Ponemon INSTITUTE

The Role of Transparency and Security Assurance in Driving Technology Decision-Making

Sponsored by Intel

Independently conducted by Ponemon Institute LLC

Publication Date: March 2021

The Role of Transparency and Security Assurance in Driving Technology Decision-making

Prepared by Ponemon Institute, March 2021

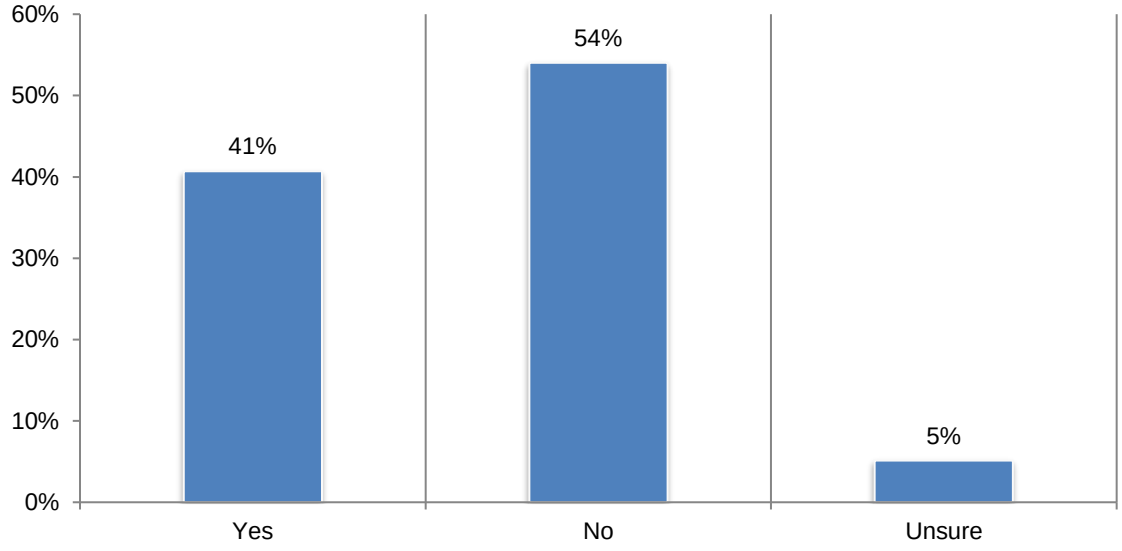
Part 1. Introduction

The purpose of this research is to understand what affects an organization's security technology investment decision-making. Sponsored by Intel, Ponemon Institute surveyed 1,875 individuals in the US, UK, EMEA and Latin America who are involved in securing or overseeing the security of their organization's information systems or IT infrastructure. In addition, they are familiar with their organization's purchase of IT security technologies and services.

A key finding from this research is the importance of technology providers being transparent and proactive in helping organizations manage their cybersecurity risks. **Seventy-three percent of respondents say their organizations are more likely to purchase technologies and services from companies that are finding, mitigating and communicating security vulnerabilities proactively.**

Sixty-six percent of respondents say it is very important for their technology provider to have the capability to adapt to the changing threat landscape. Yet as shown in Figure 1, 54 percent of respondents say their technology providers don't offer this capability.

Figure 1. Does your current technology provider have the capability to adapt to the changing landscape?



Part 2. The characteristics of the ideal technology provider

The characteristics are broken down into three categories: security assurance, innovation and adoption. Following are the most important characteristics of a technology provider and its ability to have this capability. As shown, there is a significant gap between the importance of these features and the ability of many providers to have this capability.

Respondents were asked to rate the following characteristics on a scale from 1 = not important to 10 = highly important. The following results reflect the highly important responses (7+ on a scale from 1 = low importance to 10 = highly important.

Security Assurance

The ability to identify vulnerabilities in its own products and mitigate them. Sixty-six percent say this is highly important. Only 46 percent of respondents say their current technology provider has this capability

The ability to be transparent about security updates and mitigations that are available. Sixty-four percent of respondents say this is highly important. Less than half (48 percent) of respondents say their technology providers have this capability.

Ability to offer ongoing security assurance and evidence that the components are operating in a known and trusted state. Seventy-one percent say this is highly important.

