Ponemon INSTITUTE

The Economic Value of Prevention in the Cybersecurity Lifecycle

Sponsored by: Deep Instinct

deepinstinct BEFORE YOU KNOW IT

Independently conducted by Ponemon Institute LLC

Publication Date: April 2020

Ponemon INSTITUTE

The Economic Value of Prevention in the Cybersecurity Lifecycle

Ponemon Institute, March 2020

Part 1. Introduction

Ponemon Institute is pleased to present the findings of *The Economic Value of Prevention in the Cybersecurity Lifecycle*, sponsored by Deep Instinct. The cybersecurity lifecycle is the sequence of activities an organization experiences when responding to an attack. The five high-level phases are prevention, detection, containment, recovery and remediation.

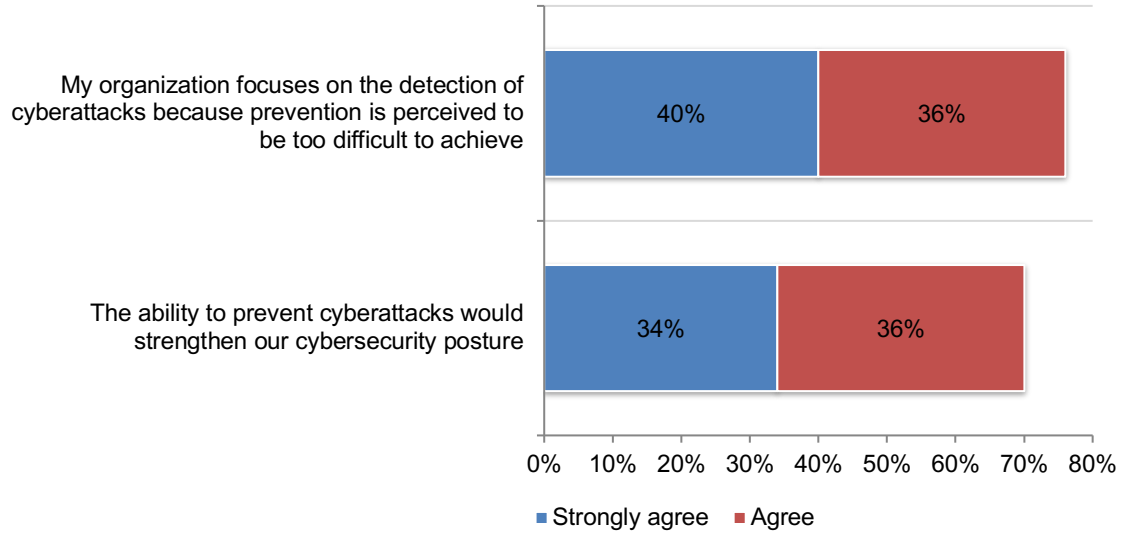
We surveyed 634 IT and IT security practitioners who are knowledgeable about their organizations' cybersecurity technologies and processes. Within their organizations, most of these respondents are responsible for maintaining and implementing security technologies, conducting assessments, leading security teams and testing controls.

The key takeaway from this research is that when attacks are prevented from entering and causing any damage, organizations can save resources, costs, damages, time and reputation.

To determine the **economic value of prevention**, respondents were first asked to estimate the cost of one of the following five types of attacks: phishing, zero-day, spyware, nation-state and ransomware. They were then asked to estimate what percentage of the cost is spent on each phase of the cybersecurity lifecycle, including prevention. Because there are fixed costs associated with the prevention phase of the cybersecurity lifecycle, such as in-house expertise and investments in technologies, there will be a cost even if the attack is stopped before doing damage. For example, the average total cost of a phishing attack is $832,500 and of that 82 percent is spent on detection, containment, recovery and remediation. Respondents estimate 18 percent is spent on prevention. Thus, if the attack is prevented the total cost saved would be $682,650 (82 percent of $832,500).

Figure 1 illustrates the dilemma organizations face with respect to prevention in the cybersecurity lifecycle. Seventy percent of respondents (34 percent + 36 percent) believe the ability to prevent cyberattacks would strengthen their organization's cybersecurity posture. However, 76 percent of respondents (40 percent + 36 percent) say they have given up on improving their ability to prevent an attack because it is too difficult to achieve.

Figure 1. Perceptions about the prevention of cyberattacks



The following are the most noteworthy findings from the research.

- **Organizations are most effective in containing cyberattacks.** Fifty-five percent of respondents say their organizations are very or highly effective at containing attacks in the cybersecurity lifecycle. Less than half of respondents (46 percent) say their organizations are very or highly effective in preventing cyberattacks. Organizations are also allocating more of the IT security budget to technologies and processes in the containment phase than in the prevention phase.

- **Prevention of a cyberattack is the most difficult to achieve in the cybersecurity lifecycle.** Eighty percent of respondents say prevention is very difficult to achieve followed by recovery from a cyberattack. The reason for the difficulty is that it takes too long to identify an attack. Other reasons are outdated or insufficient technologies and lack of in-house expertise. The technology features considered most important are the ability to prevent attacks in real-time and based on different types of files.

- **Automation and advanced technologies increase the ability to prevent cyberattacks.** Sixty percent of respondents say their organizations currently deploy AI-based or plan to deploy AI for cybersecurity within the next 12 months. Sixty-seven percent of respondents believe the use of automation and advanced technologies would increase their organizations' ability to prevent cyberattacks. Further, 67 percent of respondents expect to increase their investment in these technologies as they mature.

- **Deep learning is a form of AI and is inspired by the brain's ability to learn.** In the context of this research, deep learning is defined as follows: once a human brain learns to identify an object, its identification becomes second nature. Deep learning's artificial brains consist of complex neural networks and can process high amounts of data to get a profound and highly accurate understanding of the data analyzed. The top three reasons to incorporate a deep-learning-based-solution are to lower false positive rates, increase detection rates and prevent unknown first-seen cyberattacks.

- **Perceptions that AI could be a gimmick and lack of in-house expertise are the two challenges to deployment of AI-based technologies.** Fifty percent of respondents say when trying to gain support for the adoption of AI there is internal resistance because it is considered a gimmick. This is followed by the inability to recruit personnel with the necessary expertise (49 percent of respondents).

- **Organizations are making investments in technology that do not strengthen their cybersecurity budget based on the wrong metrics.** Fifty percent of respondents say their organizations are wasting limited budgets on investments that don't improve their cybersecurity posture. The primary reasons for the failure are system complexity, personnel and vendor support issues. Another reason is that most organizations are using return on investment (ROI) to justify investments and is not based on the technology's ability to increase prevention and detection rates.

- **IT security budgets are considered inadequate.** Only 40 percent of respondents say their budgets are sufficient to achieve a strong cybersecurity posture. The average total IT budget is $94.3 million and of this 14 percent or approximately $13 million is allocated to IT security. Nineteen percent or approximately $2.5 million will be allocated to investments in enabling security technologies such as AI, machine learning, orchestration, automation, blockchain and more.

Part 2. Key findings

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

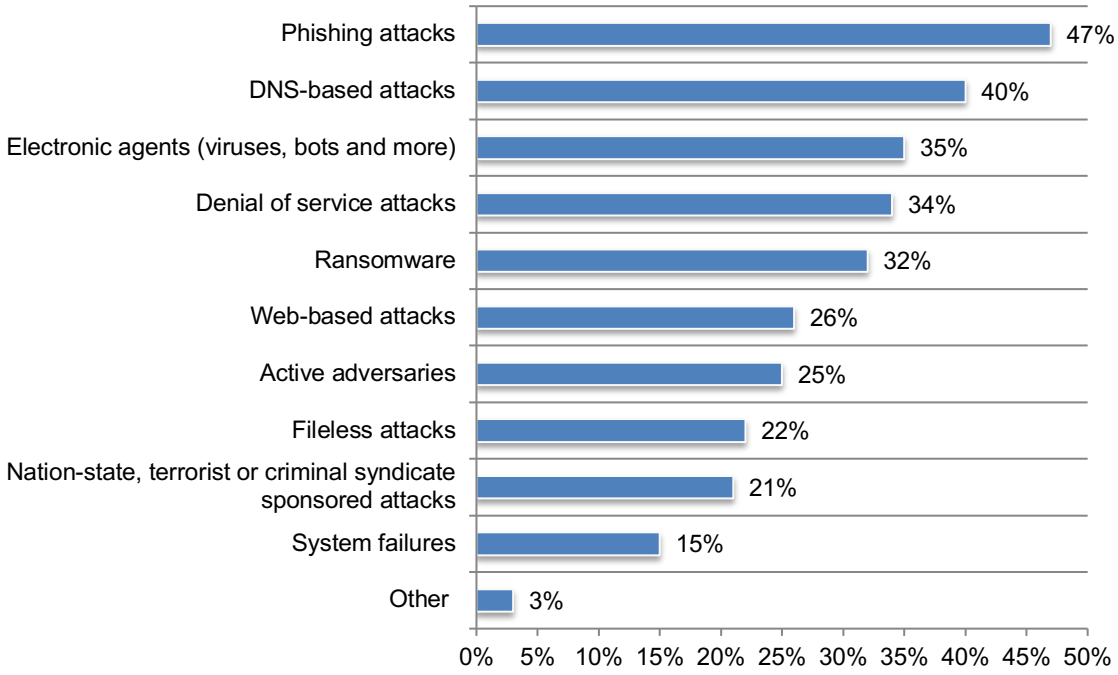
- The top security threats organizations should prevent
- Prevention in the cybersecurity lifecycle is difficult to achieve
- Attacks in the cybersecurity lifecycle
- Artificial intelligence, automation and deep learning are reshaping IT security
- Budget and investments in the cybersecurity lifecycle

The top security threats organizations should prevent

Figure 2 presents a list of security threats affecting organizations represented in this study. As shown, phishing attacks, DNS-based attacks and electronic agents top the list.

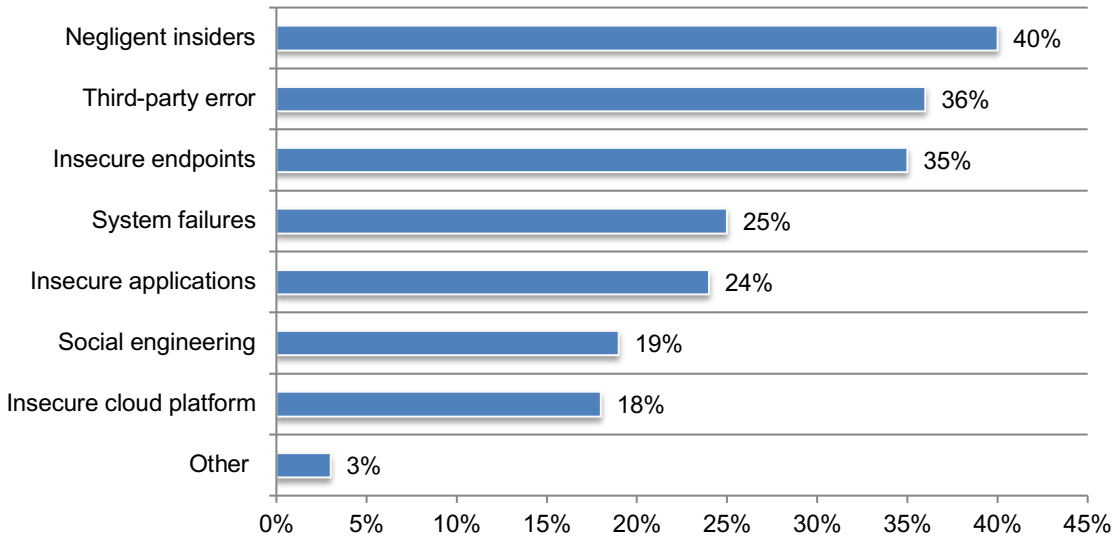
> *"Ready or not we have to be prepared for the security risks of IoT and digital transformation. The ability to prevent attacks will be critical to prevent security exploits related to unsecured IoT devices and the digital transformation process."*
>
> ***IT security manager, retail industry.***

Figure 2. What are the top security threats affecting your organization?
Three responses permitted



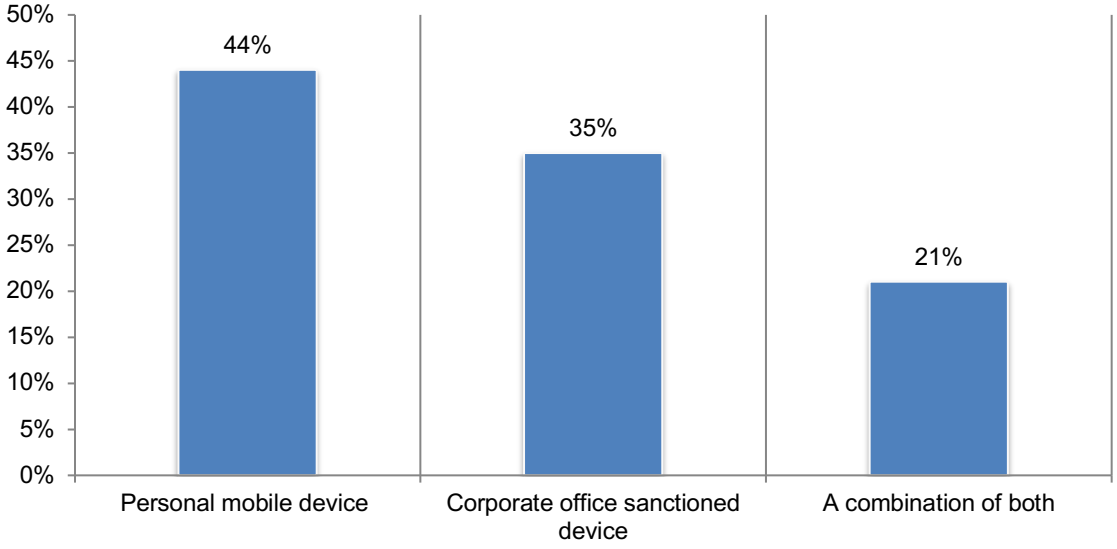
Negligent insiders, third-party error and insecure endpoints are the top security vulnerabilities that respondents believe can be the source of a security exploit.

