A Market Study on Cybersecurity Service Offerings

Sponsored by

Microsoft

Independently conducted by Ponemon Institute LLC

Publication Date: December 2018

Market Study on Cybersecurity Service Offerings

Ponemon Institute, December 2018

Part 1. Introduction

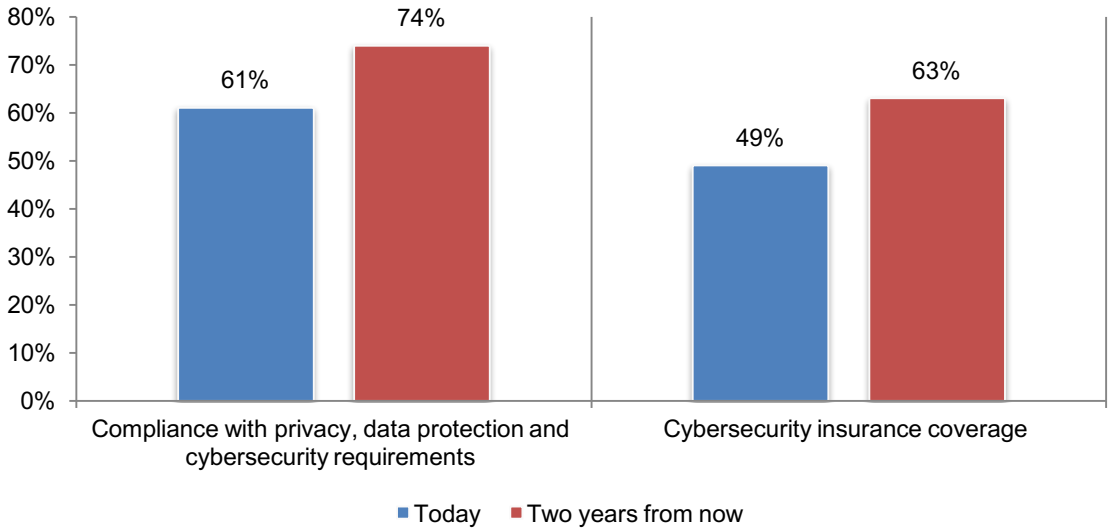
Ponemon Institute is pleased to present the results of a research study on the importance of specific cybersecurity services and technologies to a strong security posture. Sponsored by Microsoft, we surveyed 602 IT and IT security practitioners who are involved in the development of their organizations' cybersecurity strategies. The goal of the research is to understand what organizations are doing to improve their security posture and what will be the most important cybersecurity service offerings over the next two years.

According to the findings, over the next two years an organization's security posture will become more dependent on its ability to achieve compliance with privacy, data protection and cybersecurity requirements. In addition, the purchase of cybersecurity insurance to manage the financial consequences of security exploits will also become more essential.

As shown in Figure 1, 61 percent of respondents say compliance is important today and 74 percent of respondents say it will become essential in the next two years. Today, less than half (49 percent of respondents) say the purchase of cyber insurance to manage the financial consequences of security exploits is important. However, 63 percent of respondents say cybersecurity insurance will become essential.

Figure 1. The importance of compliance with regulations and cyber insurance to a strong security posture today and two years from now

Essential and very important responses combined



To support a stronger security posture, respondents believe the following are cybersecurity technologies' most essential capabilities.

- Ability to locate and control sensitives or confidential data, including unstructured data
- Ability to control the growth and proliferation of unstructured data assets
- Ability to control endpoints and mobile connections, including IoT devices
- Ability to prioritize threats and vulnerabilities

According to the findings, following are the changes in risk, cybersecurity services and technologies expected in the next two years.

- The disruptive technologies most likely to put organizations at risk over the next two years are the use of cloud-based sharing and document collaboration tools, IoT devices and use of blockchain methods.
- The importance of orchestration, automation and machine learning will increase significantly over the next two years.
- The use of artificial intelligence and machine learning will more than double in the next two years.
- Organizations will increase their use of managed security service providers (MSSPs) significantly mainly to monitor or manage firewalls or intrusion prevention systems (IPS)
- Multi-cloud strategies are defined as the use of multiple cloud computing and storage services in a heterogeneous architecture and many organizations are making this a priority.
- More of the IT security budget will be allocated to the application, endpoint and data layers over the next two years. Investments in technologies for the network and operations layer will decline.

Part 2. Key findings

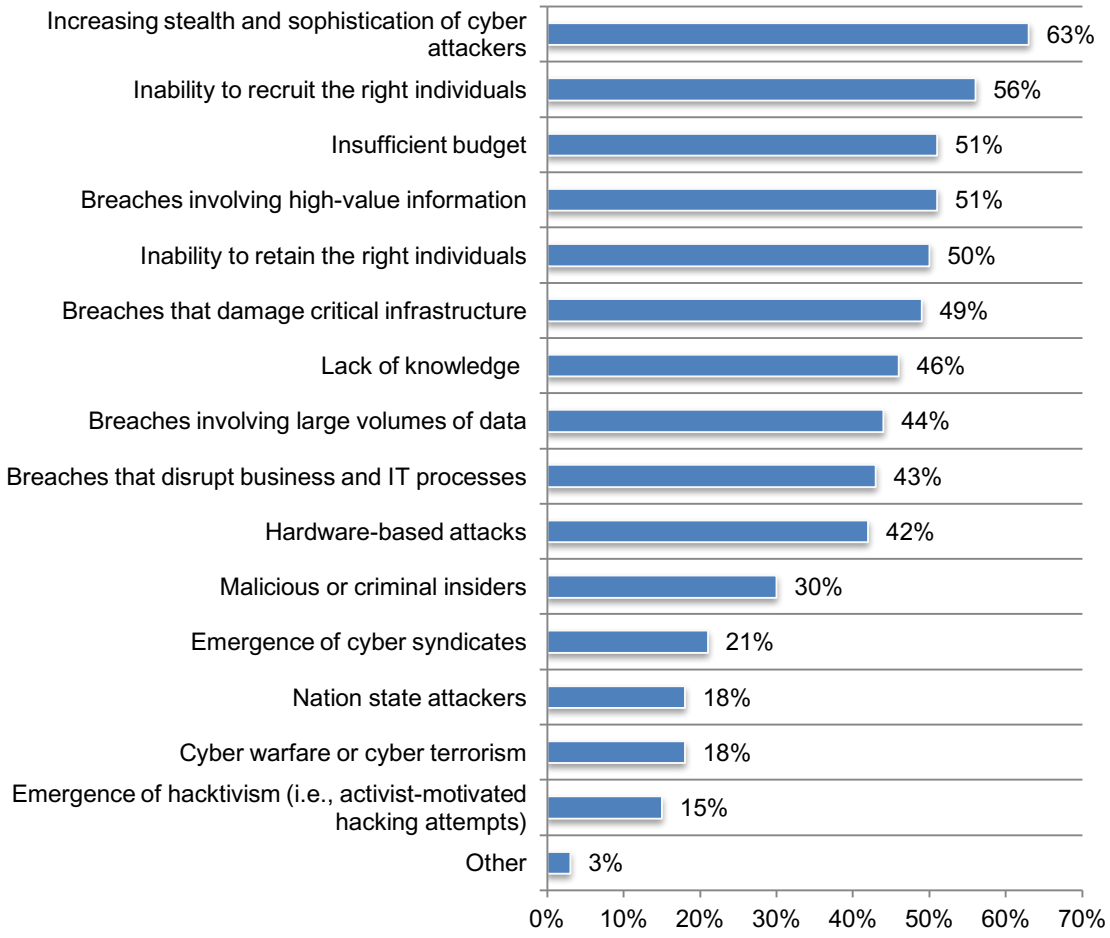
In this section, we analyze the findings of research. The complete audited findings are presented in the Appendix of this report. We have organized the findings according to the following topics.

- Challenges & risks to cybersecurity posture
- Technologies and services that support a strong cybersecurity posture
- Trends in cloud services
- Budget and investments