Ability for the technology provider to have the capability to apply ethical hacking practices to proactively identify and address vulnerabilities in its own products. Seventy-four percent of respondents believe this is highly important.

Innovation

Protecting distributed workloads, data in use and hardware-assisted capabilities to defend against software exploits are highly important. The protection of customer data from insider threats is considered highly important by 79 percent of respondents. Organizations prioritize protecting data in use over data in transit and data at rest. Similarly, 76 percent of respondents say hardware-assisted capabilities to defend against software exploits and 72 percent of respondents say protecting distributed workloads are highly important.

Adoption

Interoperability issues and installation costs are the primary influencers when making investments in technologies. The top five factors that influence the deployment of security technologies are interoperability issues (63 percent of respondents), installation costs (58 percent of respondents), system complexity issues (57 percent of respondents), vendor support issues (55 percent of respondents) and scalability issues (53 percent of respondents).

As part of their decision-making process, organizations are measuring the economic benefits of security technologies deployed by their organizations. Forty-seven percent of respondents use metrics to understand the value of their technologies. The measures most often used are ROI (58 percent of respondents), the decrease in false positive rates (48 percent of respondents) and the total cost of ownership (46 percent of respondents).

Organizations are at risk because of the inability to quickly address vulnerabilities. As discussed, a top goal of the IT function is to improve the ability to quickly address vulnerabilities. Thirty-six percent of respondents say they only scan every month or more than once a month.

While 30 percent of respondents say their organizations can patch critical or high priority vulnerabilities in a week or less, on average, it takes almost six weeks to patch a vulnerability once it is detected. The delays in patching are mainly caused by human error (63 percent of respondents), the inability to take critical applications and systems off-line in order to patch quickly (58 percent of respondents) and not having a common view of applications and assets across security and IT teams (52 percent of respondents).

Other takeaways from the research include the following.

Improving the ability to deal effectively with a data breach or cyberattack is the top goal of the IT function. Reduction of the mean time to respond, contain and remediation of a cyberattack or data breach and the ability to quickly patch vulnerabilities are the top security objectives of the IT function.

Organizations' IT budgets are not sufficient to support a strong security posture. Eighty-six percent of respondents say their IT budget is only adequate (45 percent of respondents) or less than adequate (41 percent of respondents). Fifty-three percent of respondents say the IT security budget is part of the overall IT budget.

Responsibility for security is still uncertain across organizations. Twenty-one percent of respondents agree the security leader (CISO) should be responsible for IT security objectives, while 19 percent of respondents believe the CIO/CTO and 17 percent of respondents think the business unit leader should be responsible. The conclusion is that there is uncertainty in responsibility.

Part 3. Key findings

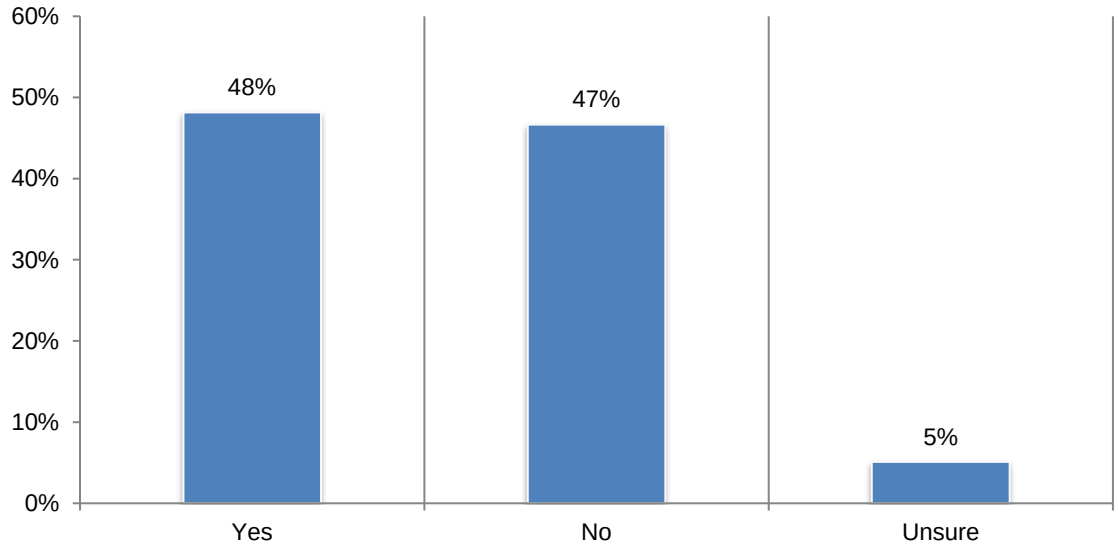
In this section, we provide an analysis of the findings. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following three themes.