Figure 2. What are the top security vulnerabilities affecting your organization?
Two responses permitted



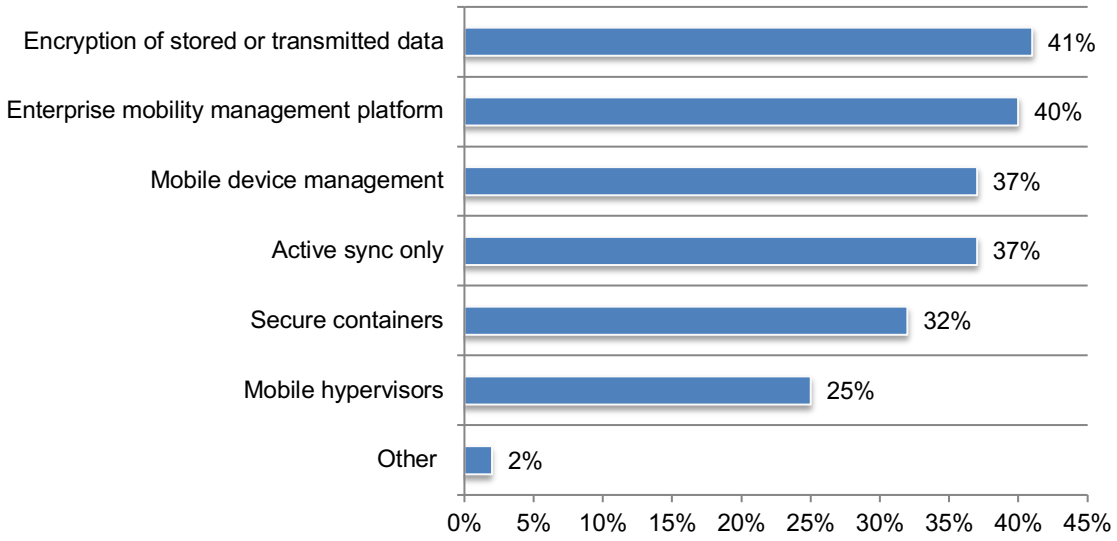
BYOD brings risk to the workplace. Fifty-four percent of respondents say their organizations allow the use of personal mobile devices in the workplace and an average of 41 percent of employees use their mobile device for work. According to Figure 3, 44 percent of respondents are using their personal device. Only 35 percent of respondents say the device is approved by the organization.

Figure 3. What type of mobile device is allowed?



Only 39 percent of respondents say their organizations take steps to protect its information assets on employees' mobile phones. According to Figure 4, the top two steps taken are to encrypt stored or transmitted data (41 percent of respondents) or the use of an enterprise mobility management platform (40 percent of respondents).

Figure 4. How does your organization secure mobile devices used by employees?
More than one response permitted



Prevention in the cybersecurity lifecycle is difficult to achieve

In the context of this research, we define each phase of the lifecycle as follows:

Prevention is the effort to stop malicious threats from running and to classify in real time what type of attacks are targeting the organization. It is the ability to stop files or fileless attacks pre-executive before any process is running.

Detection is the effort to identify cyber threats through heightened visibility of the IT security infrastructure. It is the ability to identify the malicious process while already running on the machine or network.

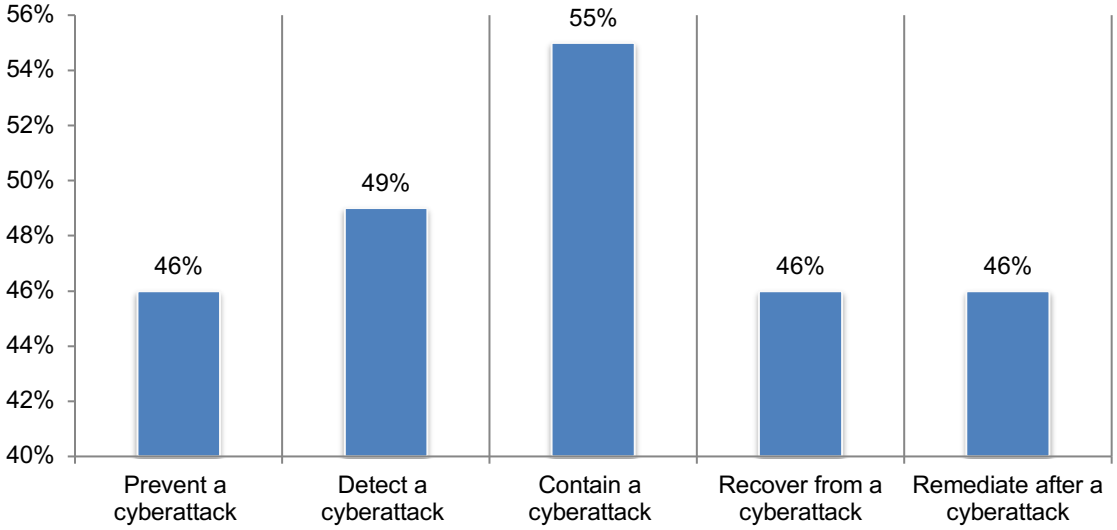
Containment occurs once a cyber threat is identified and includes efforts to stop it spread.

Recovery occurs once the cyber threat is contained and efforts are made to restore the IT security infrastructure to its previous state.

Remediation is the effort to ensure that for the present and future there are the people, processes and technologies in place to prevent future cyber threats.

Organizations are most effective in containing cyberattacks. Respondents were asked to rate the effectiveness of dealing with the five stages of the lifecycle on a scale from 1 = not effective to 10 = highly effective. Figure 5 presents the high effective responses (7+ on the 10-point scale). Fifty-five percent of respondents rate their organizations' ability to contain a cyberattack as highly effective. Less than half (46 percent of respondents) say their organizations are very effective in preventing, recovering and remediating an attack.

Figure 5. How effective is your organization in preventing, detecting, containing, recovering from and remediating a cyberattack?
On a scale of 1 = not effective to 10 = highly effective, 7+ results presented

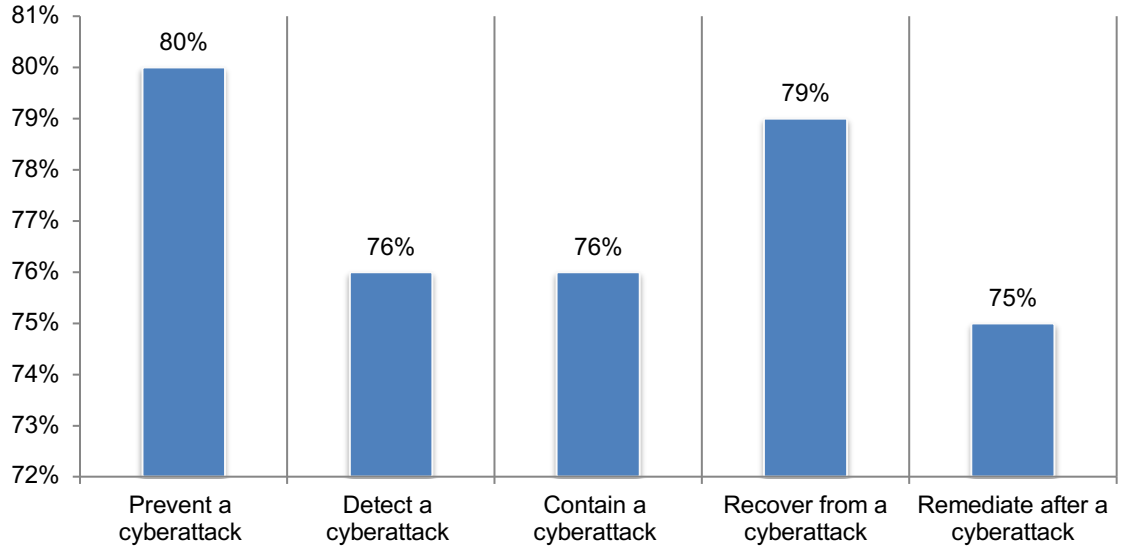


Prevention of a cyberattack is the most difficult to achieve in the cybersecurity lifecycle. According to Figure 6, 80 percent of respondents rate prevention as highly difficult (7+ responses on the 10-point scale) the next most difficult is the recovery phase.

> *"We believe the prevention of attacks is ideal and I think achievable but senior leadership accepts the fact that attacks cannot be prevented. "*
>
> ***Senior IT security manager, hospitality industry.***

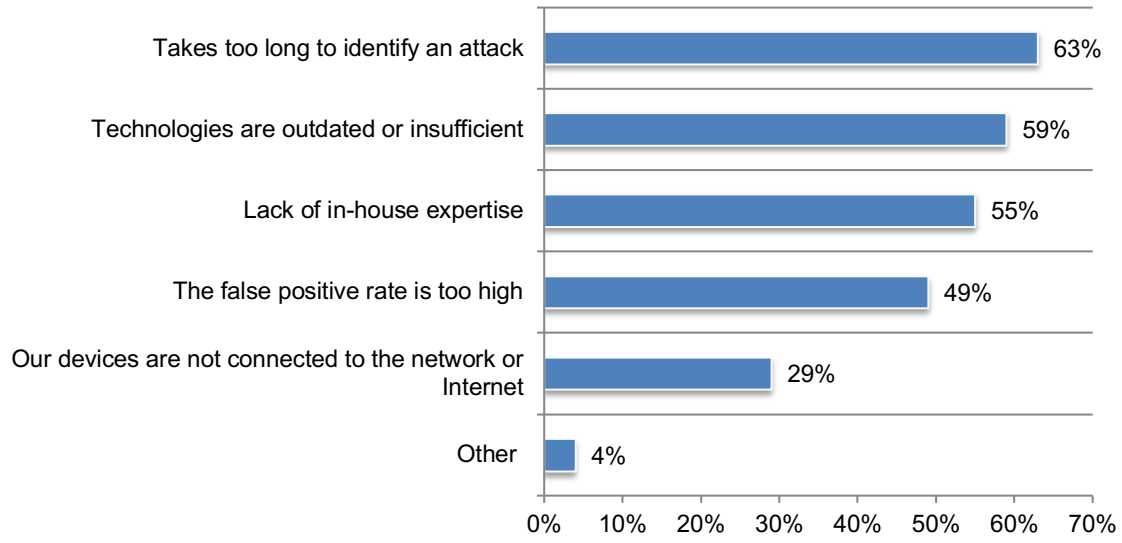
Figure 6. How difficult is it to prevent, detect, contain, recover from and remediate a cyberattack?

On a scale of 1 = not difficult to 10 = highly difficult 7+ results presented



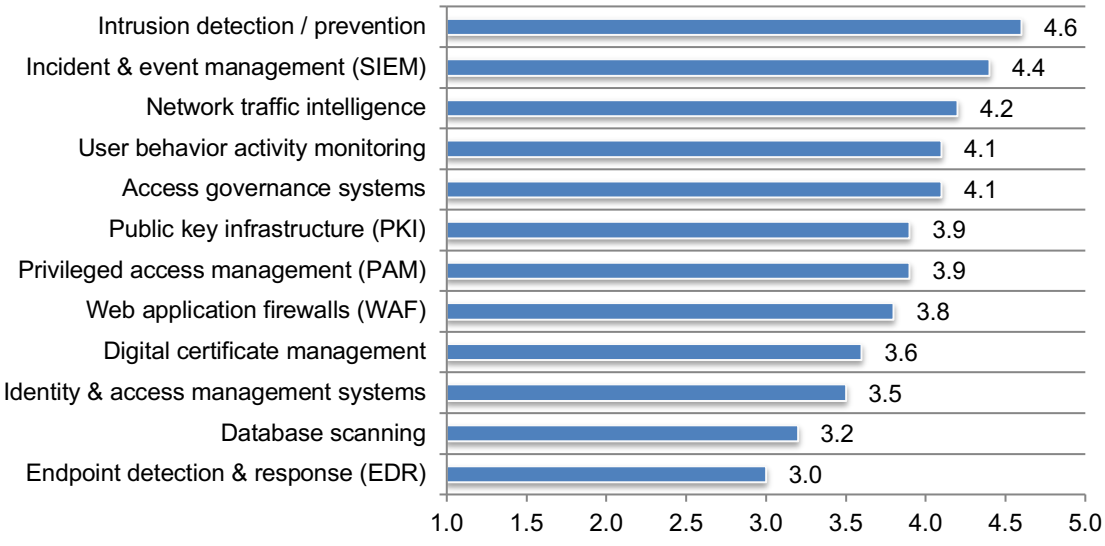
Prevention is difficult because it takes too long to identify an attack. As shown above, 80 percent of respondents say prevention is the most difficult to achieve. According to Figure 7, 63 percent of respondents say difficulty can be attributed to the length of time it takes to identify an attack and outdated or insufficient technologies (59 percent of respondents).

Figure 7. What are the barriers to preventing a cyberattack?
More than one response permitted



Respondents were asked to rate the impact of different technologies on the ability to prevent a cyberattack on a 5-point scale of 5 = very high impact to 1 = low impact. The technologies that are considered to have the greatest impact on an organization's ability to prevent cyberattacks are presented in Figure 8. Intrusion detection/prevention, SIEM, network traffic intelligence, user behavior activity monitoring and access governance systems are considered to have a high impact on improving the ability to prevent cyberattacks.

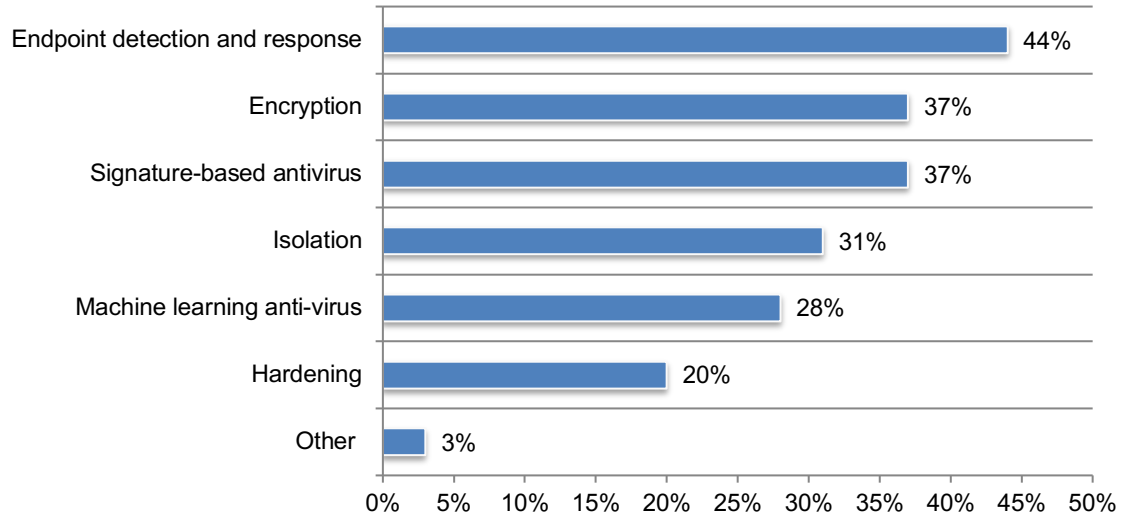
Figure 8. Technologies with the highest ability to prevent cyberattacks
On a 5-point scale of: 5 = very high impact, 4 = high impact, 3 = moderate impact, 2 = low impact and 1 = very low impact



The technologies used to prevent cyberattacks are only moderately effective. As discussed, a primary barrier to preventing cyberattacks are outdated or insufficient technologies. As shown in Figure 9, the technology most often used is endpoint detection and response, which is considered only moderately effective in improving the prevention of cyberattacks (3.0 on the 5-point scale, as shown in Figure 8).