Challenges & risks to cybersecurity posture

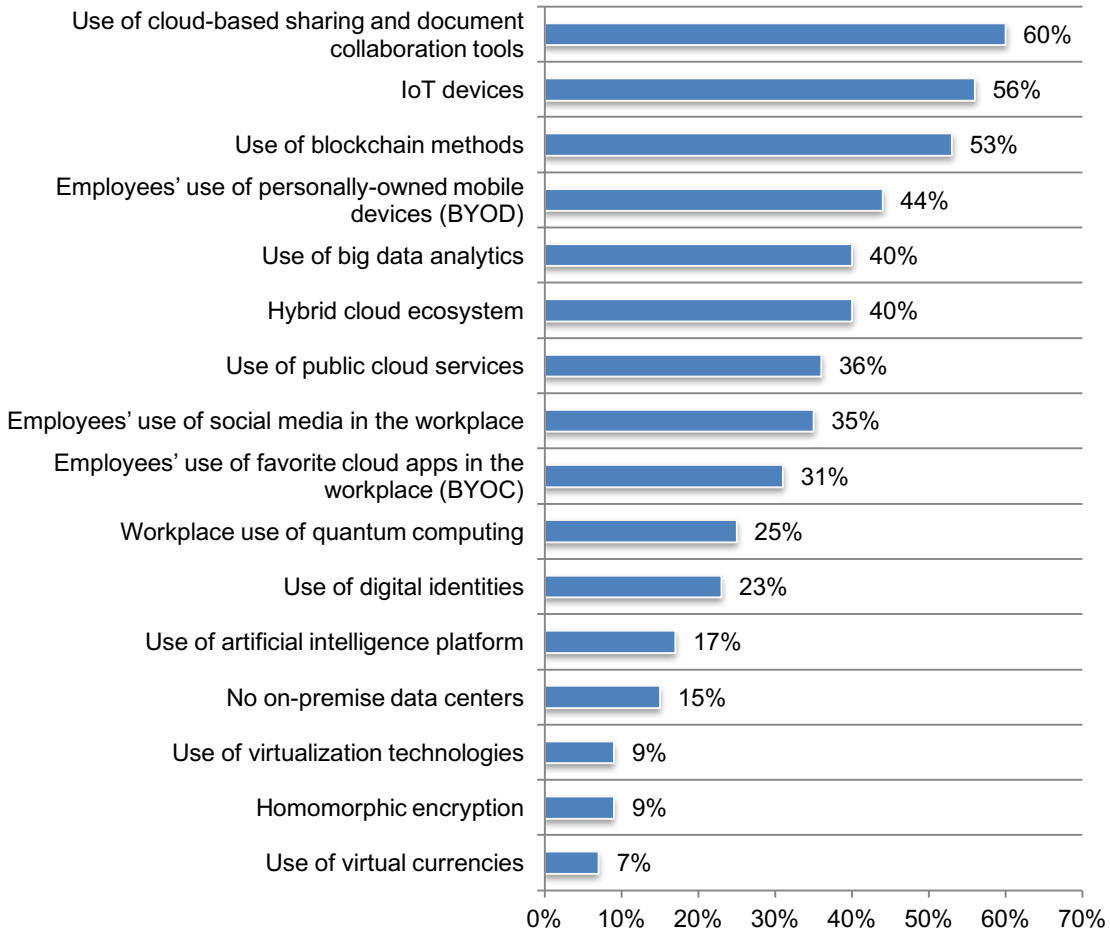
Organizations struggle to deal with the increasing stealth and sophistication of cyber attackers. According to 63 percent of respondents, their organizations face the challenge of understanding how to keep ahead of attackers. The difficulty is compounded by the inability to recruit the right individuals and having enough budget (56 percent and 51 percent of respondents, respectively.

Figure 2. What are the main cybersecurity challenges will your organization face in the next two years?
Six responses permitted



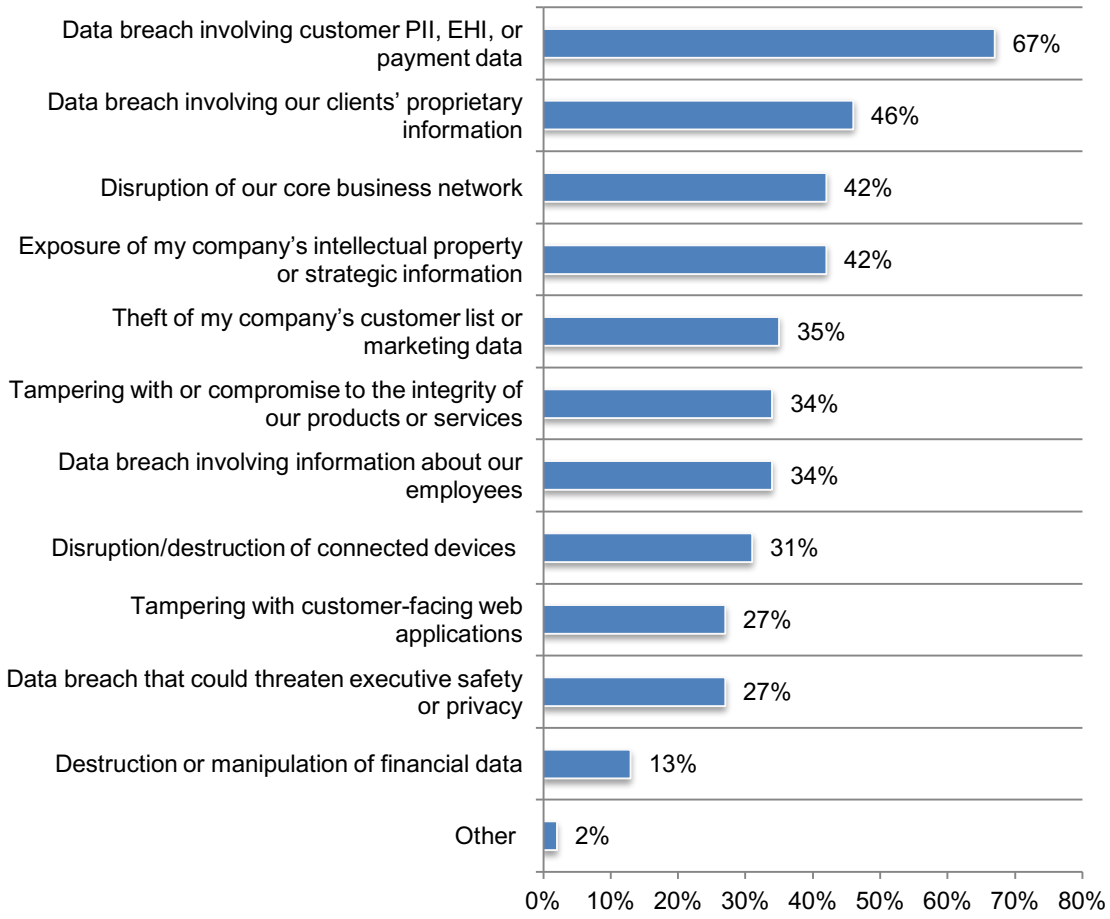
The most disruptive technologies that put organizations at risk are cloud-based sharing and document collaboration tools and IoT devices. Figure 3 presents a list of 16 disruptive technologies that if not properly secured could pose a risk to organizations. Sixty percent of respondents say the commonly used cloud-based sharing and document collaboration tools and 56 percent of respondents say IoT devices are the disruptive technologies that could put their organizations at risk. Fifty-three percent of respondents are concerned about risks associated with the use of blockchain methods

Figure 3. What disruptive technologies will put your organization at risk over the next two years?
Five responses permitted



Data breaches pose the greatest risk to business. Respondents are aware of the devastating financial consequences when individuals' sensitive and confidential information is breached. As shown in Figure 4, 67 percent of respondents say they are most concerned about how a data breach involving customer PII, EHI or payment data would affect an organization's ability to be successful. This is followed by a data breach involving clients' proprietary information (46 percent of respondents).

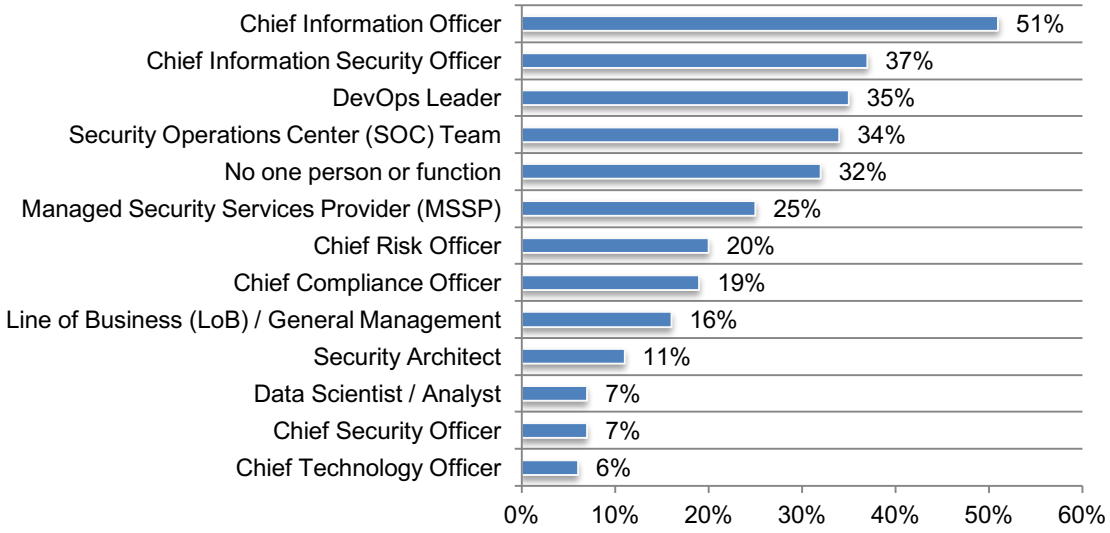
Figure 4. What types of cyberattacks pose the greatest risk to your business over the next two years?
Four responses permitted