- What impacts investments in IT security technologies
- Perceptions about the cybersecurity risks to organizations
- Country and regional differences

What impacts investments in IT security technologies

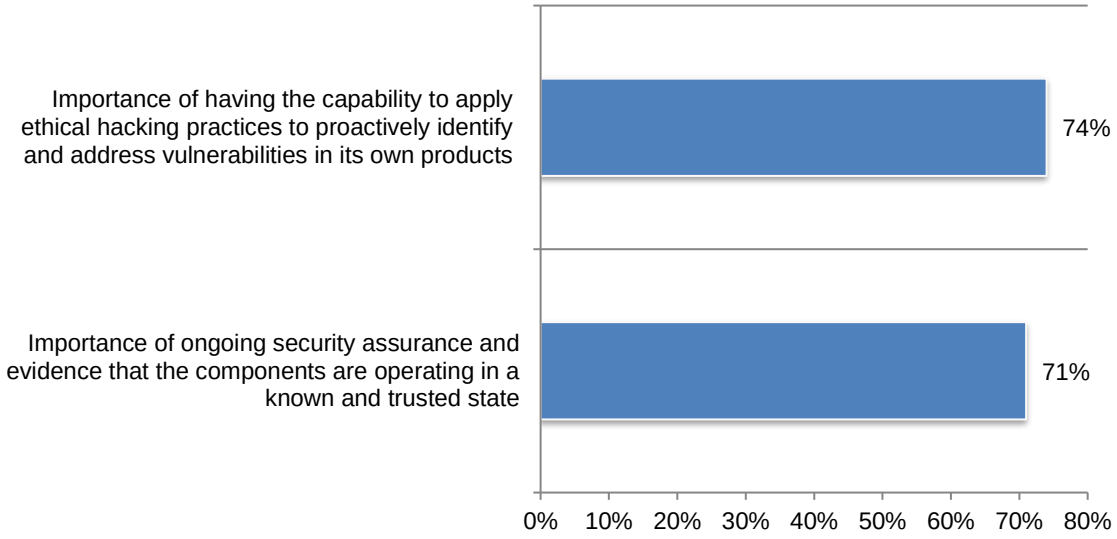
Most technology providers are not transparent about security updates and mitigations that are available. While 64 percent of respondents say it is very important for their technology providers to have this transparency, less than half (48 percent) of respondents say this is available to their organizations.

Figure 2. Is your technology provider transparent about security updates and mitigations that are available?



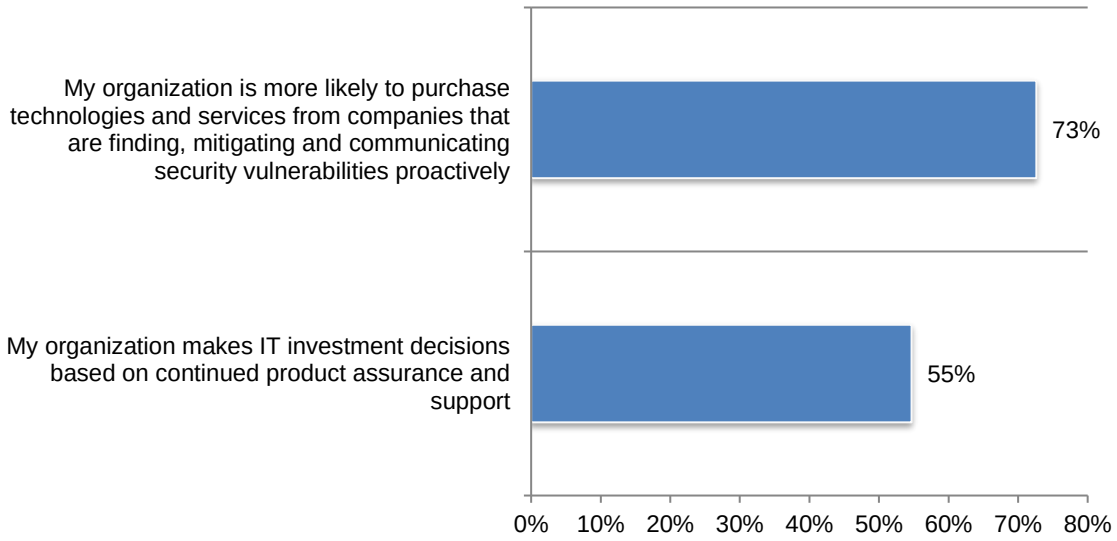
As shown in Figure 3, of all the capabilities represented in this research, the most important are the technology provider's capability to apply ethical hacking practices in order to proactively identify and address vulnerabilities in its own products and to provide ongoing assurance and evidence that the components are operating in a known and trusted state.