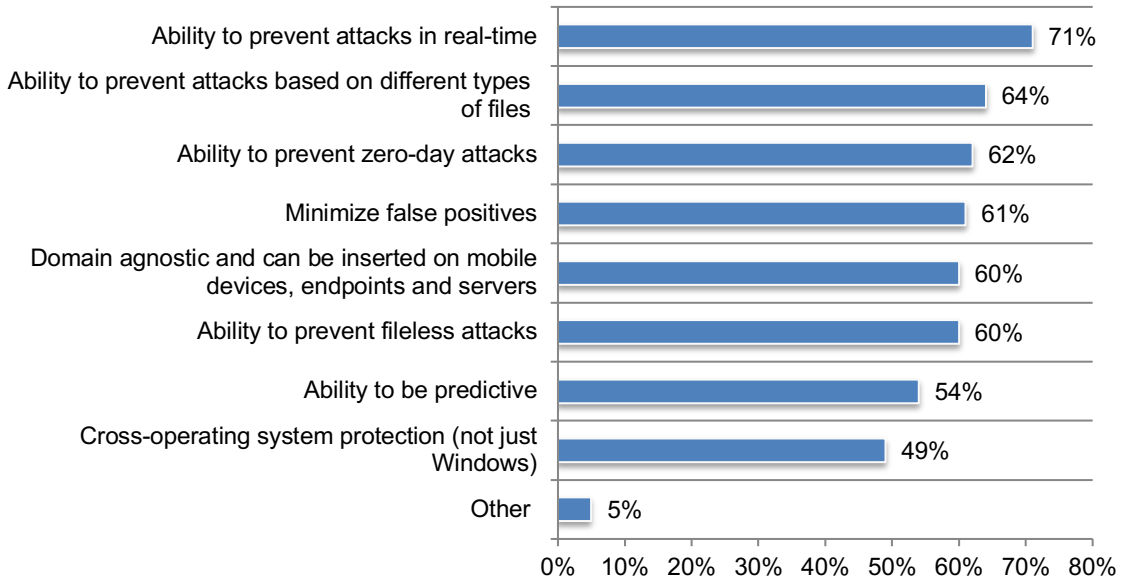
> *"Once attacks are on the inside, we cannot accurately determine the financial and reputational consequences to our company."*
>
> ***Security analyst, healthcare industry.***

Figure 9. What solutions do you currently use to prevent cyberattacks?
Two responses permitted



The ability to prevent attacks in real-time and based on different types of files are the two most important technology features, according to 71 percent and 64 percent of respondents. As shown in Figure 10, the majority of respondents believe all these features are important when attempting to prevent a cyberattack.

Figure 10. What technology features are important in the prevention of cyberattacks?
More than one response permitted

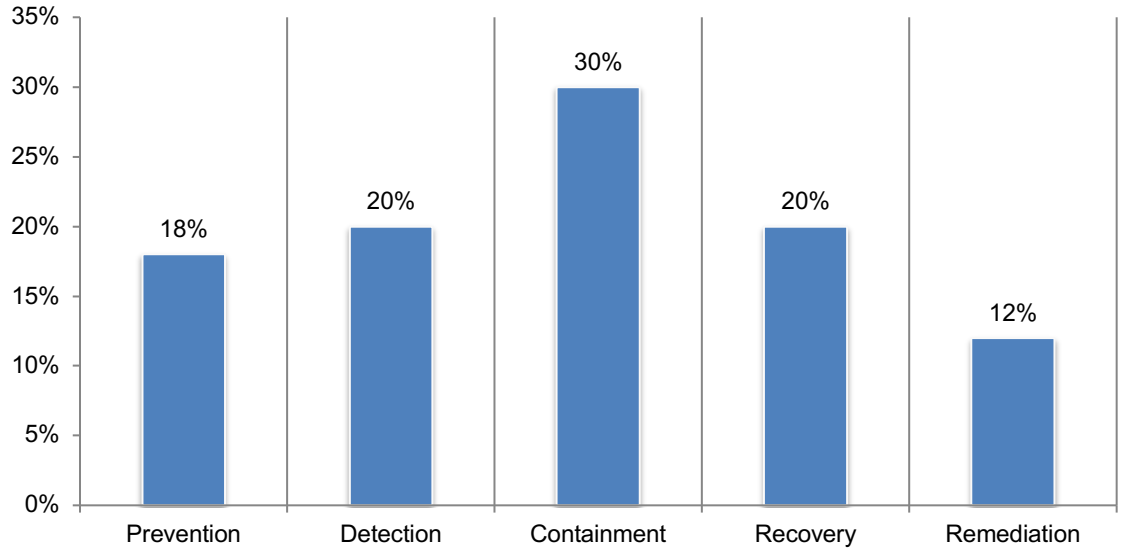


Attacks in the cybersecurity lifecycle

In this section, we discuss in what phase of the cybersecurity lifecycle organizations are able to deal with an attack. The five attacks featured in this section are: phishing, zero-day, spyware, nation-state and ransomware. According to the findings, very few respondents are able to prevent and detect these attacks. Respondents were also asked what the one attack cost their organizations and estimate the cost savings if their organization were able to prevent the attack.

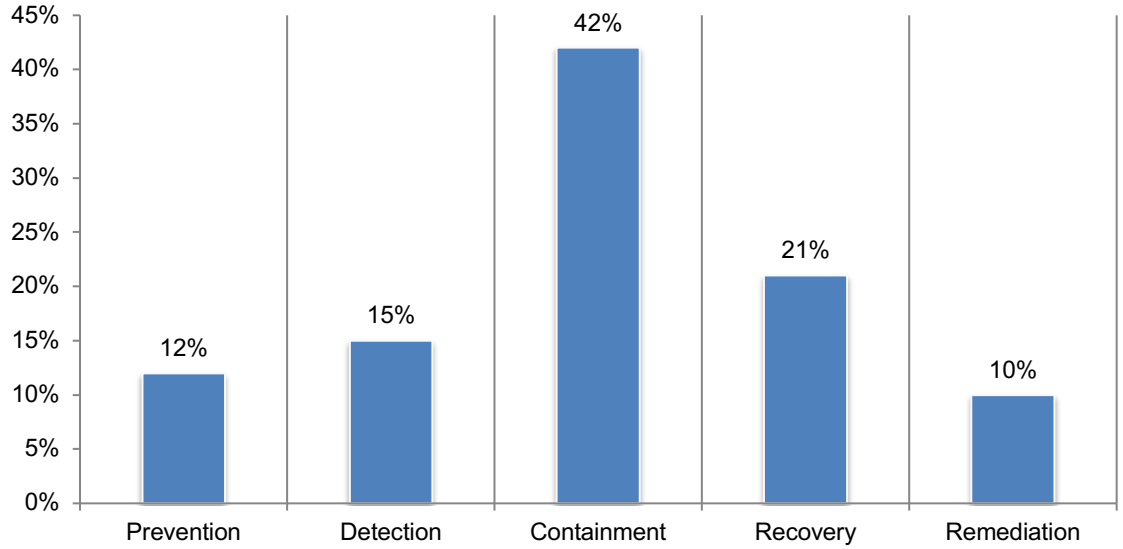
Most organizations are only able to deal with the phishing attack in the later phases of the cybersecurity lifecycle. Seventy-nine percent of respondents say their organization had a phishing attack in the past year. Of these respondents, only 18 percent were able to prevent this attack, as shown in Figure 11.

Figure 11. In what phase of the cybersecurity lifecycle were you able to deal with the phishing attack?



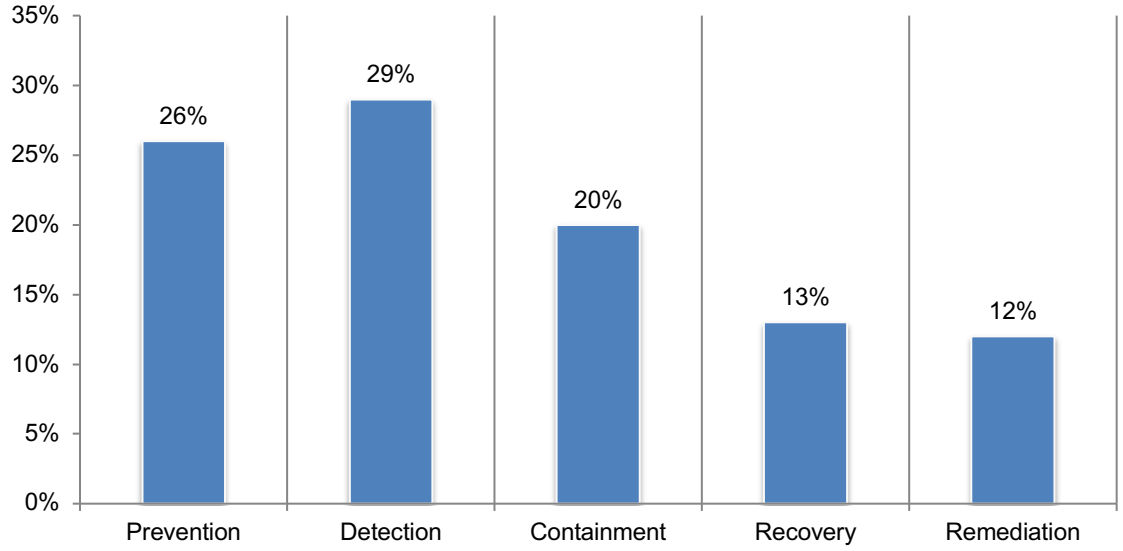
Very few organizations are able to deal with a zero-day attack. Fifty-two percent of respondents say their organization had a zero-day attack. As shown in Figure 12, only 12 percent of respondents say they were able to prevent the attack.

Figure 12. In what phase of the cybersecurity lifecycle were you able to deal with the zero-day attack?



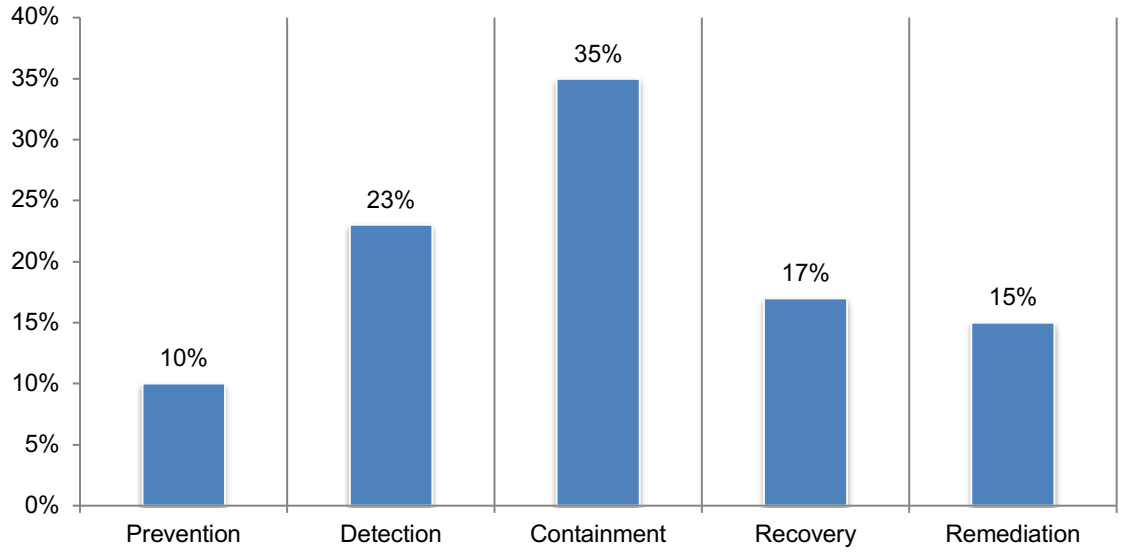
Prevention is more effective in the case of a spyware attack. Thirty-seven percent of respondents say their organizations had a spyware attack in the past year. Twenty-six percent of these respondents say their organizations were able to prevent a spyware attack, as shown in Figure 13. Only 20 percent of respondents say the spyware attack was dealt with in the containment phase.

Figure 13. In what phase of the cybersecurity lifecycle were you able to deal with the spyware attack?