Technologies and services that support a strong cybersecurity posture

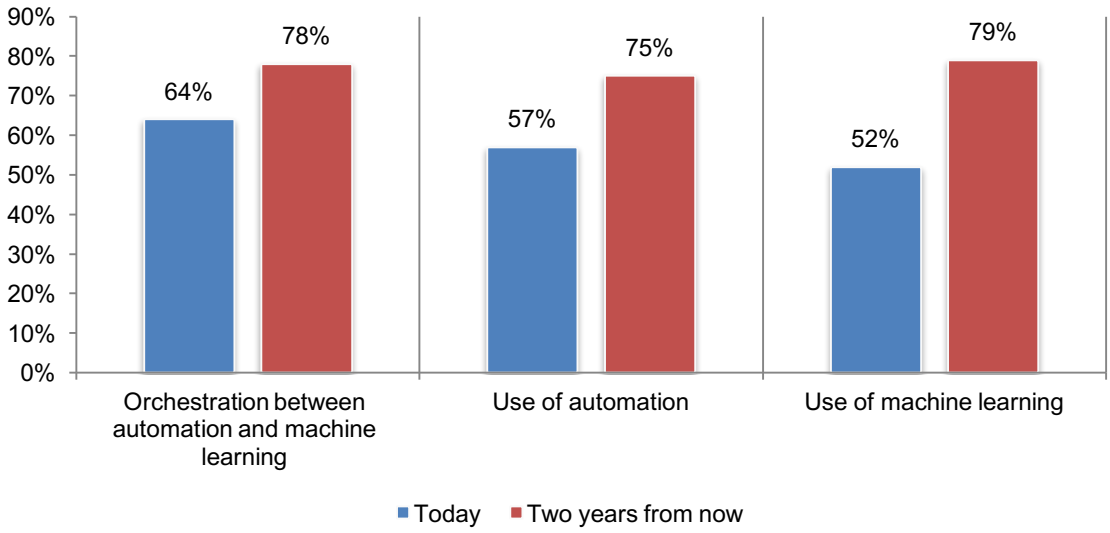
The CIO is most likely to influence the use of cybersecurity technologies. Figure 5 lists various functions that may have some influence in determining the investment in cybersecurity technologies. Fifty-one percent of respondents say the chief information officer has the most influence. However, 32 percent of respondents say no one person or function is influential.

Figure 5. Who are the key influencers in setting your organization's use of cybersecurity technologies?
Three responses permitted



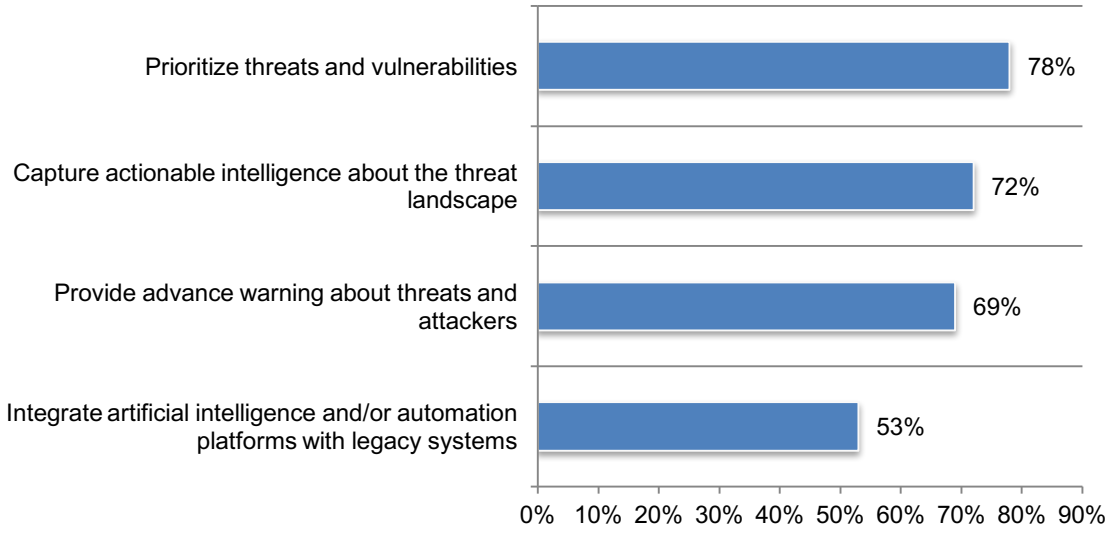
The use of orchestration, automation and machine learning will increase in importance. As shown in Figure 6, while the importance of orchestration and automation will increase significantly, the importance of machine learning increases the most from 52 percent of respondents who say it is important today to 79 percent of respondents who say it will be essential two years from now.

Figure 6. The importance of automation today and two years from now
Essential and very important responses combined



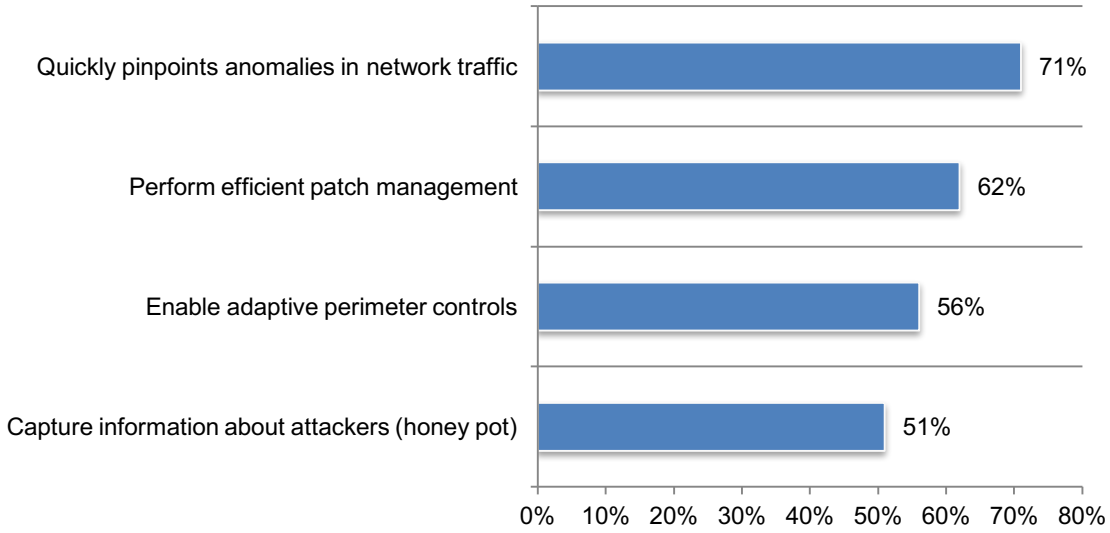
The ability to prioritize threat intelligence and vulnerabilities is critical. Respondents were asked to rate the ability of cybersecurity technologies to help their organizations deal with attacks on a scale 1 = low ability to 10 = high ability. Figure 7 shows the 7+ (very high) responses. The most important is the ability to prioritize threats and vulnerabilities (78 percent of respondents) followed by 72 percent of respondents who say the ability to capture actionable intelligence about the threat landscape.

Figure 7. The most important threat intelligence features in cybersecurity technologies
1 = low to 10 = high ability, 7+ responses presented



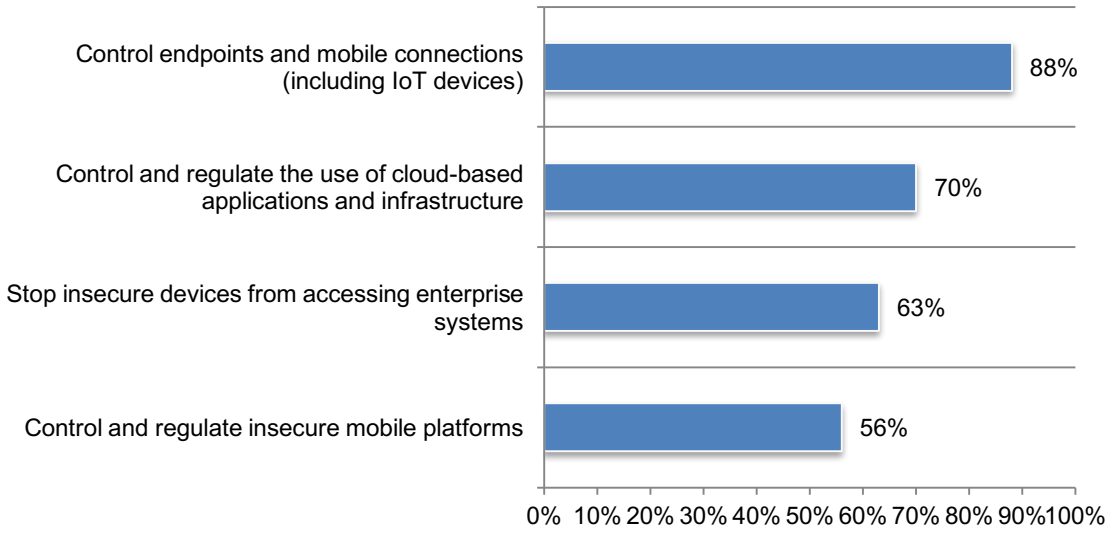
When asked to rank the importance of the ability to prevent cyberattacks on a scale of 1 = low ability to 10 = high ability, 71 percent of respondents say the ability to quickly pinpoint anomalies in network traffic and 62 percent of respondents say the ability to perform efficient patch management is very important.