Figure 3. Importance of ongoing security and security assurances and to apply ethical hacking practices to identify vulnerabilities
On a scale from 1 = not important to 10 = highly important, 7+ responses



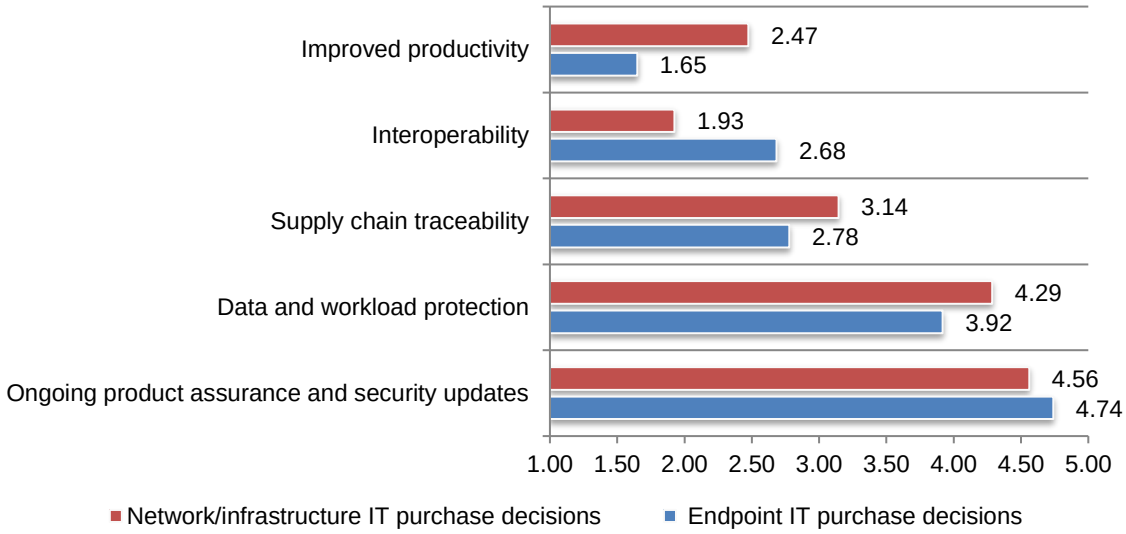
Organizations want technology providers to be transparent and proactive in helping them manage their cybersecurity risks. As shown in Figure 4, 73 percent of respondents say their organizations are more likely to purchase technologies and services from companies that are finding, mitigating and communicating security vulnerabilities proactively. Investment decisions are also based on the provider's continued product assurance and support.