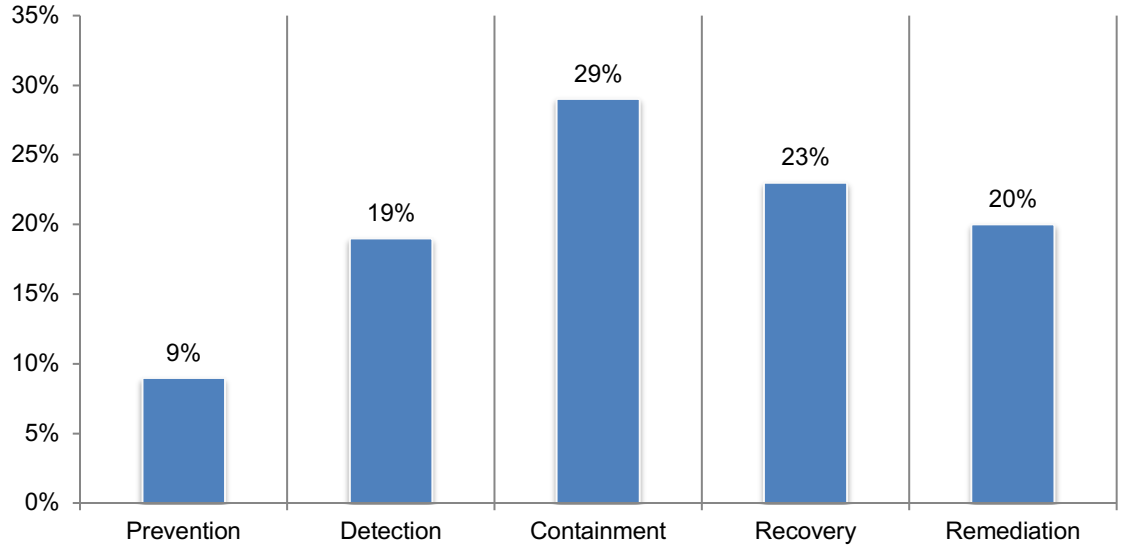
Very few organizations are able to prevent a ransomware attack. Twenty-three percent of respondents say their organization had a ransomware attack. According to Figure 14, only 10 percent of respondents were able to prevent a ransomware attack. Thirty-five percent of respondents say it was dealt with in the containment phase.

Figure 14. In what phase of the cybersecurity lifecycle were you able to deal with the ransomware attack?



Nation-state attacks are few but difficult to prevent. Eighteen percent of respondents say their organization had a nation-state attack in the past year. As shown in Figure 15, only 9 percent of respondents say they were able to prevent a nation-state attack.

Figure 15. In what phase of the cybersecurity lifecycle were you able to deal with the nation-state attack?



Prevention of attacks can reduce the cost of an attack significantly. To determine the **economic value of prevention**, respondents were first asked to estimate the cost of one of the following five types of attacks: phishing, zero-day, spyware, nation-state and ransomware. They were then asked to estimate what percentage of the cost is spent on each phase of the cybersecurity lifecycle, including prevention.

Because there are fixed costs associated with the prevention phase of the cybersecurity lifecycle, such as in-house expertise and investments in technologies, there will be a cost even if the attack is stopped before doing damage. For example, as shown in the Table below, the average total cost of a phishing attack is $832,500 and of that 82 percent is spent on detection, containment, recovery and remediation. Respondents estimate 18 percent is spent on prevention. Thus, if the attack is prevented the total cost saved would be $682,650 (82 percent of $832,500). If organizations experienced all attacks the average total cost is $4.7 million and if prevented could save the organization an average of $4 million.

"If we could quantify the cost savings of the prevention of attacks, we would be able to increase our IT security budget and debunk the C-suite's myth that AI is a gimmick. I believe AI is critical to preventing attacks "

CISO, financial services industry.

Nation-state attacks are the costliest attacks to respond to in the cybersecurity lifecycle ($1.5 million). If organizations are able to prevent these attacks, the cost savings could be an average of approximately $1.4 million per attack. A zero-day attack can cost an average of $1.2 million and if prevented could save $1.1 million if it was prevented

Type of attack	Average total cost of an attack	Percent of total cost spent on preventing an attack[1]	Average cost savings resulting from the ability to prevent an attack*
Phishing	$ 832,500	18%	$ 682,650
Zero-day	$ 1,238,000	12%	$ 1,089,440
Spyware	$ 691,500	26%	$ 511,710
Nation-state	$ 1,501,500	9%	$ 1,366,365
Ransomware	$ 440,750	10%	$ 396,675
Total/Average	$ 4,704,250	15%	$ 4,046,840

*Average total cost X (1 – percentage to cost relating to prevention)

[1] The average percent of costs related to the four phases of the cybersecurity lifecycle (detection, containment, recovery and remediation) are as follows: phishing (82 percent of the total cost), zero-day (88 percent of total cost), spyware (74 percent of total cost), nation-state (91 percent of the total cost), ransomware (90 percent of total cost).

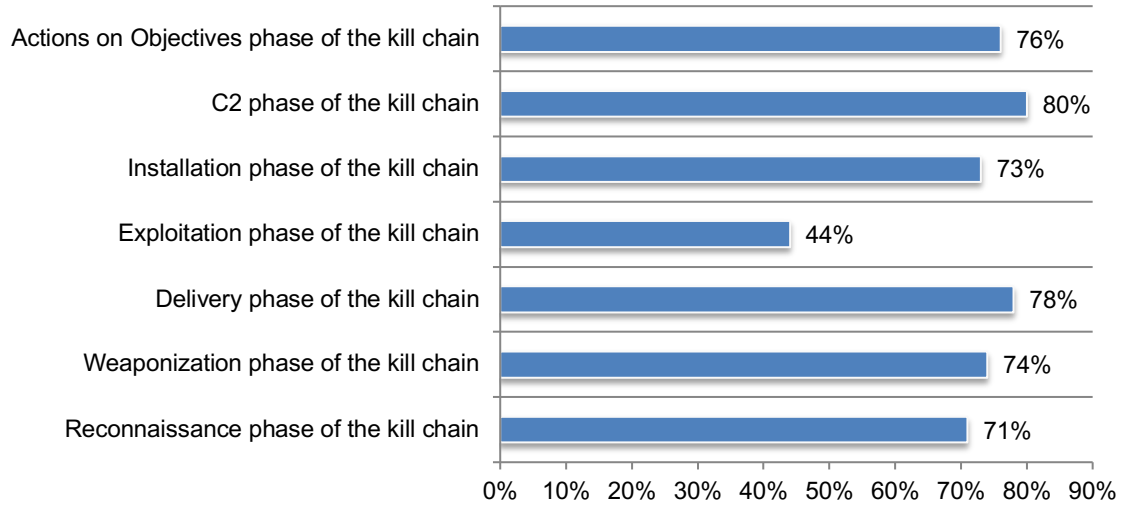
With the exception of the exploitation phase of the kill chain, zero-day attacks are very difficult to prevent in the cyber kill chain. The cyber kill chain is a way to understand the sequence of events involved in an external attack on an organization's IT environment. Understanding the cyber kill chain model is considered helpful in putting the strategies and technologies in place to "kill" or contain the attack at various stages and better protect the IT ecosystem. Following are the 7 steps in the cyber kill chain:

1. **Reconnaissance**: the intruder picks a target, researches it and looks for vulnerabilities
2. **Weaponization**: the intruder develops malware designed to exploit the vulnerability
3. **Delivery**: the intruder transmits the malware via a phishing email or another medium
4. **Exploitation:** the malware begins executing on the target system
5. **Installation:** the malware installs a backdoor or other ingress accessible to the attacker
6. **Command and Control (C2):** the intruder gains persistent access to the organization's systems/network
7. **Actions on Objective:** the Intruder initiates end goal actions, such as data theft, data corruption or data destruction

Respondents were asked to rate the difficulty in preventing a zero-day attack in every phase of the cyber kill chain on a scale of 1 = not difficult to 10 = very difficult. Figure 16 presents the very difficult responses (7+ on the 10-point scale). The most difficult phase to prevent the zero-day attack is the command and control phase (80 percent) in which the intruder gains persistent access to the organization's systems/network followed by the delivery phase of the kill chain (78 percent).

> *"We are optimistic that AI when properly deployed will make a huge difference in our ability to prevent attacks. The problem is finding the right people who can make AI work."*
>
> ***SOC analyst, consumer goods industry.***

Figure 16. How difficult is it to prevent a zero-day attack during each phase of cyber kill chain?
On a scale of 1 = not difficult to 10 = very difficult, 7+ responses presented

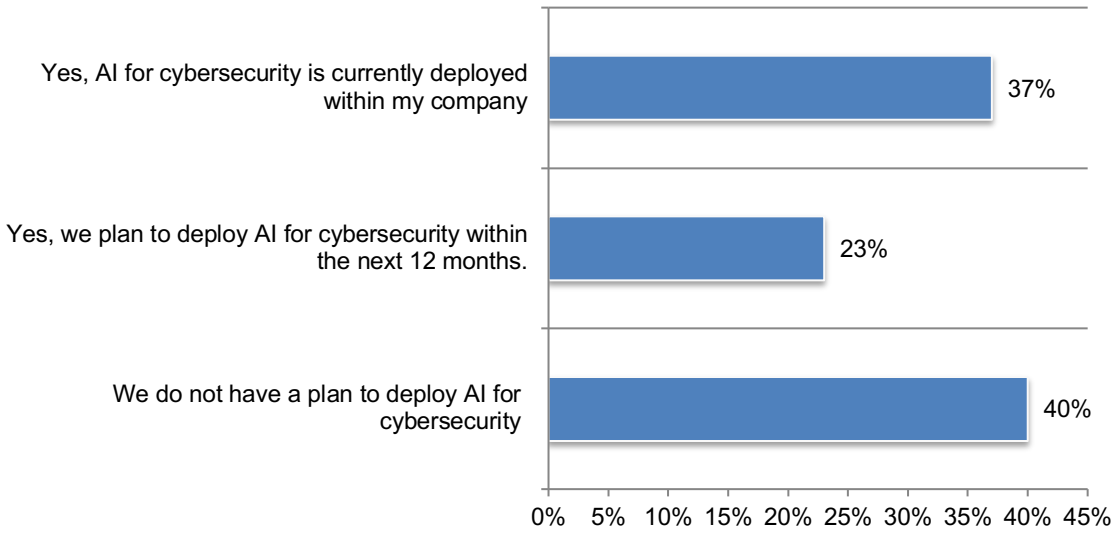


Artificial intelligence, automation and deep learning are reshaping IT security

In the context of this research, automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. Such technologies depend upon artificial intelligence (AI), machine learning and orchestration. AI refers to the development of computer systems that are able to perform tasks normally requiring human intelligence.

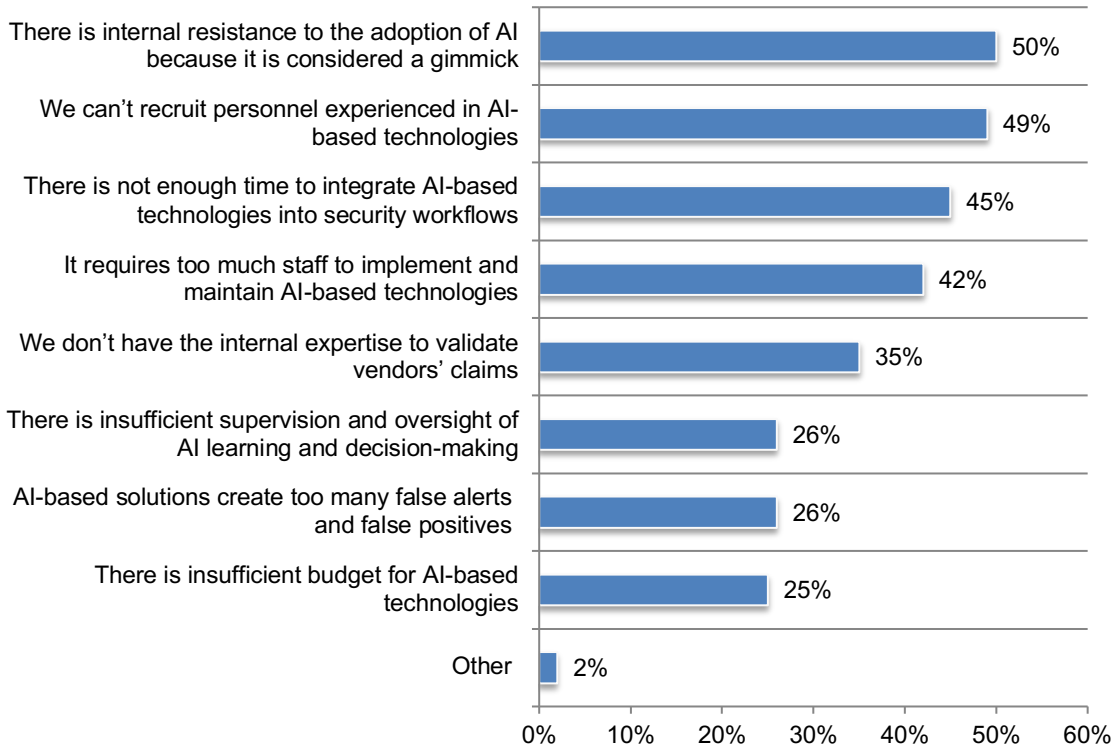
As shown in Figure 17, 60 percent of respondents say their organizations either currently deploy AI (37 percent of respondents) or plan to deploy AI for cybersecurity within the next 12 months (23 percent of respondents).

Figure 17. Does your organization presently or plan to deploy AI-based security technologies?



Perceptions that AI could just be a gimmick is the number one challenge to investing in AI-based technologies. Figure 18 lists the various challenges to the adoption of AI. Fifty percent of respondents say when trying to gain support for the adoption of AI there is internal resistance because it is considered a gimmick. This is followed by the inability to recruit personnel with the necessary expertise (49 percent of respondents) and the lack of time to integrate AI-based technologies into security workflows.