Figure 8. Features important to preventing cyberattacks
1 = low to 10 = high ability, 7+ responses presented



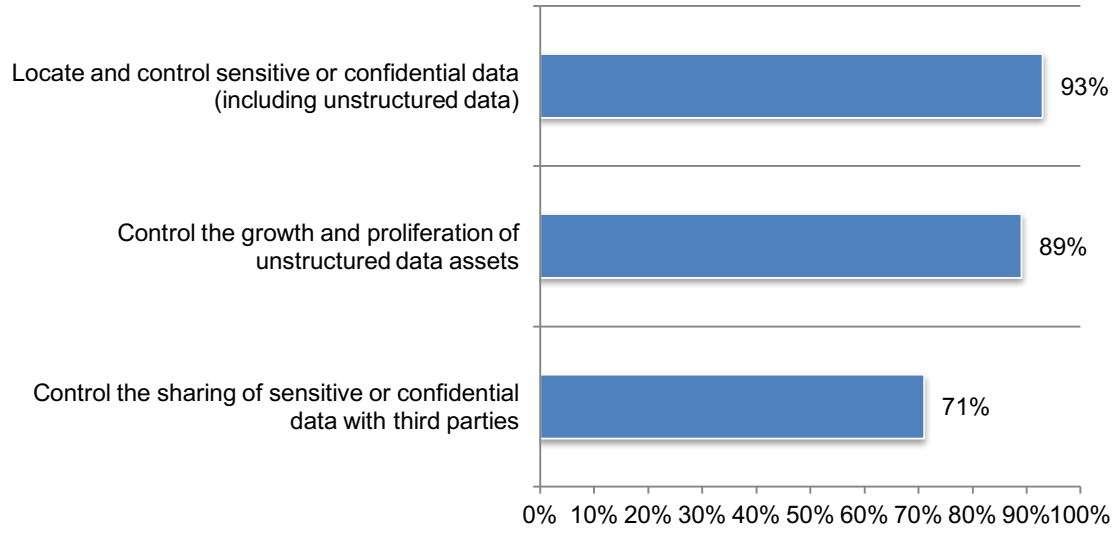
The ability to control endpoints and mobile connections, including IoT devices, is essential. As discussed previously, IoT devices and cloud-based sharing and collaboration technologies are the disruptive technologies that are most likely to put organizations at risk. As shown in Figure 9, 88 percent of respondents rate the ability to control endpoints and mobile connections as very important and 70 percent of respondents say the ability to control and regulate the use of cloud-based applications and infrastructure as essential or very important.

Figure 9. Features important to prevent attacks due to unsecured devices
1 = low to 10 = high ability, 7+ responses presented



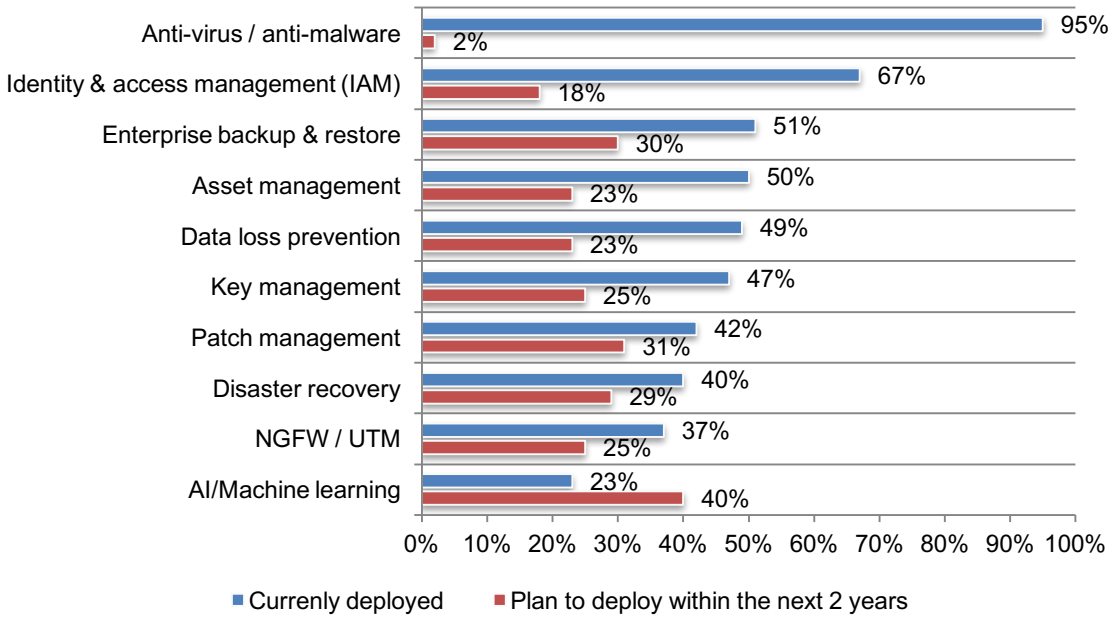
The most important feature in cyber technologies is the ability to locate and control sensitive or confidential data, including unstructured data. As discussed previously, data breaches involving individuals' sensitive or confidential data pose the greatest risk to organizations. Accordingly, 93 percent of respondents say the ability to locate and control sensitive or confidential data, including unstructured data, is the most critical feature for all cyber technologies listed in this research. Eighty-nine percent of respondents say it is to control the growth and proliferation of unstructured data assets and 71 percent of respondents say it is to reduce the risk of sharing sensitive or confidential with third parties.

Figure 10. Features important to securing data
1 = low to 10 = high ability, 7+ responses presented



The use of artificial intelligence and machine learning will more than double in the next two years. According to Figure 11, while only 23 percent of respondents say they have deployed AI/machine learning, 40 percent say they plan to deploy these technologies in the next two years. The use of patch management will be deployed by close to one-third of respondents (31 percent). Virtually all companies have anti-virus/anti-malware solutions (95 percent of respondents) so deployment over the next two years is very low.

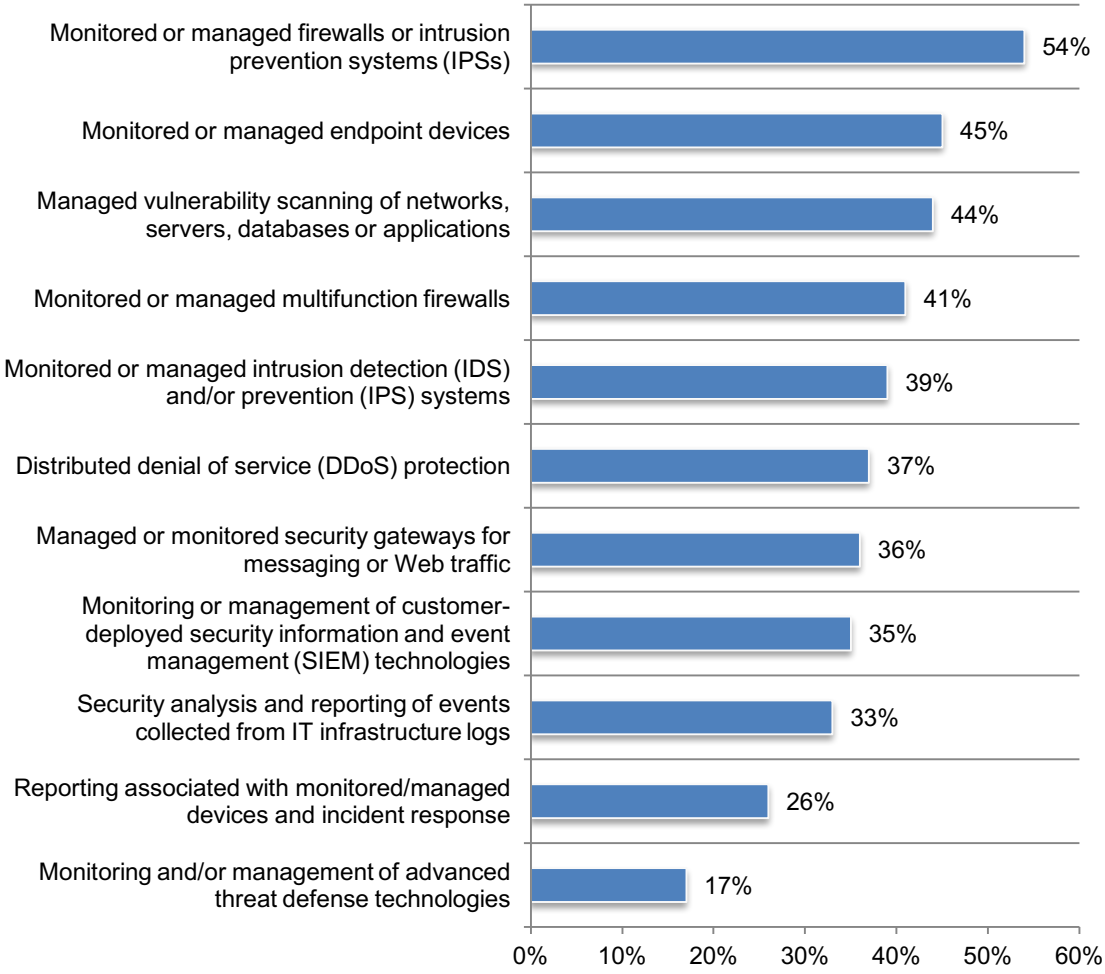
Figure 11. Technologies currently deployed or plan to deploy
More than one response permitted



Organizations will increase their use of managed security service providers (MSSPs) over the next two years. Today, an average of 23 percent of organizations' IT security operations are supported by MSSPs and in two years will almost double to an average of 40 percent. Figure 12 lists 11 core MSSP services provided to organizations.