Figure 4. Factors that influence investment decisions
Strongly agree and Agree response combined



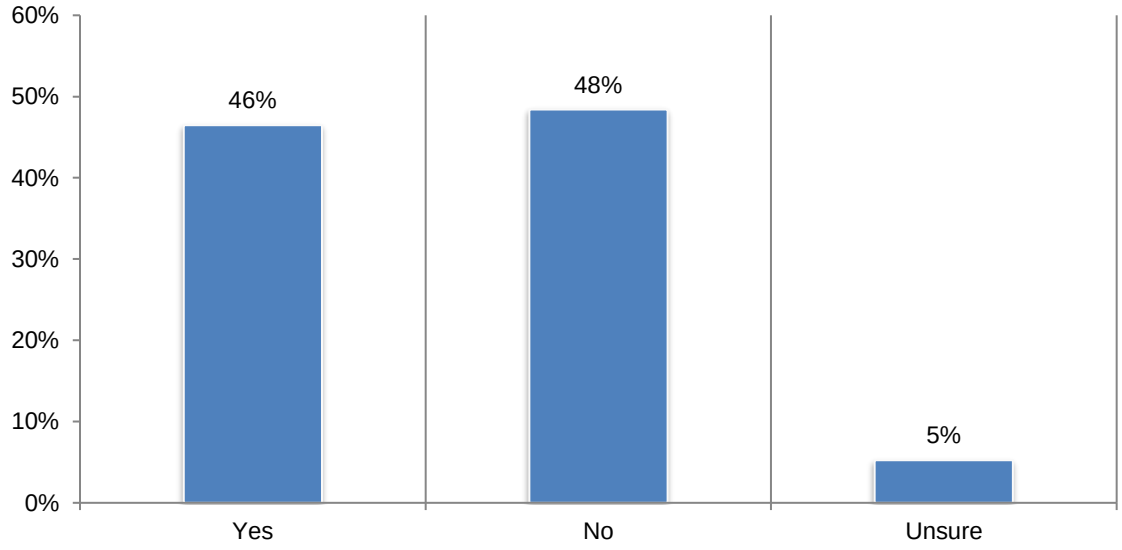
Improved productivity and interoperability are the most important features when making endpoint IT and network/infrastructure purchasing decisions. Respondents were asked to rank the importance of 5 features that influence the investment decision. These are improved productivity, interoperability, ongoing product assurance and security updates, data and workload protection and supply chain traceability. The top two features for endpoint purchases are improved productivity and interoperability. In the case of network/infrastructure purchases the top two features are also interoperability followed by improved productivity, as shown in Figure 5.

Figure 5. What features are most important when purchasing endpoint and network/ infrastructure IT solutions?
Ranking from 1= most important to 5 = least important



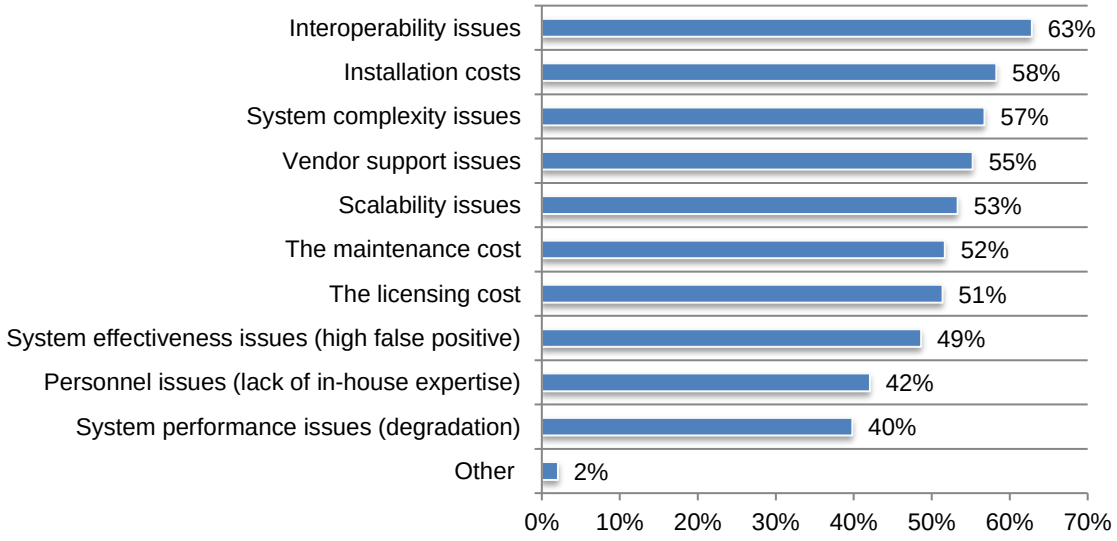
Sixty-six percent of respondents say it is very important for technology providers to identify vulnerabilities in its own products and mitigate them. However, as shown in Figure 6 only 46 percent of respondents say their technology provider has this capability.

