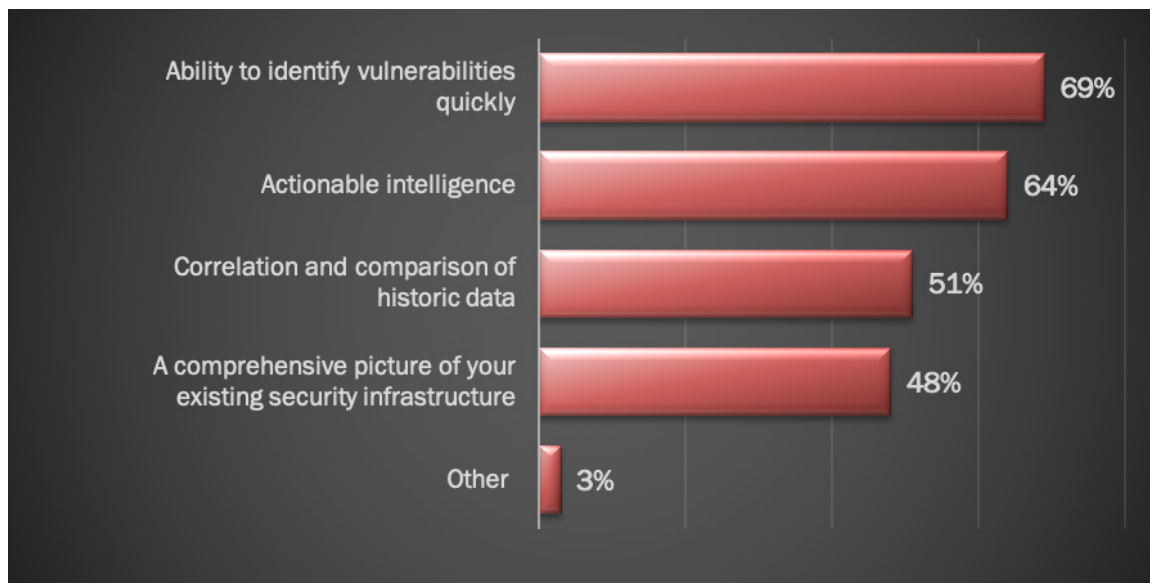
IT security teams find the CSV platform effective in finding security gaps and reducing data breach risks. Of the 48 percent of respondents who say their organizations deploy a CSV platform, 68 percent say it is effective in finding security gaps.

Figure 13. How effective is CSV in finding security gaps and mitigating the risk of data breach?



The ability to identify vulnerabilities quickly is the most important feature in a CSV platform followed by actionable intelligence as shown in Figure 14.

Figure 14. What features are important in a CSV platform?



Budgets and Investments

Most organizations will increase their IT security budget in the next 12 months. On average, organizations represented in this study will spend \$18.4 million in 2019. Fifty-eight percent of respondents say their organizations will be increasing their IT security budget by an average of 14 percent.

Respondents were asked to allocate 100 points to four investment categories. As shown in Table 1, more money will be allocated to improving, managing and maintaining threat detection tools. Incident response plans will receive more funding.

58% of companies
 will be increasing their IT security budget by an average of
14% in the next year

Only
39%
of
respondents
say they are
getting full
value from
their security
investments

Table 1. Where is your organization investing today and 12 months from now?

Where is your organization investing	Investment categories today	Investment categories in the next 12 months
Security program management (e.g. assessment, design, planning, project management and reporting)	36	30
Improvement, management and maintenance of preventive controls	21	18
Improvement, management and maintenance of threat detection tools	23	28
Planning, rehearsal and execution of incident response and remediation activities	20	24
Total points allocated	100	100