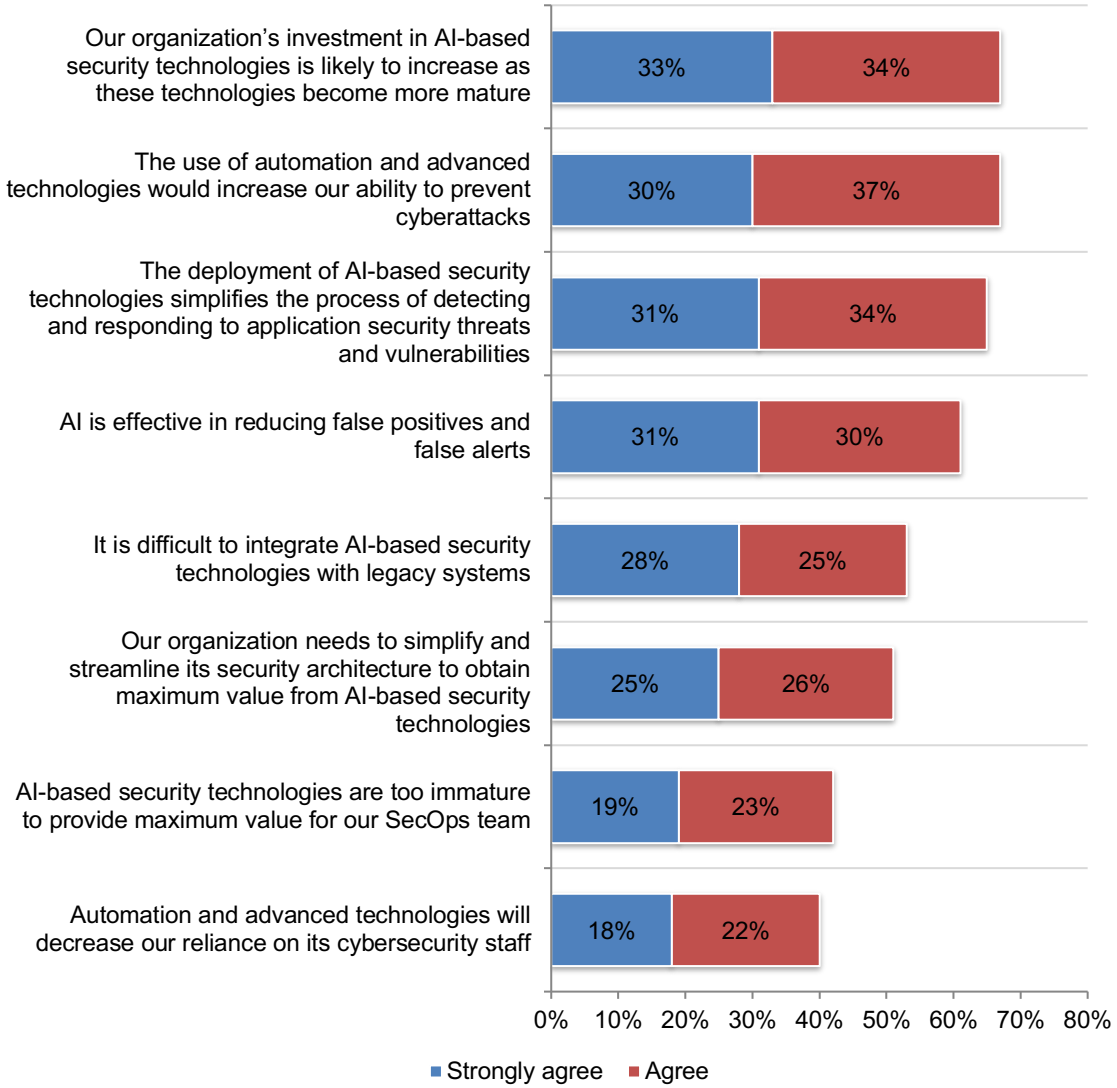
Figure 18. What are the challenges to successfully deploying AI-based technologies?
Three responses permitted



Automation and advanced technologies increase the ability to prevent cyberattacks. According to Figure 19, 67 percent of respondents (30 percent + 37 percent) believes the use of automation and advanced technologies would increase their organizations' ability to prevent cyberattacks. Further, 67 percent of respondents say their organizations expect to increase their investment in these technologies as they mature.

Features that make automation desirable are the simplification of the process that detects and responds to application security threats and vulnerabilities (65 percent of respondents) and effectiveness in reducing false positives and alerts (61 percent of respondents). The challenges with artificial intelligence are the difficulty in integrating AI-based security technologies with legacy systems (53 percent of respondents) and the need to simplify and streamline their organizations security architecture to obtain maximum value from AI-based security technologies (51 percent of respondents).

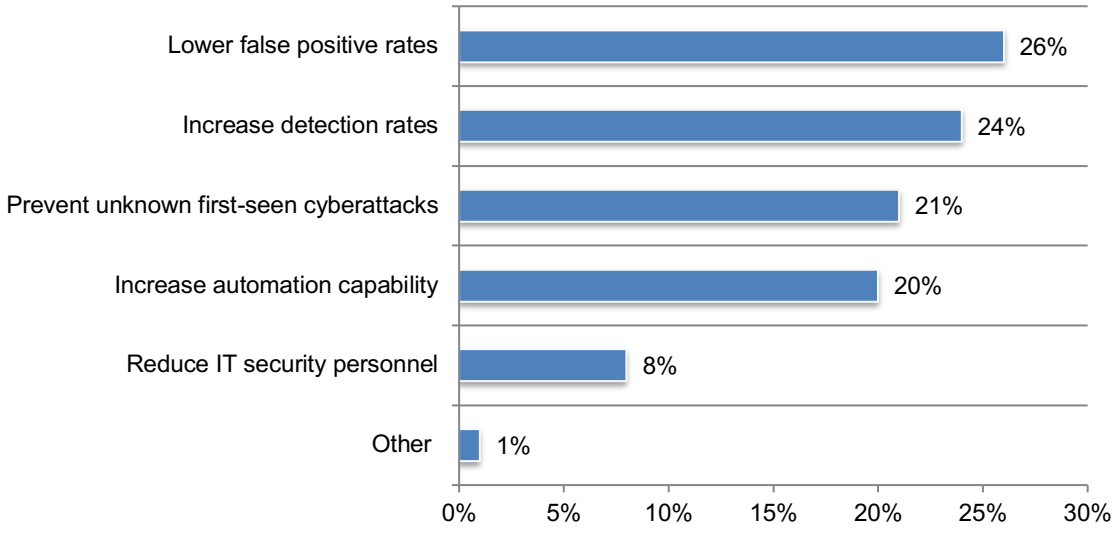
Figure 19. Perceptions about automation



Deep learning is a form of AI and is inspired by the brain's ability to learn. In the context of this research, deep learning is defined as follows: once a human brain learns to identify an object, its identification becomes second nature. Deep learning's artificial brains consist of complex neural networks and can process high amounts of data to get a profound and highly accurate understanding of the data analyzed.

When asked what is the number one reason to adopt deep learning, respondents say it is to lower false positive rates (26 percent), increase detection rates (24 percent) and prevent unknown firs-seen cyberattack (21 percent), as shown in Figure 20.

Figure 20. What would be your organization's number one reason for incorporating a deep-learning-based solution?
Only one response permitted



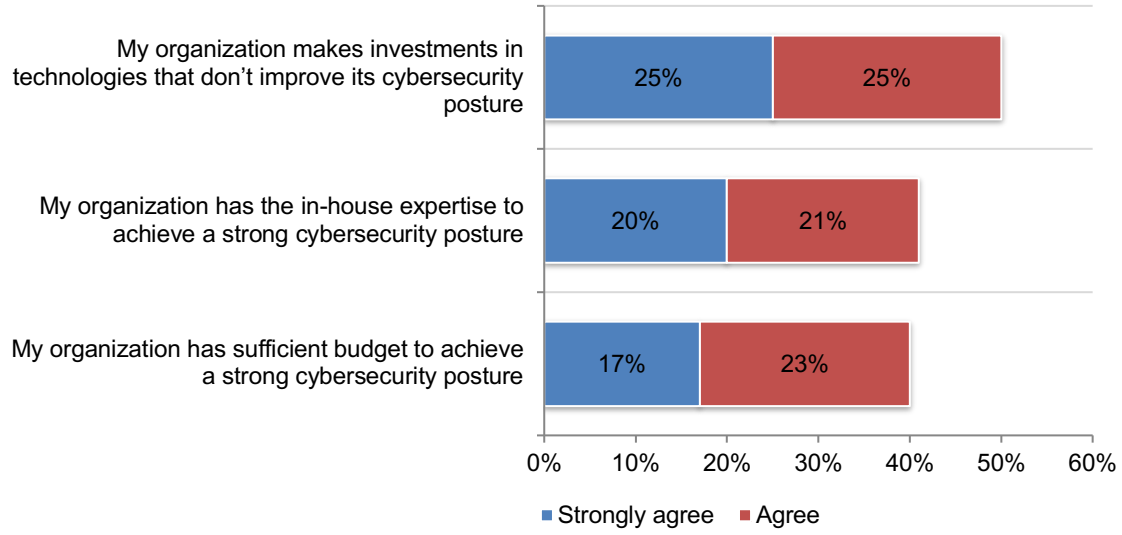
Budget and investments in the cybersecurity lifecycle

Organizations are making investments in technology that do not strengthen their cybersecurity posture. According to Figure 21, 50 percent of respondents say their organizations are wasting limited budgets on investments that don't improve their cybersecurity posture.

Only 40 percent of respondents have sufficient budget to achieve a strong cybersecurity posture. Thus, 60 percent are unsure or disagree that their organizations have enough resources to achieve a strong cybersecurity budget. As a consequence, an inadequate budget is preventing organizations from having the in-house expertise to achieve a strong cybersecurity posture.

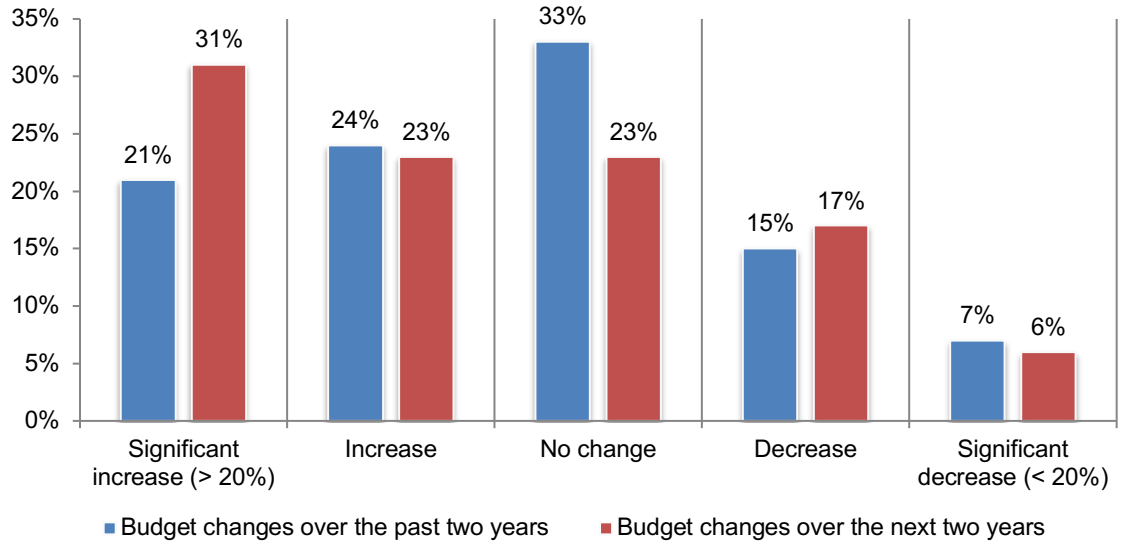
The average total IT budget is $94.3 million and of this 14 percent or approximately $13 million is allocated to IT security. Nineteen percent or approximately $2.5 million will be allocated to investments in enabling security technologies such as AI, machine learning, orchestration, automation, blockchain and more.

Figure 21. Perceptions about budget and investment
Strongly agree and agree responses combined



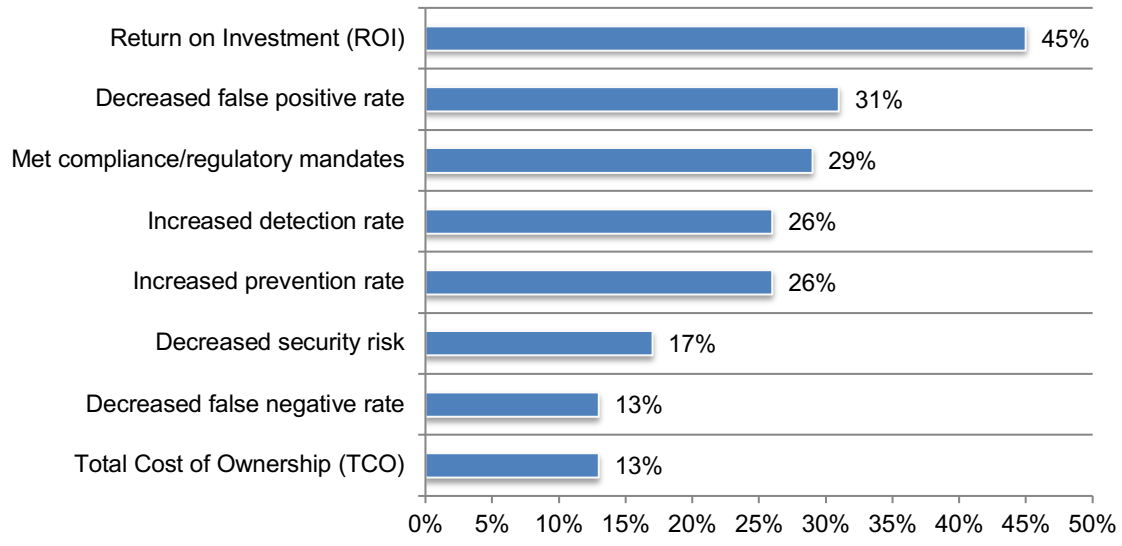
More funding will be allocated to cybersecurity budgets over the next two years. As shown in Figure 22, 21 percent of respondents say their organizations increased the cybersecurity budget significantly over the past two years. Funding will significantly increase over the next two years, according to 31 percent of respondents.

Figure 22. How has your cybersecurity budget or spending levels changed in the past two years and over the next two years?



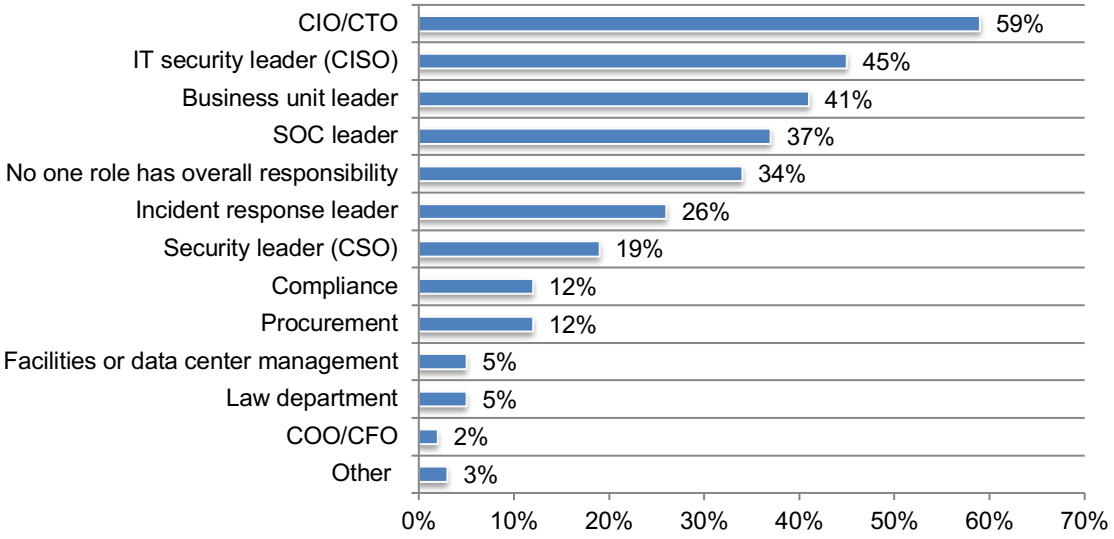
Organizations are relying upon return on investment (ROI) to justify investments followed by a decrease in false positive rates. Only 26 percent of respondents use the increased prevention rate.