Figure 6. Does your technology provider identify vulnerabilities in its own products and mitigate them?



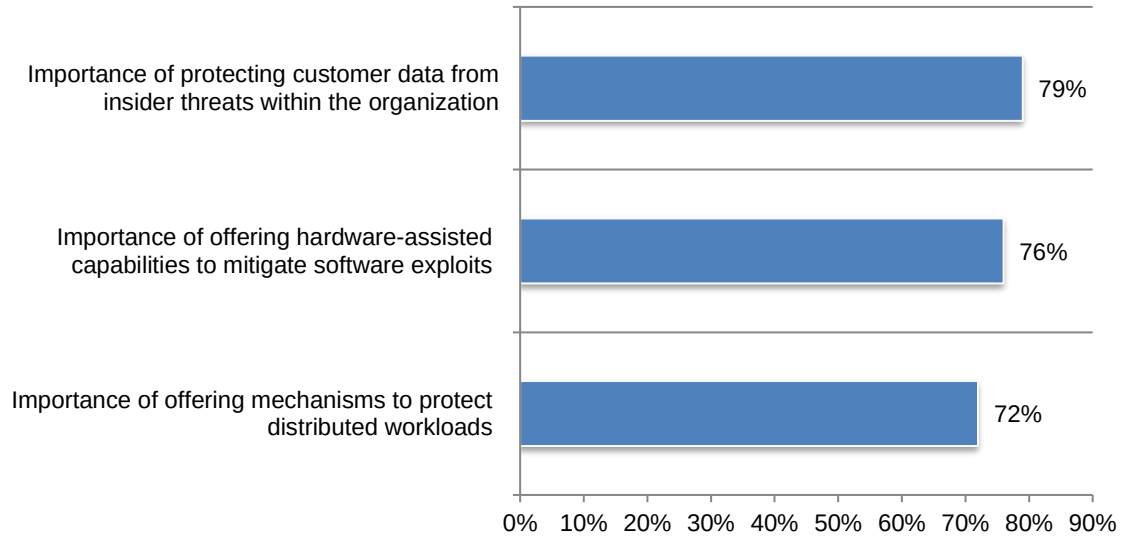
As shown in Figure 7, the top five factors that influence the deployment of security technologies are interoperability issues (63 percent of respondents), installation costs (58 percent of respondents), system complexity issues (57 percent of respondents), vendor support issues (55 percent of respondents) and scalability issues (53 percent of respondents).

Figure 7. What factors does your organization consider when deploying security technologies



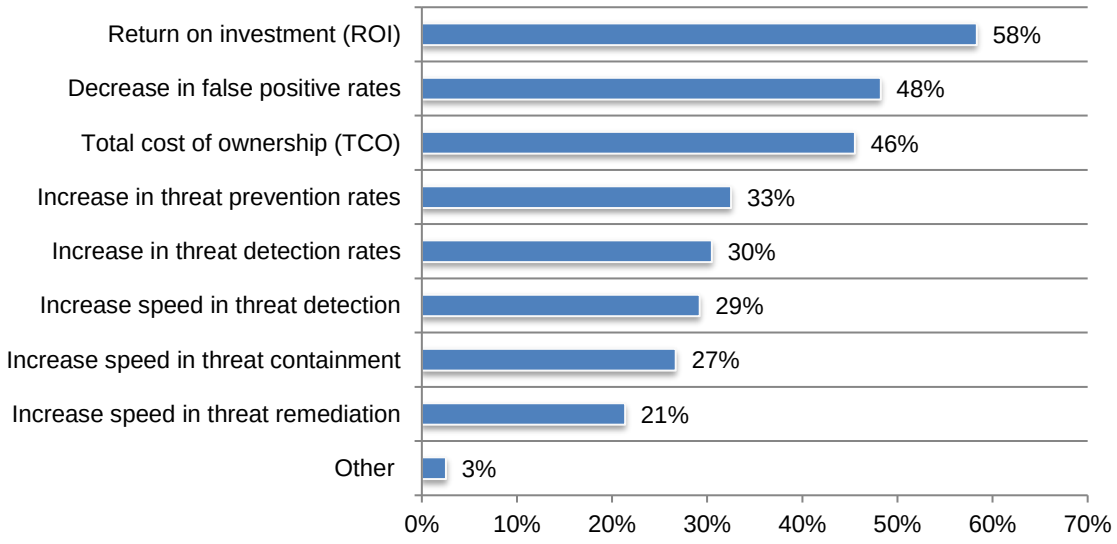
Protecting distributed workloads, customer data in use and hardware-assisted capabilities to defend against software exploit are highly important. Respondents were asked to rate the importance of these three capabilities on a scale of 1 = not important to 10 = very important. Figure 8 presents the highly important responses (7+ on the 10-point scale). As shown, the protection of customer data from insider threats is considered highly important by 79 percent of respondents. Similarly, 76 percent of respondents say hardware-assisted capabilities to defend against software exploits and 72 percent say protecting distributed workloads are highly important.