Part 3. Methods

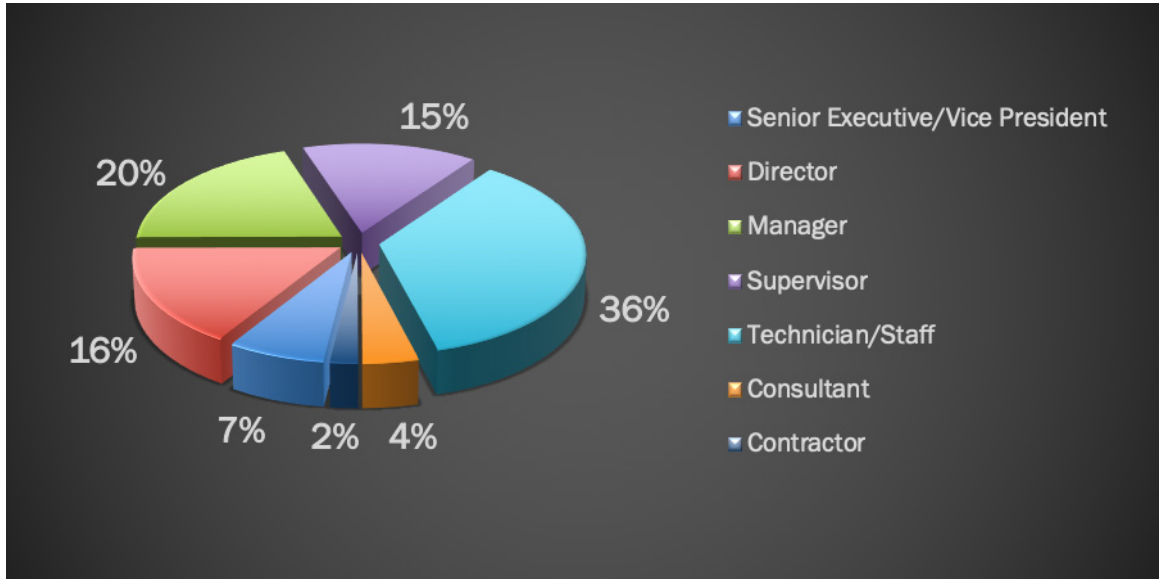
A sampling frame of 15,898 IT or IT security practitioners located in the United States and who are knowledgeable about their organization’s IT security strategy and tactics were selected as participants in the research. Table 2 shows that there were 631 total returned surveys. Screening and reliability checks led to the removal of 54 surveys. Our final sample consisted of 577 surveys, a 3.6 percent response.

Table 2. Sample Response Analysis

Sample response	Frequency	Percentage
Sampling frame	15,898	100.0%
Total returns	631	4.0%
Rejected or screened surveys	54	0.3%
Final sample	577	3.6%

Pie Chart 1 reports the respondents' organizational level within participating organizations. By design, more than half of respondents (58 percent) are at or above the supervisory levels.

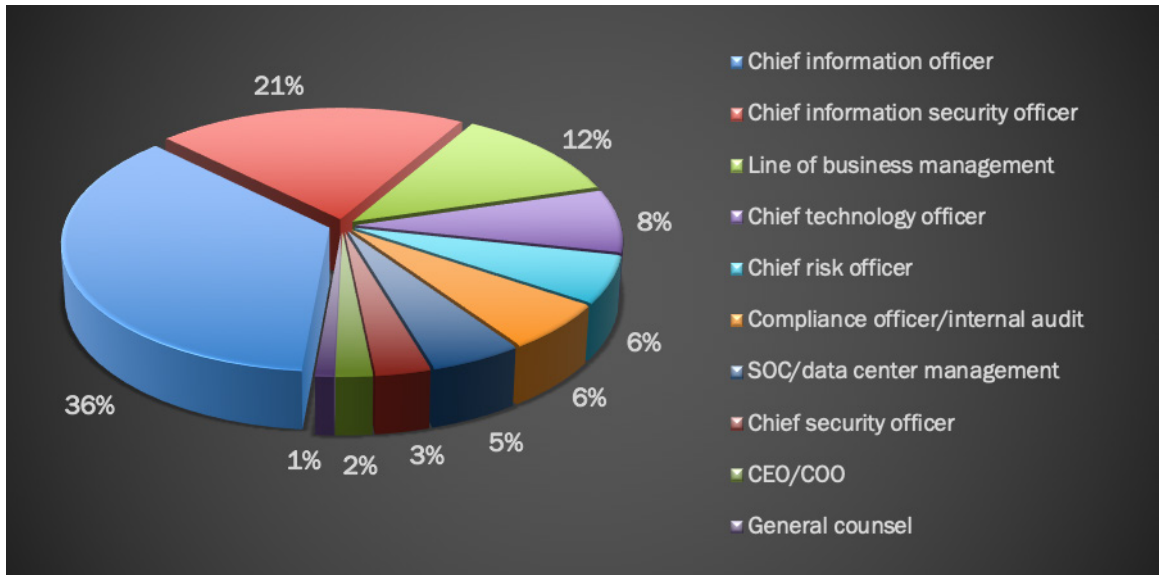
Pie Chart 1. Position level within the organization



58%
of
respondents
are at or
above the
supervisory
levels.