Fifty-four percent of respondents say they engage MSSPs to monitor or manage firewalls or intrusion prevention systems and 45 percent say it is to monitor or manage endpoint devices.

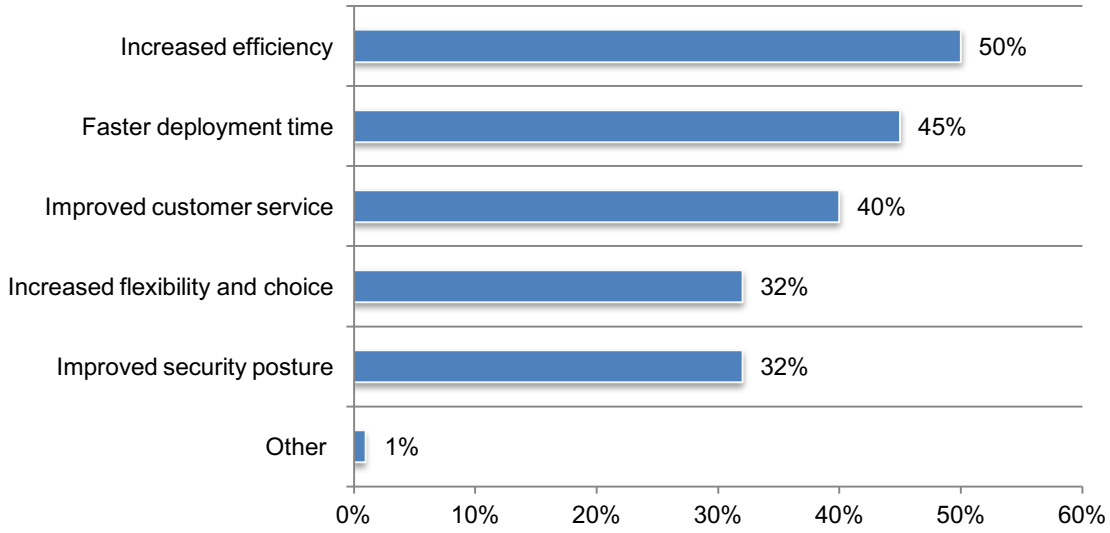
Figure 12. MSSP services provided to support organization's IT security posture



Cloud services

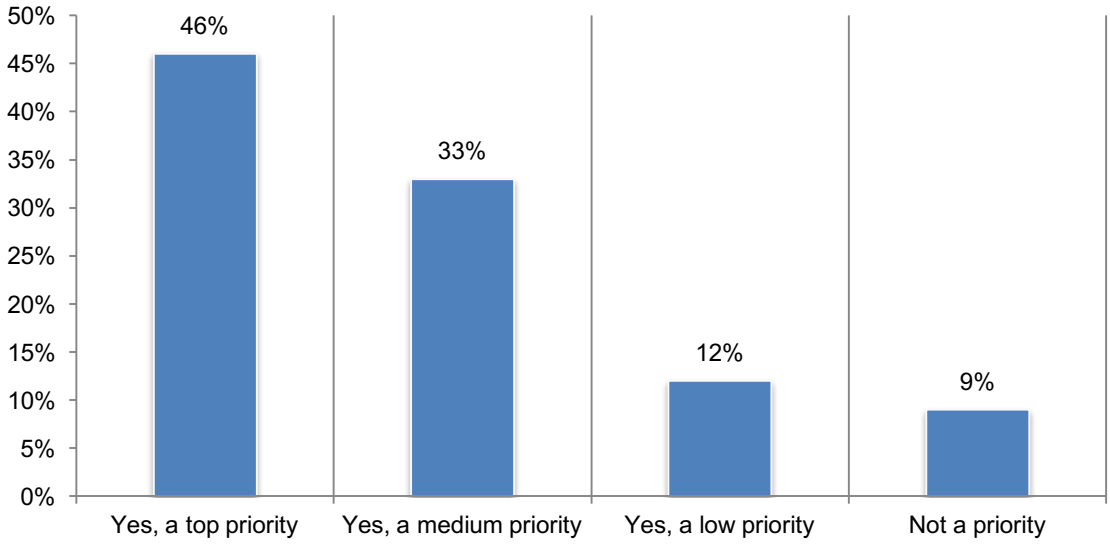
Organizations would pay more for increased efficiency and faster deployment in the cloud. Seventy-three percent of respondents say their organizations have deployed an application into production on a public cloud in the last 12 months. According to Figure 13, 50 percent of respondents say they would pay a premium to have increased efficiency and 45 percent say their organizations would pay a premium for faster deployment time. Less than one-third of respondents say their organizations would pay a premium for an enhanced security posture.

Figure 13. What cloud services would you be willing to pay a premium for?
Two responses permitted



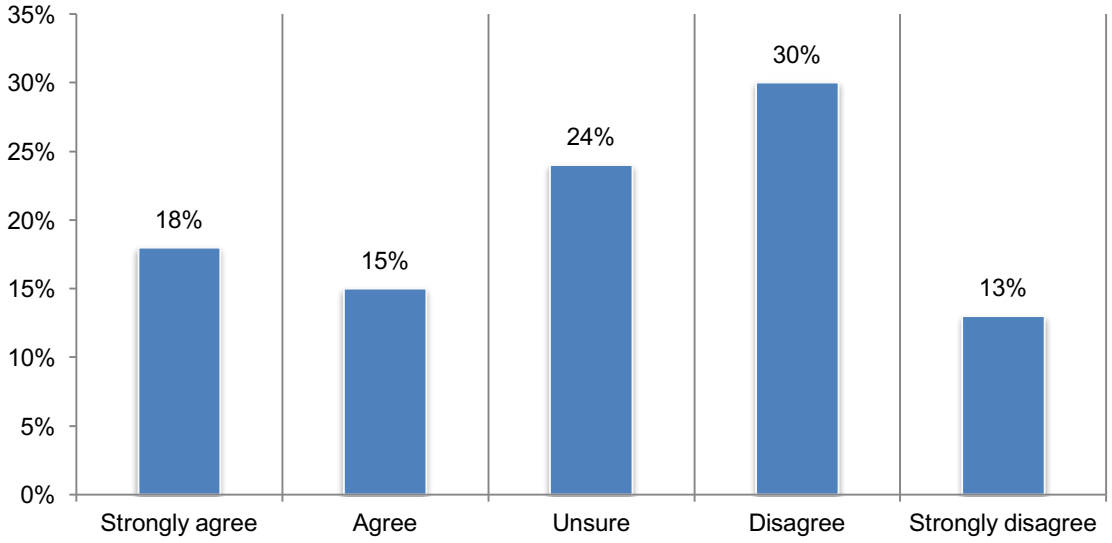
Multi-cloud strategies are a priority. In this study, we define a multi-cloud strategy as the use of multiple cloud computing and storage services in a heterogeneous architecture. According to Figure 14, 79 percent of respondents (46 percent + 33 percent) say such a strategy is a top or medium priority for their organizations.

Figure 14. Is multi-cloud strategy a priority for your organization?



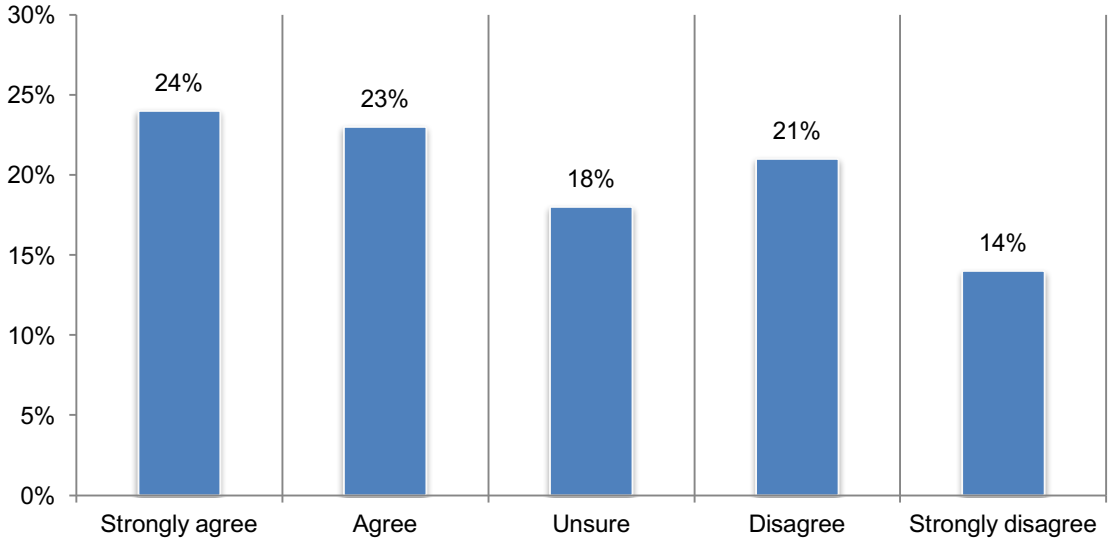
Data processing on-premises is considered more secure. According to Figure 15, only one-third of respondents agree that cloud services provide a more secure data processing environment than on-premises. Despite concerns, critical security-related workloads will increase in the cloud. An average of 35 percent of organizations' critical security-related workloads in the cloud today and this will increase to more than half (52 percent) in the next two years.