Figure 8. The importance of protecting distributed workloads, customer data and hardware-assisted capabilities to defend against software exploit
From 1 = not important to 10 = highly important, 7+ responses presented



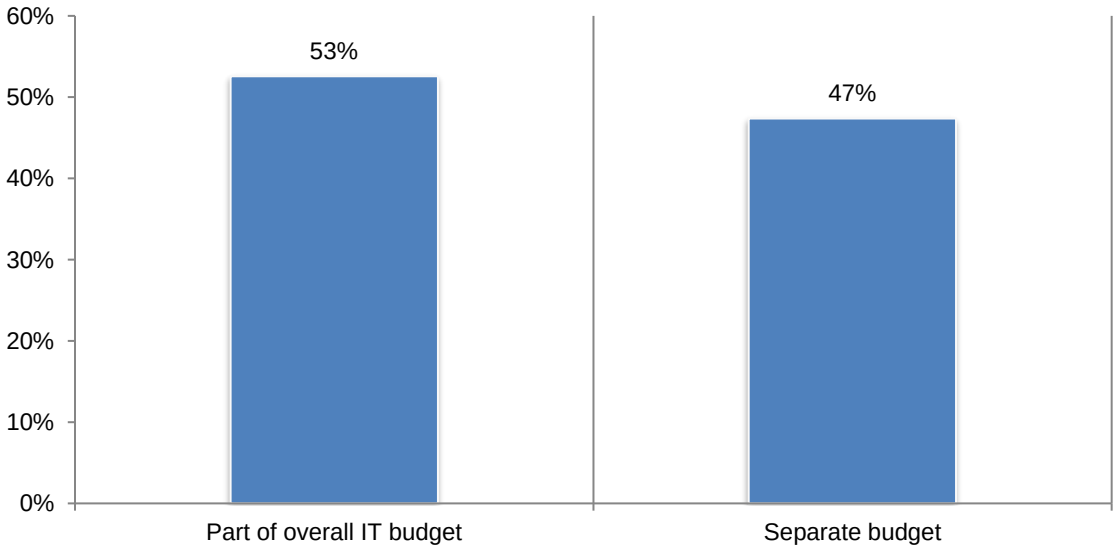
As part of their decision-making process, organizations are measuring the economic benefits of security technologies deployed by their organizations. Forty-seven percent of respondents use metrics to understand the value of their technologies. According to Figure 9, the measures most often used are ROI (58 percent of respondents), the decrease in false positive rates (48 percent of respondents) and the total cost of ownership (46 percent of respondents).

Figure 9. Metrics used to evaluate the economic benefits of security technologies deployed
More than one response permitted