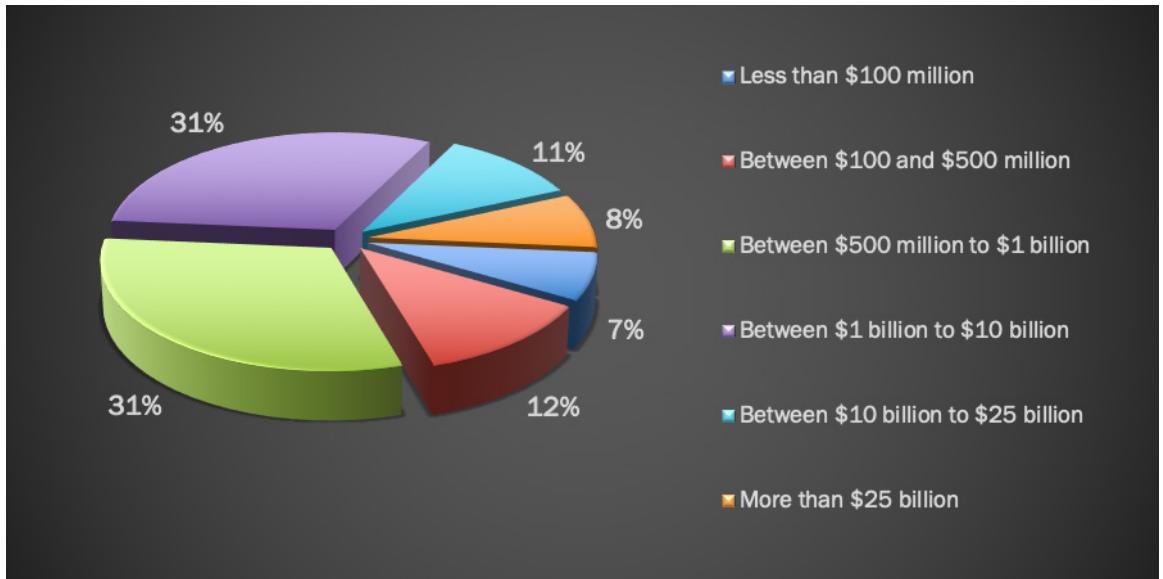
As shown in Pie Chart 2, 36 percent of respondents report to the chief information officer, 21 percent of respondents report to the chief information security officer, 12 percent of respondents report to line of business management and 8 percent of respondents report to the chief technology officer.

Pie Chart 2. Respondents reporting channel or chain of command



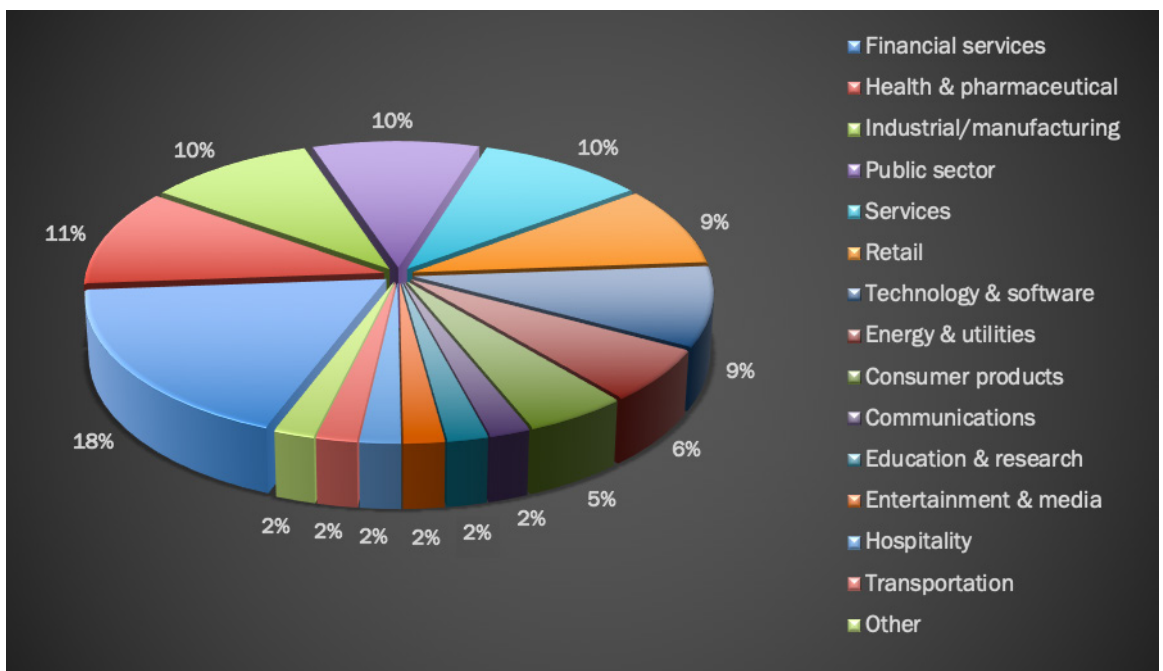
As Pie Chart 3 illustrates, 50 percent of the respondents report their global revenue to be greater than \$1 billion.