Figure 23. What metrics are most important to the cybersecurity technology investment?
Two responses permitted



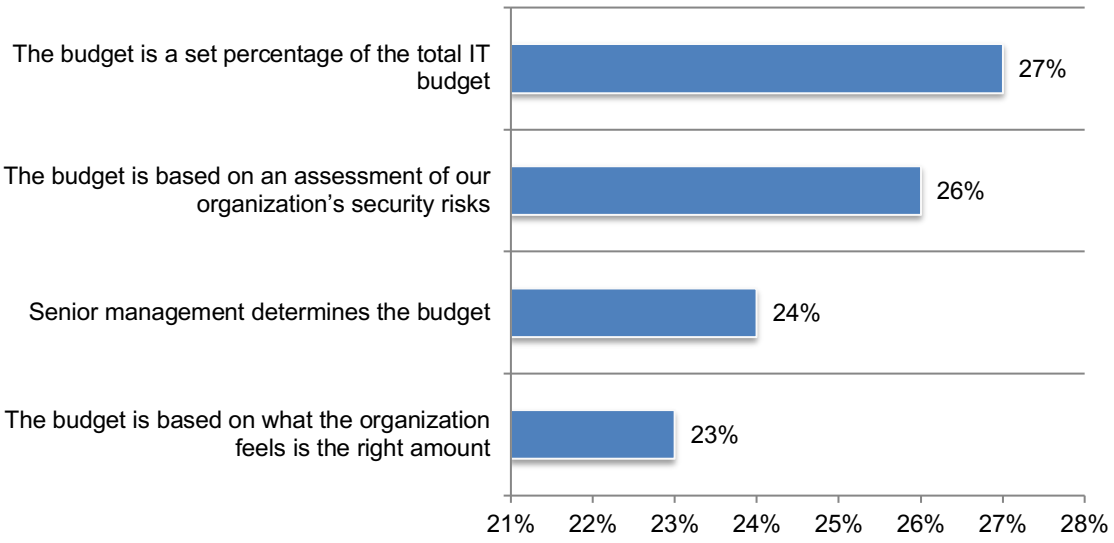
Most often it is the IT and IT security function that owns and participates in determining the cybersecurity budget. According to Figure 24, 59 percent of respondents say it is the CIO/CTO who owns the cybersecurity budget followed by 45 percent of respondents who say it is the IT security leader (CISO).

Figure 24. Who owns the cybersecurity budget?
Three responses permitted



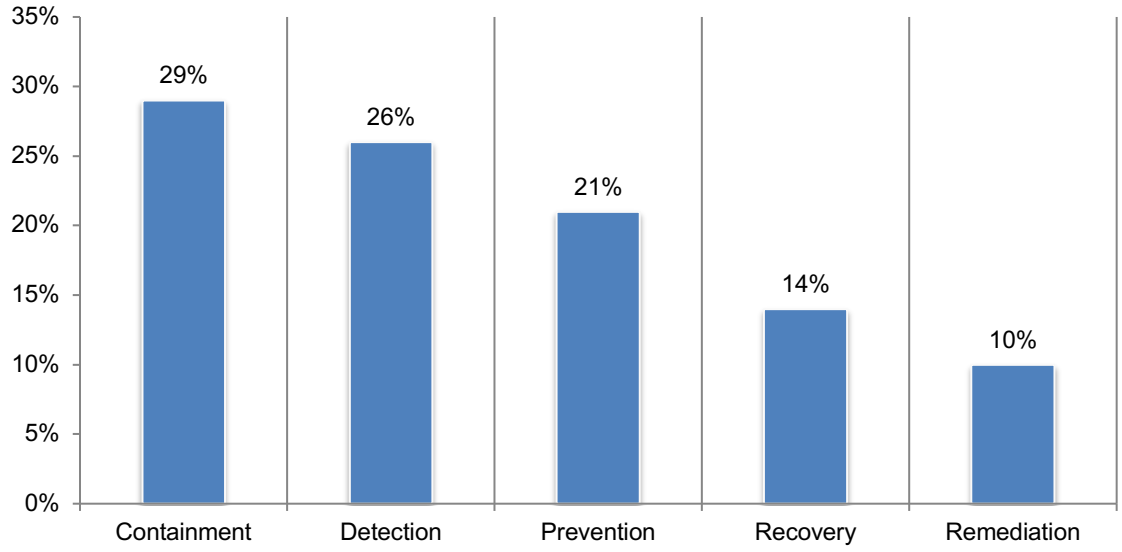
According to Figure 25, 27 percent of respondents say the budget is a set percentage of the total IT budget and 26 percent of respondents say it is based on an assessment of their organizations' security risks.

Figure 25. How does your organization determine its cybersecurity budget?



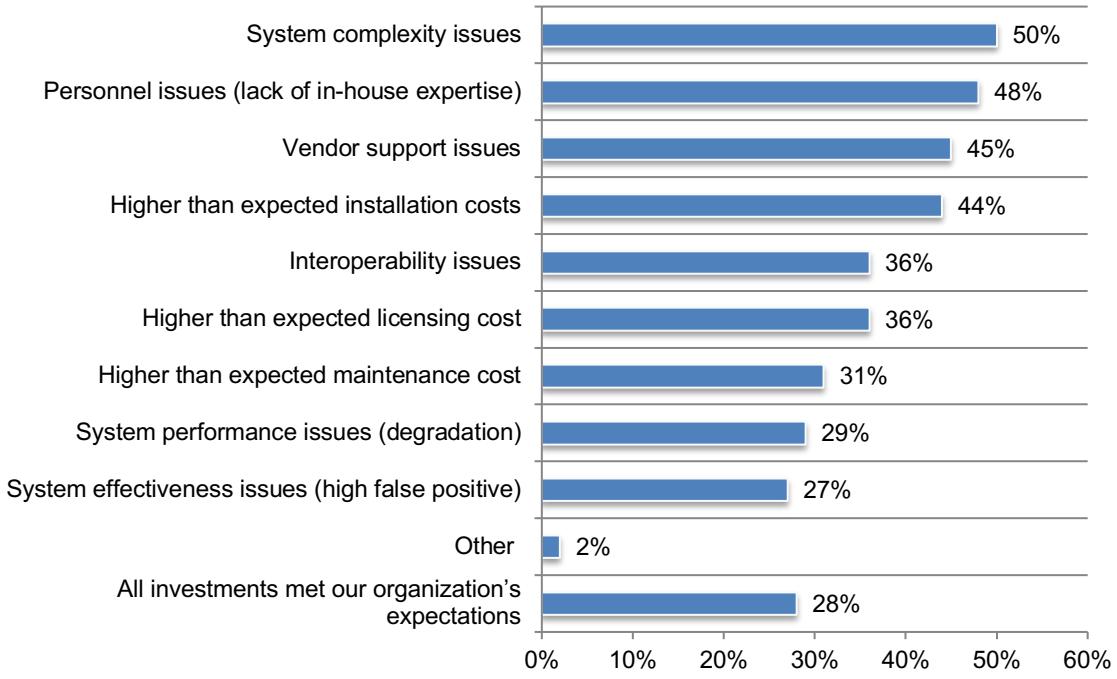
While the ability to prevent cyberattacks is believed to improve the cybersecurity posture of organizations and reduce the cost of incurred because of cyberattacks, only 21 percent of the budget is allocated to prevention. The greatest percentage of the budget is allocated to containment, as shown in Figure 26.

Figure 26. How does your organization allocate its budget for the five phases of the cybersecurity lifecycle?



Complexity and lack of in-house expertise are the primary reasons investments do not meet expectations. As discussed previously, organizations are making investments in technologies that are not strengthening their organizations' cybersecurity posture. As shown in Figure 27, system complexity issues, lack of in-house expertise and vendor support issues are the primary reasons.

Figure 27. Why investments in technology do not meet expectations
More than one response permitted



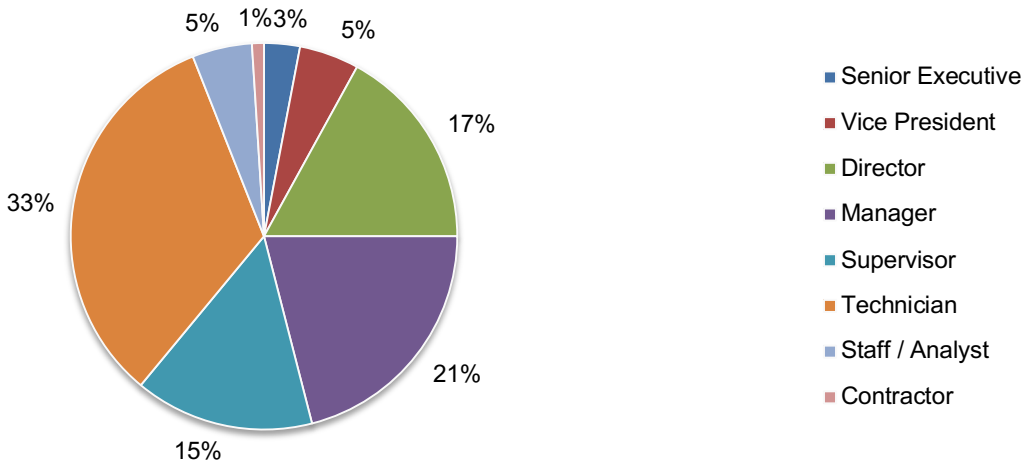
Part 3. Methods

A sampling frame of 16,771 IT and IT security professionals who are knowledgeable about their organizations' cybersecurity technologies and processes were selected as participants in this survey. Table 2 shows 701 total returns. Screening and reliability checks required the removal of 67 surveys. Our final sample consisted of 634 surveys, or a 3.8 percent response rate.

Table 2. Sample response	FY2020	Pct%
Sampling frame	16,771	100.0%
Total returns	701	4.2%
Rejected or screened surveys	67	0.4%
Final sample	634	3.8%

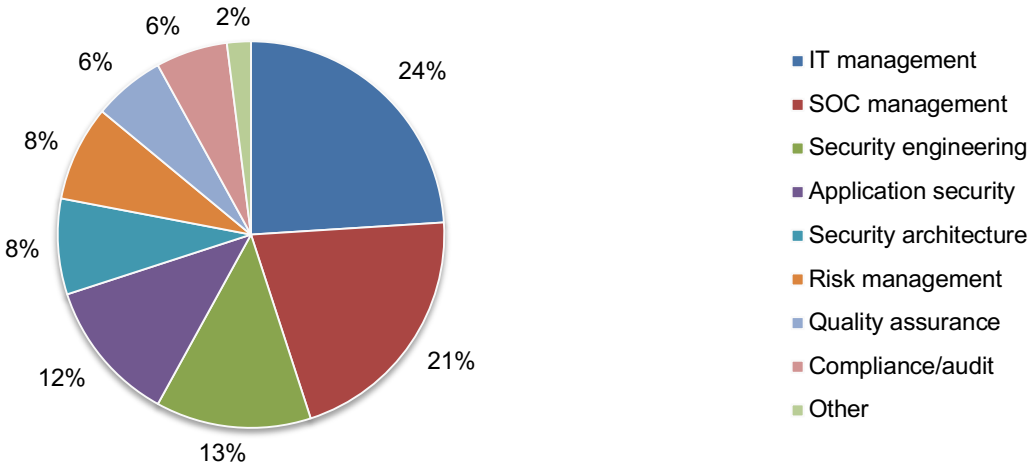
The following pie chart summarizes the position level of qualified respondents. At 33 percent, the largest segment contains those who are rank-and-file level employees (e.g., technicians or analysts). The smallest segment (1 percent) includes contractors. More than half (61 percent) of respondents are at or above the supervisory level.

Pie Chart 1. Position level of respondents



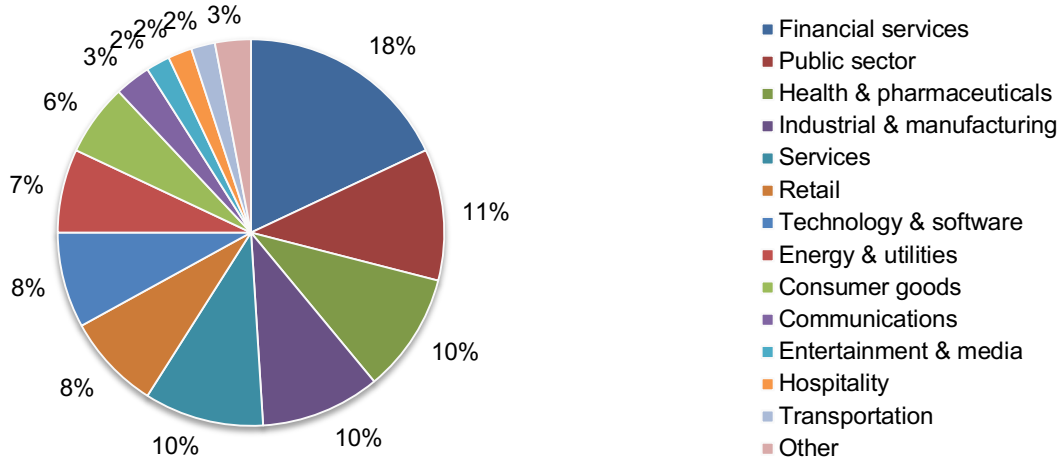
As shown in Pie Chart 2, 24 percent of respondents described their primary role as IT management, 21 percent of respondents are in SOC management, 13 percent of respondents are in security engineering and 12 percent of respondents identified their role as application security.