Figure 15. In my organization, cloud services provide a more secure data processing environment than on-premises



Almost half (47 percent of respondents) say vendor consolidation is a higher priority than investing in best-of-breed, as shown in Figure 16.

Figure 16. Vendor consolidation is a higher priority than investing in best-of-breed
Investments and budget for enabling security technologies



Budget and investments

On average, organizations have spent more than $198 million on all IT technologies in the current fiscal year and 20 percent of these technologies is dedicated to IT security or cyber security.

Table 1 shows how the budget is allocated today and will be allocated in two years. Respondents were asked to allocate a total of 100 points for the five categories. In the next two years, more budget will be allocated to the application layer, endpoint layer and data layer.

Table 1. Allocation of budget today and in two years	Budget today	Budget two years from today
Network layer	31	25
Application layer	23	25
Endpoint layer	18	21
Data layer	13	16
Operations layer	15	13

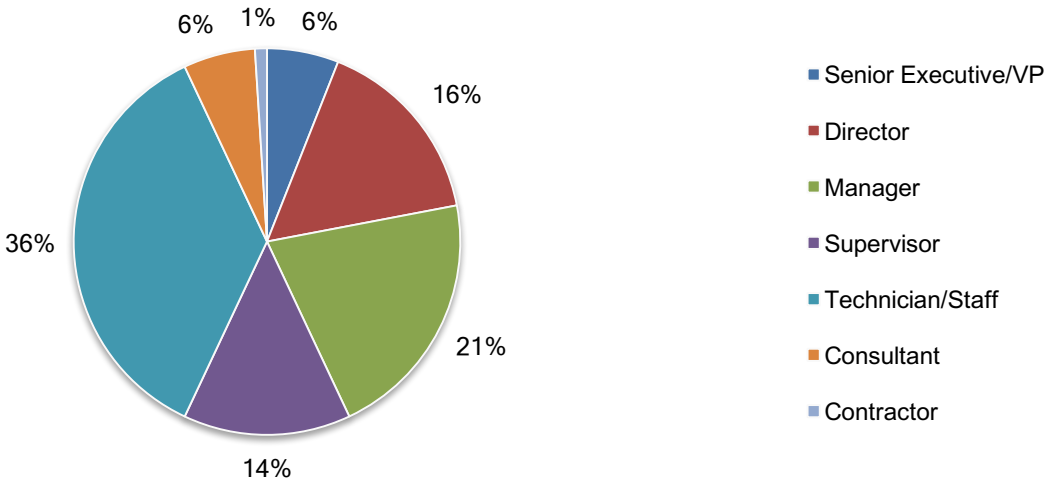
Part 3. Methods

The sampling frame is composed of 17,898 IT and IT security practitioners in the United States. As shown in Table 2, 691 respondents completed the survey. Screening removed 89 surveys. The final sample was 602 surveys (or a 3.4 percent response rate).

Table 2. Sample response	Freq	Pct%
Total sampling frame	17,898	100.0%
Total returns	691	3.9%
Rejected or screened surveys	89	0.5%
Final sample	602	3.4%

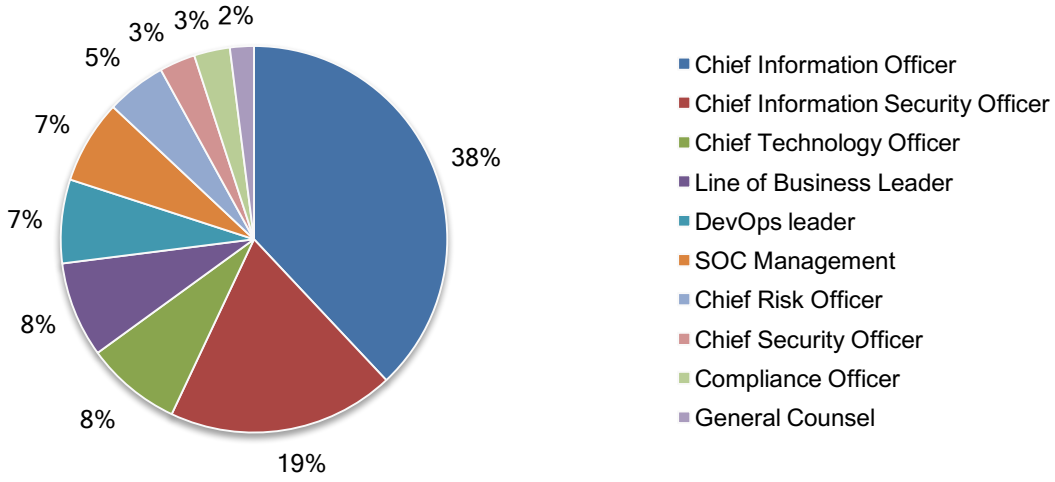
Pie Chart 1 reports the current position or organizational level of the respondents. Fifty-seven percent of respondents reported their current position as supervisory or above and 36 percent of respondents reported their position is at the technician/staff level.

Pie Chart 1. Distribution of respondents according to position level



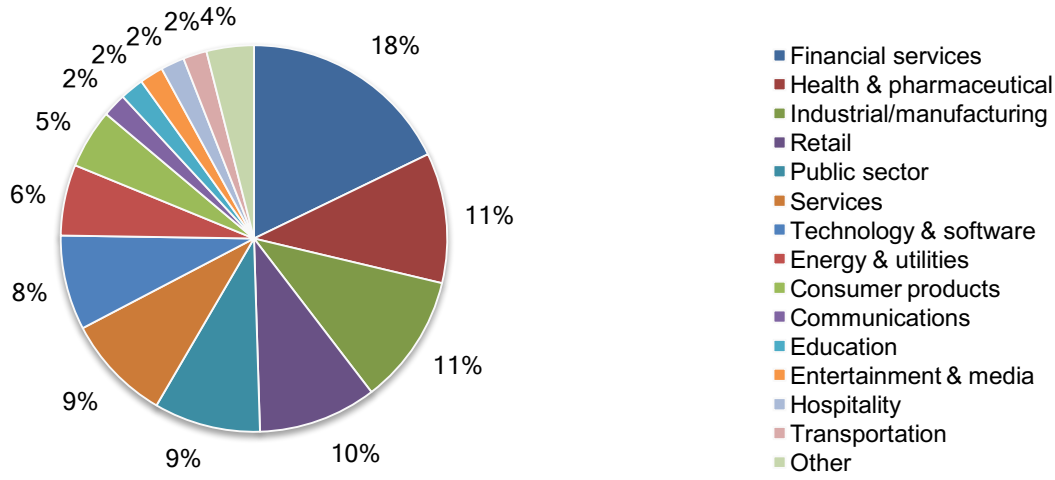
Pie Chart 2 identifies the primary person to whom the respondent or their leader reports. Thirty-eight percent of respondents identified the chief information officer as the person to whom they report. Another 19 percent indicated they report directly to the chief information security officer, 8 percent of respondents report to the chief technology officer and 8 percent of respondents report to a line of business leader.

Pie Chart 2. Distribution of respondents according to reporting channel



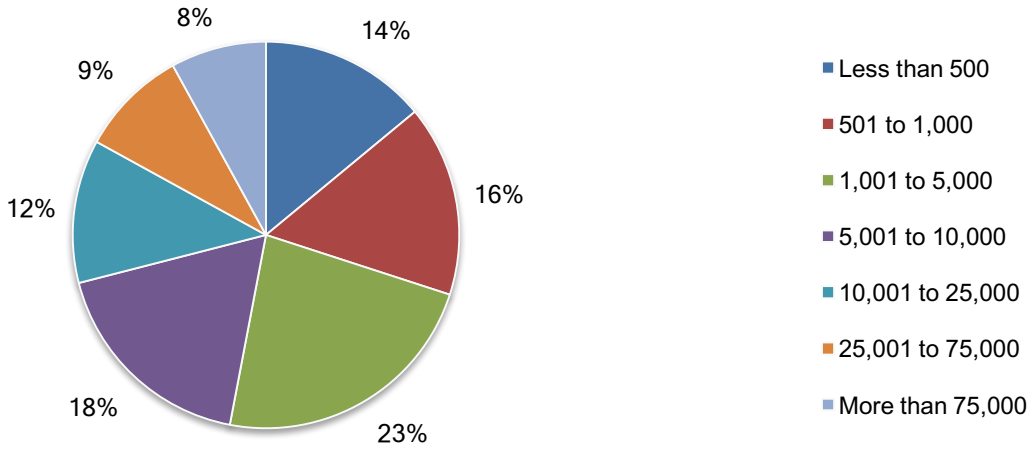
Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, followed by health and pharmaceuticals (11 percent of respondents), industrial and manufacturing (11 percent of respondents), retail sector (10 percent of respondents), public sector (9 percent of respondents) and services sector (9 percent of respondents).