Pie Chart 3. Global revenue of the organization



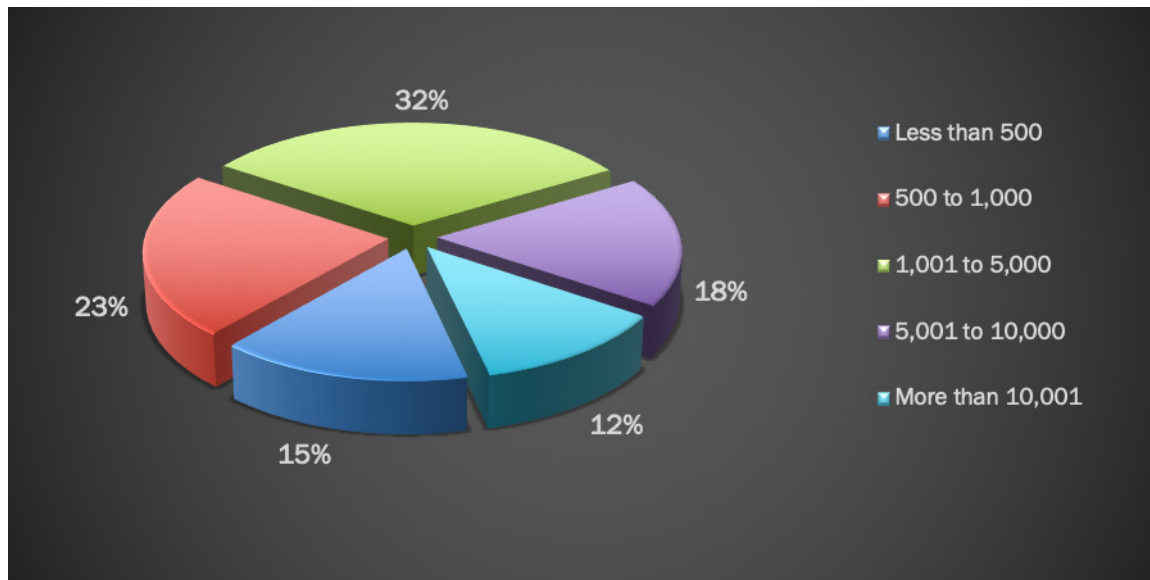
50%
of the
respondents
report their
global
revenue to be
greater than
\$1B

Pie Chart 4 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest industry classification, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceuticals (11 percent of respondents), industrial/manufacturing, public sector and service sector, each at 10 percent of respondents respectively.



According to Pie Chart 5, more than half of the respondents (62 percent) are from organizations with a headcount of over 1,000 employees.