Pie Chart 2. Primary role within the organization



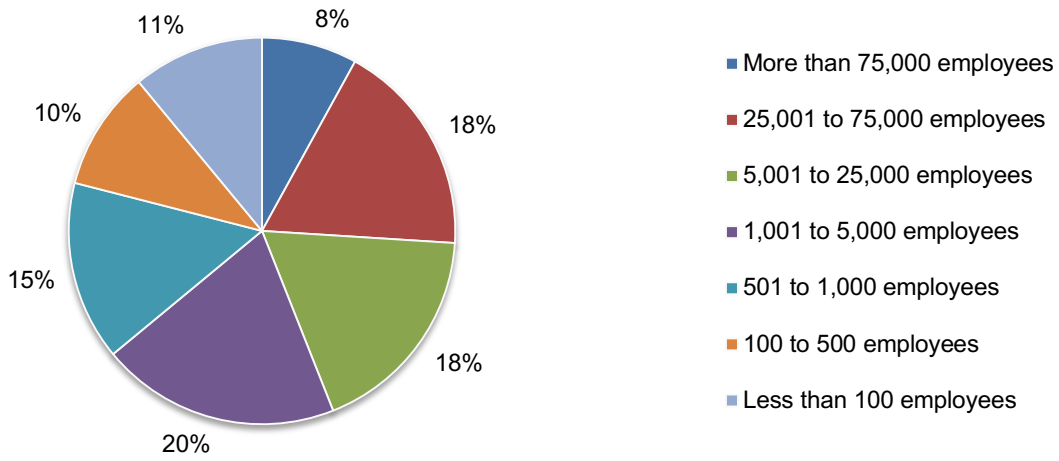
Pie Chart 3 shows the percentage distribution of respondents' companies across 14 industries. Financial services represents the largest industry sector (at 18 percent of respondents), which includes banking, insurance, brokerage, investment management and payment processing. Other large verticals include public services, health and pharma, industrial and manufacturing, and services.

Pie Chart 3. Primary industry sector of respondents' companies



Pie Chart 4 summarizes the total worldwide headcount of respondents' companies. In the context of this study, headcount serves as an indicator of size. At 20 percent, the largest segment contains larger-sized organizations with 5,001 to 25,000 full-time equivalent employees. The smallest segment (8 percent) includes larger-sized organizations with 75,000 or more employees. More than half of respondents are from organizations with a global headcount greater than 1,000 employees.

Pie Chart 4. Global headcount of respondents' organization



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 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 individuals who are knowledgeable about their organizations' cybersecurity technologies and processes. 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 between December 11, 2019 to December 23, 2019.

Survey Response	Freq	Pct%
Total sampling frame	16771	100.0%
Total returns	701	4.2%
Rejected surveys	67	0.4%
Final sample	634	3.8%

Part 1. Screening questions

S1. What best describes your knowledge of cybersecurity technologies and processes deployed in your organization?	Pct%
Very knowledgeable	41%
Knowledgeable	44%
Some knowledge	15%
No knowledge (stop)	0%
Total	100%

S2. What best describes your role within your organization's cybersecurity function? Please select all that apply.	Pct%
Defining strategy	38%
Setting standards	35%
Obtaining resources	41%
Hunting for threats	55%
Educating personnel	29%
Conducting assessments	58%
Testing controls	50%
Operating the SOC	43%
Leading security teams	57%
Evaluating performance	34%
Securing the IT infrastructure	48%
Implementing security technologies	60%
Maintaining security technologies	63%
Communicating with c-level and/or board	21%
None of the above (stop)	0%
Total	632%

S3. What percentage of your job is dedicated to cybersecurity activities?	Pct%
Less than 20% (stop)	0%
20% to 40%	15%
41% to 60%	13%
61% to 80%	24%
81% to 99%	17%
100% fully dedicated	31%
Total	100%

Part 2. Background

Q1a. How effective is your organization's ability to **prevent** a cyberattack on a scale of 1 = not effective to 10 = highly effective?	Pct%
1 or 2	8%
3 or 4	19%
5 or 6	27%
7 or 8	26%
9 or 10	20%
Total	100%
Extrapolated value	6.12

Q1b. How difficult is it to **prevent** a cyberattack on a scale of 1 = not difficult to 10 = highly difficult?	Pct%
1 or 2	0%
3 or 4	1%
5 or 6	19%
7 or 8	33%
9 or 10	47%
Total	100%
Extrapolated value	8.02

Q2a.How effective is your organization's ability to **detect** a cyberattack on a scale of 1 = not effective to 10 = highly effective?	Pct%
1 or 2	11%
3 or 4	9%
5 or 6	31%
7 or 8	25%
9 or 10	24%
Total	100%
Extrapolated value	6.34

Q2b.How difficult is it to **detect** a cyberattack on a scale of 1 = not difficult to 10 = highly effective?	Pct%
1 or 2	2%
3 or 4	4%
5 or 6	18%
7 or 8	32%
9 or 10	44%
Total	100%
Extrapolated value	7.74

Q3a. How effective is your organization's ability to **contain** a cyberattack on a scale of 1 = not effective to 10 = highly effective?	Pct%
1 or 2	11%
3 or 4	9%
5 or 6	25%
7 or 8	29%
9 or 10	26%
Total	100%
Extrapolated value	6.50

Q3b. How difficult is it to **contain** a cyberattack on a scale of 1 = not difficult to 10 = very difficult?	Pct%
1 or 2	6%
3 or 4	8%
5 or 6	10%
7 or 8	36%
9 or 10	40%
Total	100%
Extrapolated value	7.42

Q4a. How effective is your organization's ability to **recover** from a cyberattack on a scale of 1 = not effective to 10 = highly effective?	Pct%
1 or 2	9%
3 or 4	16%
5 or 6	29%
7 or 8	25%
9 or 10	21%
Total	100%
Extrapolated value	6.16

Q4b. How difficult is it to **recover** from a cyberattack on a scale of 1 = not difficult to 10 = Very difficult?	Pct%
1 or 2	2%
3 or 4	7%
5 or 6	12%
7 or 8	34%
9 or 10	45%
Total	100%
Extrapolated value	7.76

Q5a. How effective is your organization's ability to **remediate** after a cyberattack on a scale of 1 = not effective to 10 = highly effective?	Pct%
1 or 2	13%
3 or 4	12%
5 or 6	29%
7 or 8	24%
9 or 10	22%
Total	100%
Extrapolated value	6.10

Q5b. How difficult is it to **remediate** after a cyberattack on a scale of 1 = not difficult to 10 = very difficult?	Pct%
1 or 2	2%
3 or 4	5%
5 or 6	18%
7 or 8	32%
9 or 10	43%
Total	100%
Extrapolated value	7.68

Attributions: Please rate each one of the following statements using the scale provided below each item. **Strongly agree and Agree response combined.**	Strongly agree	Agree
Q6a. My organization has sufficient budget to achieve a strong cybersecurity posture.	17%	23%
Q6b. My organization has the in-house expertise to achieve a strong cybersecurity posture.	20%	21%
Q6c. My organization focuses on the detection of cyberattacks because prevention is perceived to be too difficult to achieve.	40%	36%
Q6d. My organization believes the prevention of attacks is impossible to achieve.	32%	33%
Q6e. The ability to **prevent** cyberattacks would strengthen our cybersecurity posture.	34%	36%
Q6f. The use of **automation** and advanced technologies would increase our organization's ability to **prevent** cyberattacks.	30%	37%
Q6g. Automation and advanced technologies will decrease our organization's reliance on its cybersecurity staff.	18%	22%
Q6h. My organization makes investments in technologies that don't improve its cybersecurity posture.	25%	25%

Q7. What best describes the maturity level of your organization's cybersecurity program or activities?	Pct%
Early stage – many cybersecurity program activities have not as yet been planned or deployed	20%
Middle stage – cybersecurity program activities are planned but only partially deployed	30%
Late-middle stage – many cybersecurity program activities are mostly deployed across the organization	29%
Mature stage – most cybersecurity program activities are successfully deployed, maintained and/or refined across the organization.	21%
Total	100%

Q8. What are the top security threats affecting your organization? Please select your top three choices.	Pct%
Phishing attacks	47%
System failures	15%
Active adversaries	25%
Web-based attacks	26%
Ransomware	32%
Fileless attacks	22%
DNS-based attacks	40%
Denial of service attacks	34%
Electronic agents (viruses, bots and more)	35%
Nation-state, terrorist or criminal syndicate sponsored attacks	21%
Other (please specify)	3%
Total	300%

Q9. What are the top security vulnerabilities affecting your organization? Please select your top two choices.	Pct%
Negligent insiders	40%
System failures	25%
Social engineering	19%
Insecure applications	24%
Insecure endpoints	35%
Insecure cloud platform	18%
Third-party error	36%
Other (please specify)	3%
Total	200%

Q10a. Does your organization presently deploy, or plan to deploy, AI-based security technologies?	Pct%
Yes, AI for cybersecurity is currently deployed within my company	37%
Yes, we plan to deploy AI for cybersecurity within the next 12 months.	23%
We do not have a plan to deploy AI for cybersecurity (please skip to Q11)	40%
Total	100%

Q10b. If yes, what are the challenges to successfully deploying AI-based security technologies within your organization? Please select your top three choices.	Pct%
It requires too much staff to implement and maintain AI-based technologies	42%
AI-based solutions create too many false alerts and false positives	26%
There is not enough time to integrate AI-based technologies into security workflows	45%
We can't recruit personnel experienced in AI-based technologies	49%
We don't have the internal expertise to validate vendors' claims	35%
There is insufficient budget for AI-based technologies	25%
There is insufficient supervision and oversight of AI learning and decision-making	26%
There is internal resistance to the adoption of AI because it is considered a gimmick	50%
Other (please specify)	2%
Total	300%

Q10c. If yes, is it possible to have a high detection rate without affecting the productivity of your organization's IT security team?	Pct%
Yes	48%
No	49%
Unsure	3%
Total	100%

Q11. What would be your organization's number one reason for incorporating a deep learning-based solution?	Pct%
Prevent unknown first-seen cyberattacks	21%
Increase automation capability	20%
Reduce IT security personnel	8%
Increase detection rates	24%
Lower false positive rates	26%
Other (please specify)	1%
Total	100%

Attributions: Please rate each one of the following statements using the scale provided below each item. **Strongly agree and Agree responses**	Strongly agree	Agree
Q12a. The deployment of AI-based security technologies simplifies the process of detecting and responding to application security threats and vulnerabilities.	31%	34%
Q12b. Our organization needs to simplify and streamline its security architecture to obtain maximum value from AI-based security technologies.	25%	26%
Q12c. AI-based security technologies are too immature to provide maximum value for our SecOps team.	19%	23%
Q12d. It is difficult to integrate AI-based security technologies with legacy systems.	28%	25%
Q12e. Our organization's investment in AI-based security technologies is likely to increase as these technologies become more mature.	33%	34%
Q12f. AI is effective in reducing false positives and false alerts.	31%	30%

Part 3. Cybersecurity budget

Q13. What metrics are most important to the security technology investment decision? Please select the top two.	Pct%
Return on Investment (ROI)	45%
Total Cost of Ownership (TCO)	13%
Decreased security risk	17%
Increased prevention rate	26%
Increased detection rate	26%
Decreased false positive rate	31%
Decreased false negative rate	13%
Met compliance/regulatory mandates	29%
Other (please specify)	0%
Total	200%

Q14. Who within your organization “owns” the cybersecurity budget? Please select the top three choices.	Pct%
CEO	0%
COO/CFO	2%
CIO/CTO	59%
Procurement	12%
IT security leader (CISO)	45%
Security leader (CSO)	19%
Compliance	12%
Law department	5%
Business unit leader	41%
SOC leader	37%
Incident response leader	26%
Facilities or data center management	5%
No one role has overall responsibility	34%
Other (please specify)	3%
Total	300%

Q15. What best describes your organization’s approach to determining the cybersecurity budget? Please select the one best choice.	Pct%
The budget is a set percentage of the total IT budget	27%
The budget is based on an assessment of our organization’s security risks	26%
Senior management determines the budget	24%
The budget is based on what the organization feels is the right amount	23%
Total	100%

Q16. What is your organization’s total IT budget?	Pct%
Less than $100,000	0%
$100,00 to $500,000	0%
$500,001 to $1,000,000	2%
$1,000,000 to $5,000,000	7%
$5,000,001 to $10,000,000	19%
$10,000,001 to $50,000,000	23%
$50,000,001 to $100,000,000	25%
$100,000,001 to $250,000,000	15%
$250,000,001 to $500,000,000	5%
More than $500,000,000	4%
Total	100%
Extrapolated value	$ 94,300,000

Q17. Approximately, what percentage of the current year's IT budget will go to IT security activities?	Pct%
Less than 1%	2%
1% to 2%	6%
3% to 5%	14%
6% to 10%	19%
11% to 15%	21%
16% to 20%	19%
21% to 30%	11%
31% to 40%	5%
41% to 50%	3%
More than 50%	0%
Total	100%
Extrapolated value	14%

Q18. Approximately, what percentage of the current year's IT security budget will be invested in enabling security technologies such as AI, machine learning, orchestration, automation, blockchain and more?	Pct%
Less than 1%	0%
1% to 2%	0%
3% to 5%	9%
6% to 10%	16%
11% to 15%	19%
16% to 20%	22%
21% to 30%	18%
31% to 40%	8%
41% to 50%	5%
More than 50%	3%
Total	100%
Extrapolated value	19%

Q19. The following table lists the five phases of the cybersecurity life cycle. Please allocate all 100 points to describe how your organization currently spends budgeted resources for the five phases.	Points
Prevention	21
Detection	26
Containment	29
Recovery	14
Remediation	10
Total (sum to 100 points)	100

Q20a. How has your organization's cybersecurity budget or spending levels changed over **the past two years**?	Pct%
Significant increase (> 20%)	21%
Increase	24%
No change	33%
Decrease	15%
Significant decrease (< 20%)	7%
Total	100%

Q20b. In your opinion, how will your organization's cybersecurity budget or spending levels change over t**he next two years**?	Pct%
Significant increase (> 20%)	31%
Increase	23%
No change	23%
Decrease	17%
Significant decrease (< 20%)	6%
Total	100%