Pie chart 3. Distribution of respondents according to primary industry classification



According to Pie Chart 4, 53 percent of respondents are from organizations with a global full-time headcount of more than 1,000 employees.

Pie Chart 4. Distribution of respondents according to the full-time headcount of the global organization



Part 4. Caveats

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

Non-response bias: The current findings are based on 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 IT or IT security practitioners in the United States. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

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

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between September 20 2018 and October 1, 2018.

Survey response	Freq
Total sampling frame	17,898
Total returns	691
Rejected survey	89
Final sample	602

Part 1. Screening

S1. How involved are you in the development of your organization's cybersecurity strategies?	Pct%
Very involved	30%
Involved	45%
Somewhat involved	25%
Not involved (stop)	0%
Total	100%

S2. How involved are you in your organization's selection and evaluation of security technologies?	Pct%
Very involved	40%
Involved	38%
Somewhat involved	22%
Not involved (stop)	0%
Total	100%

S3. What activities best define your role within the cybersecurity function within your organization? Please check all that apply.	Pct%
Managing budgets	40%
Recruiting personnel	41%
Leading IT security team	38%
Evaluating technologies	50%
Setting strategies	27%
Implementing tactics	38%
Influencing strategy and investments in technologies	19%
None of the above (stop)	0%
Total	253%

Part 2. The future of cybersecurity service offerings

Q1a. **Today,** how important is compliance with privacy, data protection and cybersecurity requirements in determining a strong security posture?	Pct%
Essential	30%
Very important	31%
Important	24%
Not important	12%
Irrelevant	3%
Total	100%

Q1b. **Two years from now**, how important will compliance with privacy, data protection and cybersecurity requirements be in determining a strong security posture?	Pct%
Essential	40%
Very important	34%
Important	18%
Not important	8%
Irrelevant	0%
Total	100%

Q2a. **Today,** how important is cybersecurity insurance coverage in ensuring a strong security posture?	Pct%
Essential	25%
Very important	24%
Important	26%
Not important	18%
Irrelevant	7%
Total	100%

Q2b. **Two years from now**, how important will cybersecurity insurance be in determining a strong security posture?	Pct%
Essential	33%
Very important	30%
Important	25%
Not important	9%
Irrelevant	3%
Total	100%

Q3. Following are 38 security technology categories. Which technology does your organization currently deploy or plan to deploy over the next 24 months? Please use the following legend: 1=currently deployed, 2=plan to deploy (within the next two years) and 3=no plan to use.	Currently deployed	Plan to deploy within the next 2 years	No plan to deploy
AI/Machine learning	23%	40%	37%
Anti-phishing	43%	26%	31%
Anti-virus / anti-malware	95%	2%	3%
Asset management	50%	23%	27%
Automated policy management	26%	13%	61%
Big data analytics	27%	18%	55%
Business continuity management (BCM)	33%	20%	47%
Containerization	30%	32%	38%
Disaster recovery	40%	29%	31%
Data loss prevention	49%	23%	28%
EDGE Computing	14%	15%	71%
Endpoint detection & response (EDR)	36%	24%	40%
Enterprise backup & restore	51%	30%	19%
Enterprise encryption solutions	50%	24%	26%
GRC / risk management	39%	13%	48%
Hardware supply chain security	21%	24%	55%
Hardware security modules	35%	19%	46%
Identity & access management (IAM)	67%	18%	15%
Industrial controls/SCADA	29%	16%	55%
IoT/Industrial IoT controls	16%	15%	69%
Key management	47%	25%	28%
Isolation & sandboxing tools	32%	23%	45%
Malware & reverse engineering	29%	14%	57%
MCU (Azure Sphere)	11%	23%	66%
Micro-segmentation	30%	32%	38%
NGFW / UTM	37%	25%	38%
Patch management	42%	31%	27%
Physical security / credential systems	40%	12%	48%
Public key infrastructure (PKI)	38%	18%	44%
SAST/DAST (static testing/dynamic testing)	35%	23%	42%
Security incident & event management	42%	21%	37%
Security, operations, analytics and reporting	20%	22%	58%
Switches (including sensors)	26%	17%	57%
Threat Intelligence / sharing	32%	28%	40%
Threat modeling / Threat hunting	28%	26%	46%
UEBA	30%	36%	34%
UEM (MDM / MAM)	37%	29%	34%
WAF	42%	20%	38%

Q4a. **Today**, what percentage of your organization's IT security operations are supported by managed security service providers (MSSPs)?	Pct%
None	40%
Less than 10%	13%
10% to 25%	11%
26% to 50%	16%
51% to 75%	12%
76% to 100%	8%
Total	100%
Extrapolated value	23%

Q4b. What percentage of your organization's IT security operations will be supported by managed security service providers (MSSPs) **2 years from now**?	Pct%
None	19%
Less than 10%	7%
10% to 25%	21%
26% to 50%	12%
51% to 75%	16%
76% to 100%	25%
Total	100%
Extrapolated value	40%

Q5. Following are core services typically provided by MSSPs. Please check all services provided by MSSPs to support your organization's IT security posture.	Pct%
Monitored or managed firewalls or intrusion prevention systems (IPSs)	54%
Monitored or managed endpoint devices	45%
Monitored or managed intrusion detection (IDS) and/or prevention (IPS) systems	39%
Monitored or managed multifunction firewalls	41%
Managed or monitored security gateways for messaging or Web traffic	36%
Security analysis and reporting of events collected from IT infrastructure logs	33%
Reporting associated with monitored/managed devices and incident response	26%
Managed vulnerability scanning of networks, servers, databases or applications	44%
Distributed denial of service (DDoS) protection	37%
Monitoring or management of customer-deployed security information and event management (SIEM) technologies	35%
Monitoring and/or management of advanced threat defense technologies	17%
Total	407%

Q6a. **Today**, how important is the use of automation, to achieving a strong cybersecurity posture?	Pct%
Essential	27%
Very important	30%
Important	23%
Not important	15%
Irrelevant	5%
Total	100%

Q6b. How important will the use of automation be to achieving a strong cybersecurity posture **two years from now?**	Pct%
Essential	40%
Very important	35%
Important	16%
Not important	9%
Irrelevant	0%
Total	100%

Q7a. **Today**, how important is the use of machine learning to achieving a strong cybersecurity posture?	Pct%
Essential	24%
Very important	28%
Important	22%
Not important	19%
Irrelevant	7%
Total	100%

Q7b. How important will the use of machine learning be to achieving a strong cybersecurity posture **two years from now?**	Pct%
Essential	41%
Very important	38%
Important	14%
Not important	7%
Irrelevant	0%
Total	100%

Q8a. **Today**, how important is orchestration between automation and machine learning to achieving a strong cybersecurity posture?	Pct%
Essential	26%
Very important	38%
Important	21%
Not important	10%
Irrelevant	5%
Total	100%

Q8b. How important will orchestration between automation and machine learning be to achieving a strong cybersecurity posture **two years from now?**	Pct%
Essential	37%
Very important	41%
Important	15%
Not important	7%
Irrelevant	0%
Total	100%

Q9. Who are key influencers/decision makers in setting your organization's use of technologies for cybersecurity? Please select your top three (3) choices.	Pct%
DevOps Leader	35%
Chief Information Officer	51%
Chief Information Security Officer	37%
Chief Security Officer	7%
Chief Risk Officer	20%
Chief Compliance Officer	19%
Chief Technology Officer	6%
Data Scientist / Analyst	7%
Security Architect	11%
Managed Security Services Provider (MSSP)	25%
Line of Business (LoB) / General Management	16%
Security Operations Center (SOC) Team	34%
No one person or function	32%
Total	300%

Q10. What disruptive technologies will put your organization at risk over the next two years? Please select your top five (5) choices.	Pct%
Employees' use of favorite cloud apps in the workplace (BYOC)	31%
Employees' use of personally-owned mobile devices (BYOD)	44%
Employees' use of social media in the workplace	35%
Homomorphic encryption	9%
Hybrid cloud ecosystem	40%
IoT devices	56%
No on-premise data centers	15%
Use of artificial intelligence platform	17%
Use of big data analytics	40%
Use of blockchain methods	53%
Use of cloud-based sharing and document collaboration tools	60%
Use of digital identities	23%
Use of public cloud services	36%
Use of virtual currencies	7%
Use of virtualization technologies	9%
Workplace use of quantum computing	25%
Other (please specify)	0%
Total	500%

Q11. What types of cyberattacks pose the greatest risk to your business over the next two years? Please select your top four (4) choices.	Pct%
Data breach involving customer PII, EHI, or payment data	67%
Data breach involving information about our employees	34%
Data breach involving our clients' proprietary information	46%
Exposure of my company's intellectual property or strategic information	42%
Theft of my company's customer list or marketing data	35%
Data breach that could threaten executive safety or privacy	27%
Tampering with or compromise to the integrity of our products or services	34%
Destruction or manipulation of financial data	13%
Disruption of our core business network	42%
Disruption/destruction of connected devices (such as biomedical technologies, controls systems, robotic devices, automatic teller machines)	31%
Tampering with customer-facing web applications	27%
Other (please specify)	2%
Total	400%