Pie Chart 5. The number of employees within the organization

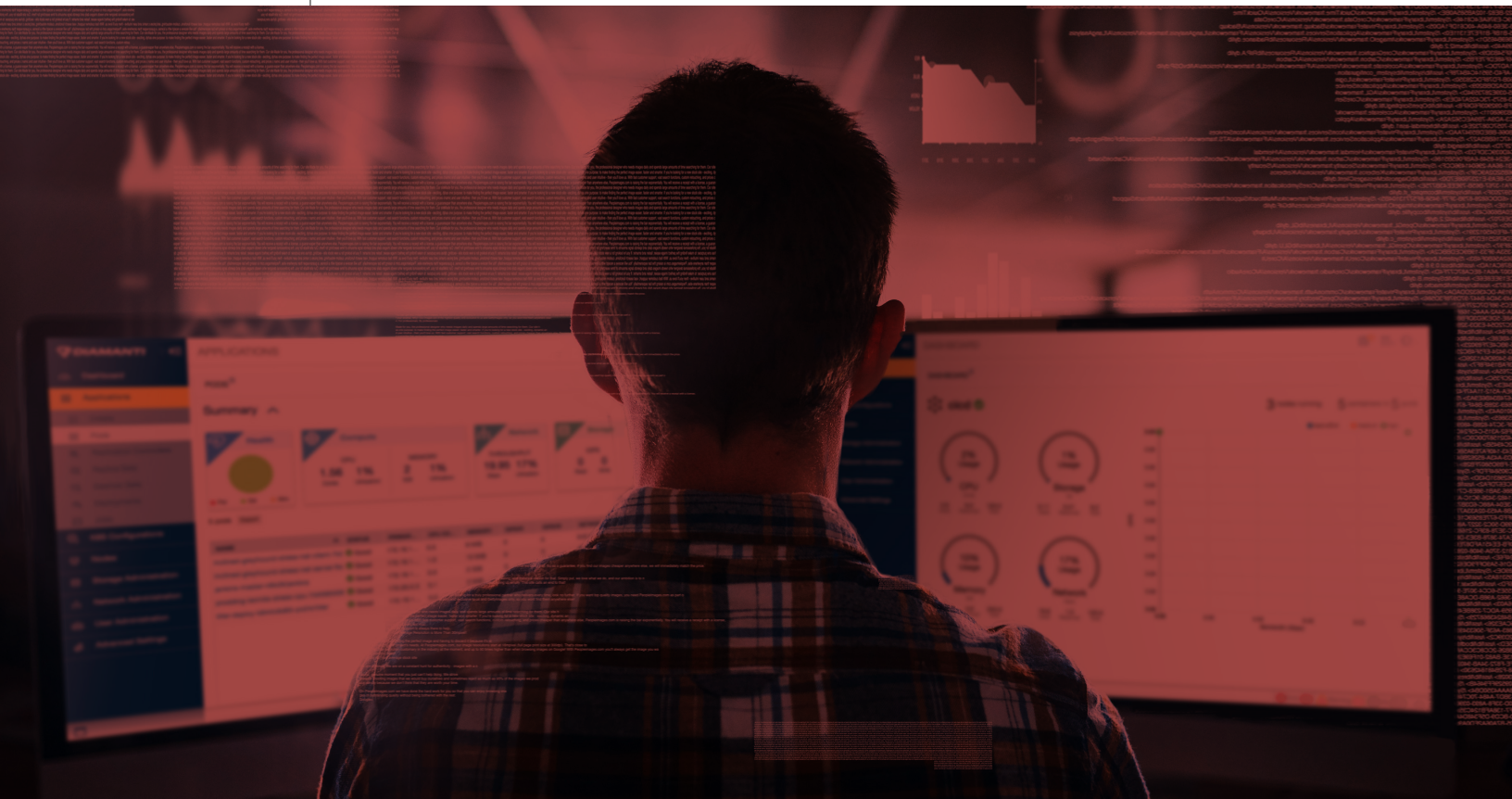


62%
of
respondents
are from
organizations
with a
headcount
of over 1,000
employees.

Part 4. Caveats to this study

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 a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners, 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 individuals who are knowledgeable about their organization's IT security strategy and tactics. Because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **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, the possibility remains 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 April 8 to 22, 2019.

Part 1. Survey

Survey Response	Frequency	Percentage
Total sampling frame	15,898	100.0%
Total returns	631	4.0%
Rejected surveys	54	0.3%
Final sample	577	3.6%

S1. What best describes your involvement in IT security investments within your organization?	Percentage
None (stop)	0%
Responsible for overall solution/purchase	45%
Responsible for administration/management	41%
Involved in evaluating solutions	67%
Total	153%

S2. What best describes your role within your organization's IT or IT security department?	Percentage
IT leadership (CIO)	9%
Security leadership (CSO/CISO)	8%
IT management	13%
IT operations	14%
Security management	9%
Security monitoring and response	11%
Data administration	11%
Compliance administration	10%
Applications development	12%
Data Protection Office	3%
I'm not involved in my organization's IT or IT security function (stop)	0%
Total	100%

S3. How knowledgeable are you about your organization's IT security strategy and tactics?	Percentage
Very knowledgeable	40%
Knowledgeable	33%
Somewhat knowledgeable	27%
Slightly knowledgeable (stop)	0%
No knowledge (stop)	0%
Total	100%

Part 2. Attributions

Q1. Please rate each one of the following statements using the agreement scale provided below each item. Strongly agree and agree responses combined.	Percentage
Q1a. In my experience, our IT security infrastructure has gaps in coverage that allow attackers to penetrate its defenses.	56%
Q1b. Our IT security team is effective in determining gaps in coverage and closing those gaps.	41%
Q1c. My organization is getting the full value from our current security investments.	39%
Q1d. Our IT security leadership is not certain if the technologies deployed are working as promised and protecting the network.	53%
Q1e. Our organization has a complex suite of security solutions that make it difficult to determine if our security strategy is effective.	60%
Q1f. Our IT security leadership needs better monitoring tools that will improve the ability to communicate the effectiveness of our security infrastructure, including potential gaps, to our C-suite and board of directors.	63%
Q1g. Our organization’s security approach is reactive and incident driven.	69%
Q1h. Our IT security team is able to respond to security incidents within one day.	25%
Q1i. Our IT security team is able to assess the effectiveness of our organization’s security practices, technologies and controls.	40%

Q2. What are the primary barriers to maturing your security program? Please select all that apply.	Percentage
Too many alerts to address	63%
Security staff and skills shortages	68%
Inability to identify and repair vulnerabilities quickly	59%
Too many false positives	51%
Security solutions can't keep up with exponentially increasing amounts of data	57%
Hard to protect expanding and blurring IT perimeter with IoT, BYOD, mobile and cloud	60%
Siloed security solutions	47%
Inability of traditional perimeter-based security solutions to detect and stop advanced targeted attacks	50%
Lack of visibility into every user and device connected to the IT infrastructure	64%
Lack of visibility into what every user and device is doing while connected to the IT infrastructure	62%
Complexity and the inability to integrate security solutions	65%
Other	2%
Total	648%