Q21. Did your organization make any investments in security technologies that fell below your expectations (i.e. regrets) for any of the following reasons? Please check all that apply.	Pct%
Higher than expected licensing cost	36%
Higher than expected maintenance cost	31%
Higher than expected installation costs	44%
System performance issues (degradation)	29%
System effectiveness issues (high false positive)	27%
System complexity issues	50%
Personnel issues (lack of in-house expertise)	48%
Interoperability issues	36%
Vendor support issues	45%
Other (please specify)	2%
All investments met our organization's expectations	28%
Total	376%

Q22. Please indicate the impact of each technology on your organization's **ability to prevent** cyber attacks using the following 5-point scale: 5 = very high impact, 4 = high impact, 3 = moderate impact, 2 = low impact and 1 = very low impact	Impact score
Access governance systems	4.1
Anti-malware	2.8
Anti-DDoS	2.4
Automated code review or debugger	1.0
Analytics for security modelling	1.9
Content aware firewalls (NGFW or UTM)	2.1
Data loss prevention (DLP)	2.7
Database activity monitoring	3.0
Database scanning	3.2
Digital certificate management	3.6
Encryption of data at rest	3.2
Encryption of data in motion	2.9
Endpoint detection & response (EDR)	3.0
Hardware security modules (HSM)	1.9
Identity & access management systems	3.5
Incident & event management (SIEM)	4.4
Intrusion detection / prevention	4.6
Network traffic intelligence	4.2
Location surveillance systems	1.4
Privileged access management (PAM)	3.9
Public key infrastructure (PKI)	3.9
Sandbox or isolation capabilities	3.1
User behavior activity monitoring	4.1
Virtual private network (VPN)	1.8
Web & email content filtering	2.0
Web application firewalls (WAF)	3.8
Average	3.0

Part 4. Mobile security

Q23a. Does your organization allow the use of personal mobile devices in the workplace (e.g. BYOD)?	Pct%
Yes	54%
No (skip to Q26)	46%
Total	100%

Q23b. If yes, what type of mobile device is allowed? Please select only one.	Pct%
Personal mobile device (e.g. BYOD)	44%
Corporate office sanctioned device	35%
A combination of both	21%
Total	100%

Q24. What percentage of employees use their mobile device for work?	Pct%
Less than 10 percent	14%
10 percent to 25 percent	21%
26 percent to 50 percent	32%
51 percent to 75 percent	19%
76 percent to 100 percent	14%
Total	100%
Extrapolated value	41%

Q25a. Does your organization take steps to protect its information assets on employees' mobile phones?	Pct%
Yes	39%
No	61%
Total	100%

Q25b. If yes, how does your organization secure mobile devices used by employees in the workplace? Please select all that apply.	Pct%
Active sync only	37%
Encryption of stored or transmitted data	41%
Mobile hypervisors	25%
Secure containers	32%
Mobile device management	37%
Enterprise mobility management platform	40%
Other (please specify)	2%
Total	214%

Part 5. Attacks in the cybersecurity lifecycle

Q26. Currently, what percentage of all attacks can your organization **prevent pre-execution**?	Pct%
Less than 1%	0%
1% to 2%	0%
3% to 5%	3%
6% to 10%	7%
11% to 15%	8%
16% to 20%	11%
21% to 30%	12%
31% to 40%	12%
41% to 50%	26%
More than 50%	21%
Total	100%
Extrapolated value	0.34

Q27. Currently what percentage of all attacks can your organization **detect and respond on execution/post infection**?	Pct%
Less than 1%	2%
1% to 2%	0%
3% to 5%	3%
6% to 10%	7%
11% to 15%	5%
16% to 20%	4%
21% to 30%	11%
31% to 40%	8%
41% to 50%	27%
More than 50%	33%
Total	100%
Extrapolated value	0.38

Q28. What are the barriers to **preventing** a cyberattack? Please check all that apply.	Pct%
Lack of in-house expertise	55%
Technologies are outdated or insufficient	59%
Takes too long to identify an attack	63%
Our devices are not connected to the network or Internet	29%
The false positive rate is too high	49%
Other (please specify)	4%
Total	259%

Q29. What is the average Mean Time to Contain (MTTC) a cyberattack	Pct%
Less than 1 week	2%
1 to 2 weeks	6%
3 to 4 weeks	8%
5 to 6 weeks	12%
7 to 8 weeks	20%
9 to 10 weeks	27%
More than 10 weeks	25%
Total	100%
Extrapolated value (weeks)	8.11

Q30. What solutions do you currently use to prevent cyberattacks? Please select your top two choices.	Pct%
Signature-based antivirus	37%
Machine learning anti-virus	28%
Endpoint detection and response	44%
Encryption	37%
Hardening	20%
Isolation	31%
Other (please specify)	3%
Total	200%

Q31. What technology features are important in the prevention of cyberattacks? Please select all that apply.	Pct%
Ability to be predictive	54%
Ability to prevent attacks in real-time	71%
Ability to prevent attacks based on different types of files	64%
Ability to prevent fileless attacks	60%
Cross-operating system protection (not just Windows)	49%
Minimize false positives	61%
Domain agnostic and can be inserted on mobile devices, endpoints and servers	60%
Ability to prevent zero-day attacks	62%
Other (please specify)	5%
Total	486%

Q32a. Did your organization have a phishing attack in the past year?	Pct%
Yes	79%
No (Skip to 33a)	21%
Total	100%

Q32b. If yes, in what stage of the cybersecurity lifecycle were you able to deal with the attack?	Pct%
Prevention	18%
Detection	20%
Containment	30%
Recovery	20%
Remediation	12%
Total	100%

Q32c. Please estimate the total cost incurred by your company as a result of this phishing attack.	Pct%
Less than $50,000	12%
$50,000 to $100,000	30%
$100,001 to $500,000	34%
$500,001 to $1,000,000	12%
$1,000,000 to $5,000,000	9%
$5,000,001 to $10,000,000	3%
More than $10,000,000	1%
Total	101%
Extrapolated value	$ 832,500

Q32d. Please estimate the cost savings if your organization prevented the phishing attack.	Pct%
Less than $50,000	31%
$50,000 to $100,000	36%
$100,001 to $500,000	18%
$500,001 to $1,000,000	15%
$1,000,001 to $5,000,000	0%
More than $5,000,000	0%
Total	100%
Extrapolated value	$ 201,250

Q33a. Did your organization have a zero-day attack in the past year?	Pct%
Yes	52%
No (skip to Q34a)	48%
Total	100%

Q33b. If yes, in what stage of the cybersecurity lifecycle were you able to deal with the zero-day attack?	Pct%
Prevention	12%
Detection	15%
Containment	42%
Recovery	21%
Remediation	10%
Total	100%

Q33c. Please estimate the total cost incurred by your company as a result of this zero-day attack.	Pct%
Less than $50,000	5%
$50,000 to $100,000	17%
$100,001 to $500,000	23%
$500,001 to $1,000,000	32%
$1,000,000 to $5,000,000	19%
$5,000,001 to $10,000,000	3%
More than $10,000,000	1%
Total	100%
Extrapolated value	$ 1,238,000

Q33d. Please estimate the cost savings if your organization prevented the zero-day attack.	Pct%
Less than $50,000	13%
$50,000 to $100,000	23%
$100,001 to $500,000	29%
$500,001 to $1,000,000	25%
$1,000,001 to $5,000,000	4%
More than $5,000,000	6%
Total	100%
Extrapolated value	$ 775,000

Q34a. Did your organization have a spyware attack in the past year?	Pct%
Yes	37%
No (skip to Q35a)	63%
Total	100%

Q34b. If yes, in what stage of the cybersecurity lifecycle were you able to deal with the spyware attack?	Pct%
Prevention	26%
Detection	29%
Containment	20%
Recovery	13%
Remediation	12%
Total	100%

Q34c. Please estimate the total cost incurred by your company as a result of this spyware attack.	Pct%
Less than $50,000	18%
$50,000 to $100,000	30%
$100,001 to $500,000	29%
$500,001 to $1,000,000	11%
$1,000,000 to $5,000,000	9%
$5,000,001 to $10,000,000	3%
More than $10,000,000	0%
Total	100%
Extrapolated value	$ 691,500

Q34d. Please estimate the cost savings if your organization prevented the spyware attack.	Pct%
Less than $50,000	21%
$50,000 to $100,000	40%
$100,001 to $500,000	33%
$500,001 to $1,000,000	6%
$1,000,001 to $5,000,000	0%
More than $5,000,000	0%
Total	100%
Extrapolated value	$ 179,250

Q35a. Did your organization have a ransomware attack in the past year?	Pct%
Yes	23%
No (skip to 36a)	77%
Total	100%

Q35b. If yes, in what stage of the cybersecurity lifecycle were you able to deal with the ransomware attack?	Pct%
Prevention	10%
Detection	23%
Containment	35%
Recovery	17%
Remediation	15%
Total	100%

Q35c. Please estimate the total cost incurred by your company as a result of this attack.	Pct%
Less than $50,000	20%
$50,000 to $100,000	25%
$100,001 to $500,000	34%
$500,001 to $1,000,000	16%
$1,000,000 to $5,000,000	4%
$5,000,001 to $10,000,000	1%
More than $10,000,000	0%
Total	100%
Extrapolated value	$ 440,750

Q35d. Please estimate the cost savings if your organization prevented the ransomware attack.	Pct%
Less than $50,000	19%
$50,000 to $100,000	42%
$100,001 to $500,000	31%
$500,001 to $1,000,000	8%
$1,000,001 to $5,000,000	0%
More than $5,000,000	0%
Total	100%
Extrapolated value	$ 189,250

Q36a. Did your organization have a nation-state attack in the past year?	Pct%
Yes	18%
No (skip to Q37)	82%
Total	100%

Q36b. If yes, in what stage of the cybersecurity lifecycle were you able to deal with the nation-state attack?	Pct%
Prevention	9%
Detection	19%
Containment	29%
Recovery	23%
Remediation	20%
Total	100%

Q36c. Please estimate the total cost incurred by your company as a result of this nation-state attack.	Pct%
Less than $50,000	0%
$50,000 to $100,000	8%
$100,001 to $500,000	21%
$500,001 to $1,000,000	41%
$1,000,000 to $5,000,000	26%
$5,000,001 to $10,000,000	3%
More than $10,000,000	1%
Total	100%
Extrapolated value	$ 1,501,500

Q36d. Please estimate the cost savings if your organization prevented the ransomware attack.	Pct%
Less than $50,000	2%
$50,000 to $100,000	14%
$100,001 to $500,000	37%
$500,001 to $1,000,000	26%
$1,000,001 to $5,000,000	18%
More than $5,000,000	3%
Total	100%
Extrapolated value	$ 1,037,000

Part 5. The Cyber Kill Chain and zero-day attacks

Q37. How familiar are you with the term Cyber Kill Chain?	Pct%
Very familiar	32%
Familiar	36%
Not familiar	17%
No knowledge (Skip to Part 6)	15%
Total	100%

Q38a. How important is the Cyber Kill Chain framework for preventing a zero-day attack? 1 = not important to 10 = very important.	Pct%
1 or 2	5%
3 or 4	9%
5 or 6	18%
7 or 8	33%
9 or 10	35%
Total	100%
Extrapolated value	7.18

Q38b. In your opinion, how difficult is it to prevent a zero-day attack during the Reconnaissance phase of the kill chain? 1 = not difficult to 10 = very difficult.	Pct%
1 or 2	5%
3 or 4	6%
5 or 6	18%
7 or 8	31%
9 or 10	40%
Total	100%
Extrapolated value	7.40

Q38c. In your opinion, how difficult is it to prevent a zero-day attack in the Weaponization phase of the kill chain? 1 = not difficult to 10 = very difficult	Pct%
1 or 2	3%
3 or 4	6%
5 or 6	17%
7 or 8	30%
9 or 10	44%
Total	100%
Extrapolated value	7.62

Q38d. In your opinion, how difficult is it to prevent a zero-day attack during the Delivery phase of the kill chain? 1 = not difficult to 10 = very difficult	Pct%
1 or 2	1%
3 or 4	5%
5 or 6	16%
7 or 8	37%
9 or 10	41%
Total	100%
Extrapolated value	7.74

Q38e. In your opinion, how difficult is it to prevent a zero-day attack during the Exploitation phase of the kill chain? 1 = not difficult to 10 = very difficult	Pct%
1 or 2	7%
3 or 4	8%
5 or 6	12%
7 or 8	29%
9 or 10	44%
Total	100%
Extrapolated value	7.40

Q38f. In your opinion, how difficult is it to prevent a zero-day attack cyberattacks during the Installation phase of the kill chain? 1 = not difficult to 10 = very difficult	Pct%
1 or 2	4%
3 or 4	11%
5 or 6	12%
7 or 8	29%
9 or 10	44%
Total	100%
Extrapolated value	7.46

Q38g. In your opinion, how difficult is it to prevent a zero-day attack during the C2 phase of the kill chain? 1 = not difficult to 10 = very difficult	Pct%
1 or 2	3%
3 or 4	5%
5 or 6	12%
7 or 8	41%
9 or 10	39%
Total	100%
Extrapolated value	7.66

Q38h. In your opinion, how difficult is it to prevent a zero-day attack during the Actions on Objectives phase of the kill chain? 1 = not difficult to 10 = very difficult	Pct%
1 or 2	2%
3 or 4	6%
5 or 6	16%
7 or 8	30%
9 or 10	46%
Total	100%
Extrapolated value	7.74

Part 6. Demographics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	3%
Vice President	5%
Director	17%
Manager	21%
Supervisor	15%
Technician	33%
Staff / Analyst	5%
Contractor	1%
Other	0%
Total	100%

D2. What best describes your primary role in the organization?	Pct%
Application security	12%
Security architecture	8%
IT management	24%
SOC management	21%
Quality assurance	6%
Compliance/audit	6%
Risk management	8%
Security engineering	13%
Other	2%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct%
Agriculture & food services	1%
Communications	3%
Consumer goods	6%
Defense & aerospace	1%
Energy & utilities	7%
Entertainment & media	2%
Financial services	18%
Health & pharmaceuticals	10%
Hospitality	2%
Industrial & manufacturing	10%
Public sector	11%
Retail	8%
Services	10%
Technology & software	8%
Transportation	2%
Other	1%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
Less than 100 employees	11%
100 to 500 employees	10%
501 to 1,000 employees	15%
1,001 to 5,000 employees	20%
5,001 to 25,000 employees	18%
25,001 to 75,000 employees	18%
More than 75,000 employees	8%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

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.