Part 3. Most promising cybersecurity technologies

Following are security technology features considered important by many organizations. What is the relative importance of each feature for achieving a strong cybersecurity posture? **Please rate each feature using the 10-point scale from 1 = low to 10 = high ability**	
Q12. The ability to integrate artificial intelligence and/or automation platforms with legacy systems	Pct%
1 or 2	12%
3 or 4	12%
5 or 6	23%
7 or 8	28%
9 or 10	25%
Total	100%
Extrapolated value	6.34

Q13. The ability to quickly pinpoints anomalies in network traffic	Pct%
1 or 2	9%
3 or 4	8%
5 or 6	12%
7 or 8	40%
9 or 10	31%
Total	100%
Extrapolated value	7.02

Q14. The ability to provide advance warning about threats and attackers	Pct%
1 or 2	7%
3 or 4	11%
5 or 6	13%
7 or 8	38%
9 or 10	31%
Total	100%
Extrapolated value	7.00

Q15. The ability to enable adaptive perimeter controls	Pct%
1 or 2	13%
3 or 4	12%
5 or 6	19%
7 or 8	33%
9 or 10	23%
Total	100%
Extrapolated value	6.32

Q16. The ability to capture actionable intelligence about the threat landscape	Pct%
1 or 2	8%
3 or 4	9%
5 or 6	11%
7 or 8	25%
9 or 10	47%
Total	100%
Extrapolated value	7.38

Q17. The ability to perform efficient patch management	Pct%
1 or 2	9%
3 or 4	13%
5 or 6	16%
7 or 8	33%
9 or 10	29%
Total	100%
Extrapolated value	6.70

Q18. The ability to capture information about attackers (honey pot)	Pct%
1 or 2	13%
3 or 4	15%
5 or 6	21%
7 or 8	26%
9 or 10	25%
Total	100%
Extrapolated value	6.20

Q19. The ability to prioritize threats and vulnerabilities	Pct%
1 or 2	5%
3 or 4	6%
5 or 6	11%
7 or 8	33%
9 or 10	45%
Total	100%
Extrapolated value	7.64

Q20. The ability to control and regulate insecure mobile platforms	Pct%
1 or 2	14%
3 or 4	11%
5 or 6	19%
7 or 8	30%
9 or 10	26%
Total	100%
Extrapolated value	6.36

Q21. The ability to stop insecure devices from accessing enterprise systems	Pct%
1 or 2	12%
3 or 4	10%
5 or 6	15%
7 or 8	32%
9 or 10	31%
Total	100%
Extrapolated value	6.70

Q22. The ability to locate and control sensitive or confidential data (including unstructured data)	Pct%
1 or 2	1%
3 or 4	0%
5 or 6	6%
7 or 8	42%
9 or 10	51%
Total	100%
Extrapolated value	8.34

Q23. The ability to control the growth and proliferation of unstructured data assets	Pct%
1 or 2	3%
3 or 4	1%
5 or 6	7%
7 or 8	43%
9 or 10	46%
Total	100%
Extrapolated value	8.06

Q24. The ability to control the sharing of sensitive or confidential data with third parties	Pct%
1 or 2	7%
3 or 4	11%
5 or 6	21%
7 or 8	41%
9 or 10	30%
Total	110%
Extrapolated value	7.57

Q25. The ability to control endpoints and mobile connections (including IoT devices)	Pct%
1 or 2	2%
3 or 4	5%
5 or 6	5%
7 or 8	32%
9 or 10	56%
Total	100%
Extrapolated value	8.20

Q26. The ability to control and regulate the use of cloud-based applications and infrastructure	Pct%
1 or 2	9%
3 or 4	11%
5 or 6	10%
7 or 8	40%
9 or 10	30%
Total	100%
Extrapolated value	6.92

Q27. What are the main cybersecurity challenges will your organization face in the next two years? Please select the top six (6) choices.	Pct%
Breaches involving high-value information	51%
Breaches involving large volumes of data	44%
Breaches that damage critical infrastructure	49%
Breaches that disrupt business and IT processes	43%
Cyber warfare or cyber terrorism	18%
Emergence of cyber syndicates	21%
Emergence of hacktivism (i.e. activist-motivated hacking attempts)	15%
Hardware-based attacks	42%
Inability to recruit the right individuals	56%
Inability to retain the right individuals	50%
Increasing stealth and sophistication of cyber attackers	63%
Insufficient budget	51%
Lack of knowledge (unable to keep up with the latest attack method)	46%
Malicious or criminal insiders	30%
Nation state attackers	18%
Other (please specify)	3%
Total	600%

Part 4. Cloud services

Q28. Has your organization deployed an application into production on a public cloud in the last 12 months?	Pct%
Yes	73%
No	27%
Total	100%

Q29. What cloud services would you be willing to pay a premium for? Please select only your two top choices.	Pct%
Increased efficiency	50%
Improved security posture	32%
Faster deployment time	45%
Increased flexibility and choice	32%
Improved customer service	40%
Other (please specify)	1%
Total	200%

Multi-cloud is the use of multiple cloud computing and storage services in a single heterogeneous architecture. This also refers to the distribution of cloud assets, software, applications, etc. across several cloud-hosting environments. With a typical multi-cloud architecture utilizing two or more public clouds as well as multiple private clouds, a multicloud environment aims to eliminate the reliance on any single cloud provider.

Q30. Is multi-cloud strategy a priority for your organization?	Pct%
Yes, a top priority	46%
Yes, a medium priority	33%
Yes, a low priority	12%
Not a priority	9%
Total	100%

Q31a. What percent of your organization's critical security-related workloads is in the cloud **today**?	Pct%
Less than 10%	6%
Between 11 to 20%	15%
Between 21 to 30%	30%
Between 31 to 40%	16%
Between 40 to 50%	15%
Between 50 to 75%	11%
Between 76 to 90%	3%
More than 90%	4%
Total	100%
Extrapolated value	0.35

Q31b. What percent of your organization's critical security-related workloads will be in the cloud **in the next two years?**	Pct%
Less than 10%	1%
Between 11 to 20%	4%
Between 21 to 30%	9%
Between 31 to 40%	23%
Between 40 to 50%	21%
Between 50 to 75%	18%
Between 76 to 90%	13%
More than 90%	11%
Total	100%
Extraploated value	0.52

Q32. In my organization, cloud services provide a more secure data processing environment than on-premises computing.	Pct%
Strongly agree	18%
Agree	15%
Unsure	24%
Disagree	30%
Strongly disagree	13%
Total	100%

Q33. With respect to security products or services, vendor consolidation is a higher priority than investing in best-of-breed.	Pct%
Strongly agree	24%
Agree	23%
Unsure	18%
Disagree	21%
Strongly disagree	14%
Total	100%

Part 5. Investments in enabling security technologies

Q34. Approximately, what best describes the amount of dollars (US$) spent on all IT technologies in the current fiscal year?	Pct%
Less than $1 million	1%
$1 to $10 million	2%
$11 to $25 million	5%
$26 to $50 million	29%
$51 to $100 million	17%
$101 to $250 million	13%
$251 to $500 million	21%
More than $500 million	12%
Total	100%
Extrapolated value (US$ millions)	$ 198.35

Q35. Approximately, what best describes the percentage of all IT technologies dedicated to IT/cyber security?	Pct%
Less than 10%	26%
Between 11 to 20%	25%
Between 21 to 30%	35%
Between 31 to 40%	7%
Between 41 to 50%	4%
More than 50%	3%
Total	100%
Extrapolated value	20%

Q36. The following table provides five spending categories for enabling security technology layers, Please use the following table to allocate 100 points to weigh the amount of spending for each layer **as of today and two years in the future.**

Allocation of budget today	Points
Network layer	31
Application layer	23
Endpoints layer	18
Data layer	13
Operations layer	15
Total points	100

Allocation of budget two years from today	Points
Network layer	25
Application layer	25
Endpoints layer	21
Data layer	16
Operations layer	13
Total points	100

Part 6. Demographics

D1. What organizational level best describes your current position?	Pct%
Senior Executive/VP	6%
Director	16%
Manager	21%
Supervisor	14%
Technician/Staff	36%
Consultant	6%
Contractor	1%
Other	0%
Total	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	Pct%
CEO / Executive Committee	0%
Chief Information Officer	38%
Chief Information Security Officer	19%
Chief Privacy Officer	0%
Chief Risk Officer	5%
Chief Security Officer	3%
Chief Technology Officer	8%
Compliance Officer	3%
Data Protection Officer	0%
DevOps leader	7%
General Counsel	2%
Line of Business Leader	8%
SOC Management	7%
Other	0%
Total	100%

D3. What best describes your organization's primary industry classification?	Pct%
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education	2%
Energy & utilities	6%
Entertainment & media	2%
Financial services	18%
Health & pharmaceutical	11%
Hospitality	2%
Industrial/manufacturing	11%
Public sector	9%
Retail	10%
Services	9%
Technology & software	8%
Transportation	2%
Other	2%
Total	100%

D4. What range best describes the full-time headcount of your global organization?	Pct%
Less than 500	14%
501 to 1,000	16%
1,001 to 5,000	23%
5,001 to 10,000	18%
10,001 to 25,000	12%
25,001 to 75,000	9%
More than 75,000	8%
Total	100%

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