Q3. Despite all the cybersecurity investments made by companies, why are breaches still happening? Please select all that apply.	Percentage
It is difficult to protect complex and dynamically changing attack surfaces (mobile, byod, cloud, etc.)	66%
Difficulty keeping security tools updated	48%
Misconfigured or incorrectly installed tools	45%
Networks are not scanned frequently for vulnerabilities	58%
Lack of control over access privileges	50%
Inability to prevent employees from falling for a phishing scam	61%
There is a lack of adequate security staff with the necessary skills	65%
Attackers are persistent, sophisticated, well trained and well financed	70%
Lack of visibility into the operations of our security program	56%
Threats that have evaded traditional security defenses and are now inside the IT environment	39%
Human error	62%
System glitches	49%
Other	3%
Total	672%

Q4. Which of the following are obstacles to your organization's ability to effectively respond to cyberattacks? Please select all that apply	Percentage
Poor incident escalation procedures	33%
We do not know all the gaps in our security posture	45%
Inability to prioritize incidents based on potential business impact	49%
Lack of understanding about how attackers operate	41%
Shortage of skilled incident response personnel	65%
Inability to collect the forensic data from the right sources	39%
Inability to collect real-time forensic data	50%
Inability to study a detected attacker's behavior in real time	45%
Difficulty mining and correlating data from available security tools and information sources	52%
Lack of timely response and engagement with other departments and functions	60%
Internal policies that prevent rapid triage	31%
Other	2%
Total	512%

Part 3. Testing and validating the efficacy of the organization’s security posture

Q5. Who within your organization is most responsible for validating the efficacy of its security strategy, technologies and controls?	Percentage
Chief information officer (CIO)	30%
Chief technology officer (CTO)	8%
Chief information security officer (CISO)	21%
Chief risk officer (CRO)	7%
Chief security officer (CSO)	3%
Line of business leadership	12%
End-users of IoT devices	5%
Data Protection Officer (DPO)	3%
No one function has overall responsibility	11%
Other	0%
Total	100%

Q6. Approximately, how many separate security solutions and technologies does your organization deploy today?	Percentage
Less than 10	6%
10 to 20	11%
21 to 30	23%
31 to 50	30%
51 to 100	20%
100+	10%
Total	100%
Extrapolate value	46.7

Q7a. Does your IT security team attempt to quantify and track the company's IT security posture?	Percentage
Yes, we have a fairly mature measurement and metrics program	24%
Yes, we have a partial program in place	30%
No, we do not quantify and track the company's IT security posture	40%
Don't know	5%
Other (please specify)	1%
Total	100%

Q7b. If yes, do you report these metrics to the board of directors and CEO?	Percentage
Yes	39%
No	61%
Total	100%

Q7c. If no, why don't you report these metrics and measurements?	Percentage
The information is too technical to communicate effectively	35%
The information does not provide an accurate and comprehensive view of the threats facing the organization	38%
The information does not reveal the gaps in our security posture	26%
Other	1%
Total	100%

Q8. How often does your organization's IT security leadership report to the board?	Percentage
Monthly	5%
Quarterly	12%
Annually	20%
On an as needed basis	9%
Only following a security incident	14%
The IT security leadership does not report to the board	40%
Total	100%

Q9. What describes the involvement of the board and CEO in your organization's IT security program?	Percentage
Determines and/or approves the acceptable level of cyber risk for the organization	28%
Reviews the IT security budget	19%
Has a cybersecurity committee	34%
Reviews cyber insurance	19%
Reviews regulatory compliance	45%
Reviews vendor/supply chain requirements	37%
Requires cybersecurity due diligence in a merger and acquisition process	21%
Requires an outside cyber-risk assessment and evaluation of the overall culture of cybersecurity	53%
None of the above	15%
Other	3%
Total	274%

Q10. How do you measure the efficiency and effectiveness of your organization's security program?	Percentage
A decrease in the cost of dealing with known threats	43%
Decrease in the impact of residual risks	36%
Decrease in the cost of demonstrating compliance	21%
Maintaining level of protection with less impact on the bottom line	18%
The decrease in time to respond to an incident	50%
Less downtime	49%
Supports new business innovations	30%
Other	3%
Total	250%

Q11. Please rate your level of certainty that your organization's investments in security solutions will reduce the likelihood of a data breach from 1 = no certainty to 10 = high certainty.	Percentage
1 or 2	13%
3 or 4	24%
5 or 6	22%
7 or 8	23%
9 or 10	18%
Total	100%
Extrapolated value	5.68

Q12. Please rate your level of certainty that your organization's IT security staff and processes will reduce the likelihood of a data breach from 1 = no certainty to 10 = high certainty.	Percentage
1 or 2	9%
3 or 4	18%
5 or 6	24%
7 or 8	25%
9 or 10	24%
Total	100%
Extrapolated value	6.24

Q13. How do you measure gaps in your organization's IT security infrastructure?	Percentage
Manually	23%
Scripts	24%
Automated solution	24%
Combination of automated and manual solutions	29%
Total	100%

Q14. Has a security product update ever affected the efficacy of your organization's security posture?	Percentage
Yes	60%
No	35%
Don't know	5%
Total	100%

Group Policy is a feature of the Microsoft Windows NT family of operating systems that controls the working environment of user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and users’ settings in an active directory environment. A set of Group Policy configurations is called a Group Policy Object (GPO). A version of Group Policy called Local Group Policy (LGPO or LocalGPO) allows Group Policy Object management without Active Directory on standalone computers.

Source: Wikipedia

Q15. Have you ever found that a group policy implementation does not actually provide the expected functionality?	Percentage
Yes	56%
No	40%
Don't know	4%
Total	100%

Q16. How often is your network access policy evaluated?	Percentage
Daily	5%
Weekly	20%
Monthly	45%
Annually	25%
Don't know	5%
Total	100%

Q17a. Do you conduct penetration testing?	Percentage
Yes	57%
No (please skip to Q23.)	43%
Total	100%

Q18. How often does your organization conduct penetration testing?	Percentage
Daily	13%
Weekly	17%
Monthly	30%
Annually	9%
No set schedule	31%
Total	100%

Q19. How effective is penetration testing in uncovering security gaps?	Percentage
Very effective	32%
Effective	33%
Somewhat effective	15%
Not effective	20%
Total	100%

Q20. Are the same protection failures uncovered from previous tests?	Percentage
Yes	46%
No	54%
Total	100%

Q22. If yes, how often do you confirm security gaps found by penetration test?	Percentage
Every time	17%
Frequently	30%
Somewhat frequently	32%
Occasionally	21%
Total	100%

Q23. Have you ever observed a security control reporting it blocked an attack when it did not?	Percentage
Yes	63%
No	30%
Don't know	7%
Total	100%

Q24. Does your organization monitor the use of Windows native tools used by attackers (WMI, PowerShell)?	Percentage
Yes	54%
No	43%
Don't know	3%
Total	100%

Q25. Do you have user specific restriction of departments that do not have use from advanced Windows native tools?	Percentage
Yes	36%
No	59%
Don't know	5%
Total	100%

A continuous security validation (CSV) platform enables organizations to test the efficacy of their security solution and determine how well security solutions are performing. It identifies gaps in coverage and misconfigurations to prioritize remediation efforts.

Q26a. Do you deploy a CSV platform using attack simulations?	Percentage
Yes	48%
No (please skip to Q27)	52%
Total	100%

Q26b. If yes, how effective is CSV in finding security gaps and mitigating the risk of a data breach?	Percentage
Very effective	28%
Effective	40%
Somewhat effective	21%
Not effective	11%
Total	100%

Q26c. If yes, what features are important in a CSV platform?	Percentage
A comprehensive picture of your existing security infrastructure	48%
Actionable intelligence	64%
Correlation and comparison of historic data	51%
Ability to identify vulnerabilities quickly	69%
Other	3%
Total	235%

Q27. Using the following 10-point scale, please rate your level of visibility to be able to detect attacks from 1 = low confidence to 10 = high confidence	
Q27a. Network traffic visibility	Percentage
1 or 2	8%
3 or 4	12%
5 or 6	28%
7 or 8	29%
9 or 10	23%
Total	100%
Extrapolated value	6.44

Q27b. Server visibility	Percentage
1 or 2	10%
3 or 4	14%
5 or 6	22%
7 or 8	24%
9 or 10	30%
Total	100%
Extrapolated value	6.50

Q27c. Application visibility	Percentage
1 or 2	9%
3 or 4	11%
5 or 6	21%
7 or 8	29%
9 or 10	30%
Total	100%
Extrapolated value	6.70

Q27d. Data visibility	Percentage
1 or 2	20%
3 or 4	14%
5 or 6	23%
7 or 8	23%
9 or 10	20%
Total	100%
Extrapolated value	5.68

Q27e. Cloud visibility	Percentage
1 or 2	15%
3 or 4	25%
5 or 6	25%
7 or 8	19%
9 or 10	16%
Total	100%
Extrapolated value	5.42

Q27f. IoT visibility	Percentage
1 or 2	23%
3 or 4	25%
5 or 6	25%
7 or 8	14%
9 or 10	13%
Total	100%
Extrapolated value	4.88

Q27g. Endpoint Visibility	Percentage
1 or 2	8%
3 or 4	15%
5 or 6	23%
7 or 8	25%
9 or 10	29%
Total	100%
Extrapolated value	6.54

Q28. The following table lists 19 enabling security technologies that may be deployed by your organization. For each item, indicate if you are confident in your organization's ability to determine the efficacy of the solution. Leave blank if your organization does not deploy a given technology. Very confident and confident responses combined.	Percentage
Access governance systems	45%
Advanced firewalls (e.g., NGFW and UTM)	39%
Big data analytics for cybersecurity	35%
Data loss prevention (DLP)	62%
Distributed deception technology	19%
Endpoint security solutions/EDR	40%
Forensic suite	37%
Honeypots	29%
Identity & access management (IAM)	52%
Incident response orchestration	38%
Intrusion detection systems (IDS)	52%
Intrusion prevention systems (IPS)	49%
Mobile threat prevention	30%
Netflow or network behavior analysis tools	40%
Security incident & event management (SIEM)	47%
Sinkholes	23%
User/employee behavior analytics (UEBA)	42%
VPN or secure gateways	25%
Web application firewalls (WAF)	50%

Part 4. Budgets and investments

Q29a. Will your organization's IT security budget increase in the next 12 months?	Percentage
Yes	58%
No	42%
Total	100%

Q29b. If yes, how much will your organization's IT security budget increase?	Percentage
Less than 10%	23%
10% to 15%	42%
16% to 20%	21%
21% to 30%	9%
31% to 40%	4%
41% to 50%	1%
55% to 75%	0%
76% to 100%	0%
Total	100%
Extrapolated value	14%

Q30. Approximately, what is the dollar range that best describes your organization's cybersecurity budget for 2019?	Percentage
< \$1 million	0%
\$1 to 5 million	4%
\$6 to \$10 million	9%
\$11 to \$15 million	31%
\$16 to \$20 million	22%
\$21 to \$25 million	25%
\$26 to \$50 million	7%
> \$50 million	2%
Total	100%
Extrapolated value	\$ 18.44

Q31a. Please allocate 100 percentage points to show how your IT security budget is allocated today.	Points
Security program management (e.g. assessment, design, planning, project management and reporting)	36
Improvement, management and maintenance of preventive controls	21
Improvement, management and maintenance of threat detection	23
Planning, rehearsal and execution of incident response and remediation activities	20
Total	100

Q31b. Please allocate 100 percentage points to show how your IT security budget will be allocated in the next 12 months.	Points
Security program management (e.g. assessment, design, planning, project management and reporting)	30
Improvement, management and maintenance of preventive controls	18
Improvement, management and maintenance of threat detection	28
Planning, rehearsal and execution of incident response and remediation activities	24
Total	100

Part 5. Your role and organization

D1. What organizational level best describes your current position?	Percentage
Senior Executive/Vice President	7%
Director	16%
Manager	20%
Supervisor	15%
Technician/Staff	36%
Consultant	4%
Contractor	2%
Other	0%
Total	100%

D2. Check the Primary Person you or your IT security leader reports to within the organization.	Percentage
CEO/COO	2%
Chief financial officer (CFO)	0%
General counsel	1%
Chief information officer (CIO)	36%
Chief technology officer (CTO)	8%
Chief risk officer (CRO)	6%
Chief information security officer (CISO)	21%
Compliance officer/internal audit	6%
Human resources VP	0%
Chief security officer (CSO)	3%
Line of business (LOB) management	12%
SOC/data center management	5%
Other	0%
Total	100%

D3. What range best defines the worldwide revenue of your organization?	Percentage
Less than \$100 million	7%
Between \$100 and \$500 million	12%
Between \$500 million to \$1 billion	31%
Between \$1 billion to \$10 billion	31%
Between \$10 billion to \$25 billion	11%
More than \$25 billion	8%
Total	100%

D4. What best describes your organization's primary industry classification?	Percentage
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	2%
Financial services	18%
Health & pharmaceutical	11%
Hospitality	2%
Industrial/manufacturing	10%
Public sector	10%
Retail	9%
Services	10%
Technology & software	9%
Transportation	2%
Total	100%

D5. How many employees are in your organization?	Percentage
Less than 500	15%
500 to 1,000	23%
1,001 to 5,000	32%
5,001 to 10,000	18%
More than 10,001	12%
Total	100%

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 organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

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

About AttackIQ

AttackIQ, a leader in the emerging market of continuous security validation, built the industry’s first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ™ supports the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying defenses work as expected. AttackIQ’s platform is trusted by leading companies around the world. For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.