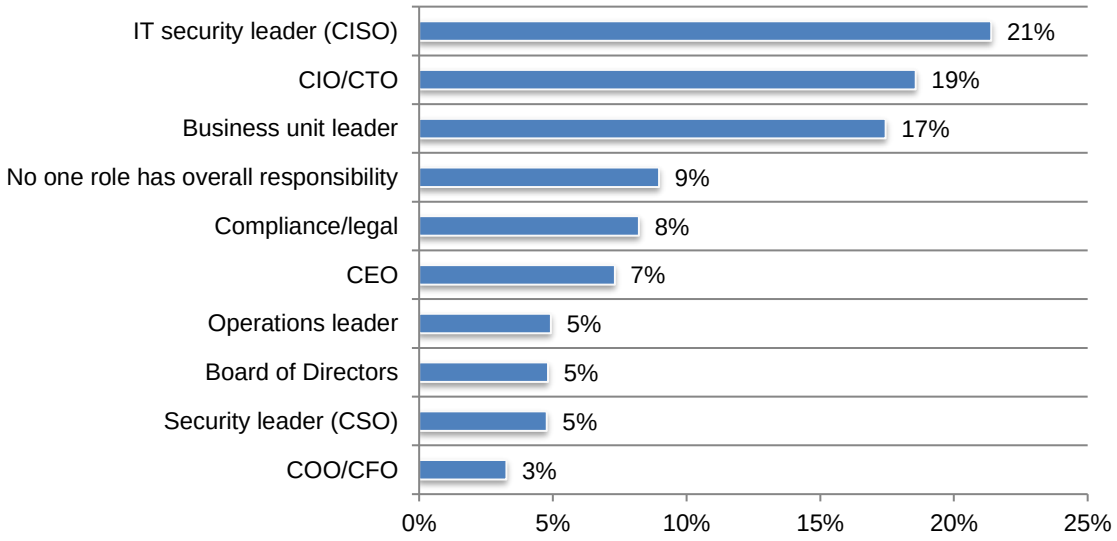
Organizations' IT budgets are not sufficient to support a strong security posture. Eighty-six percent of respondents say their IT budget is only adequate (45 percent of respondents) or less than adequate (41 percent of respondents). Fifty-three percent of respondents say the IT security budget is part of the overall IT budget, as shown in Figure 10.

Figure 10. Is the IT security budget part of or separate from the overall IT budget?



Responsibility for security is still uncertain across organizations. As shown in Figure 11, 21 percent of respondents agree the security leader (CISO) should be responsible for IT security objectives, while 19 percent of respondents believe the CIO/CTO and 17 percent of respondents think the business unit leader should be responsible. The conclusion is that there is uncertainty in responsibility.

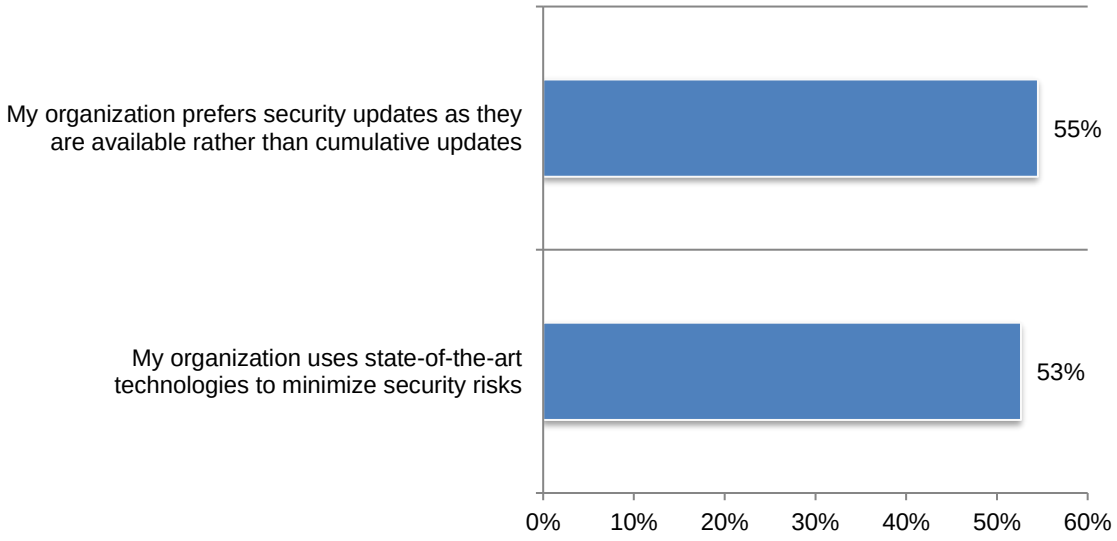
Figure 11. Who is most responsible for ensuring IT security objectives are achieved within your organization?



Perceptions about the cybersecurity risks to organizations

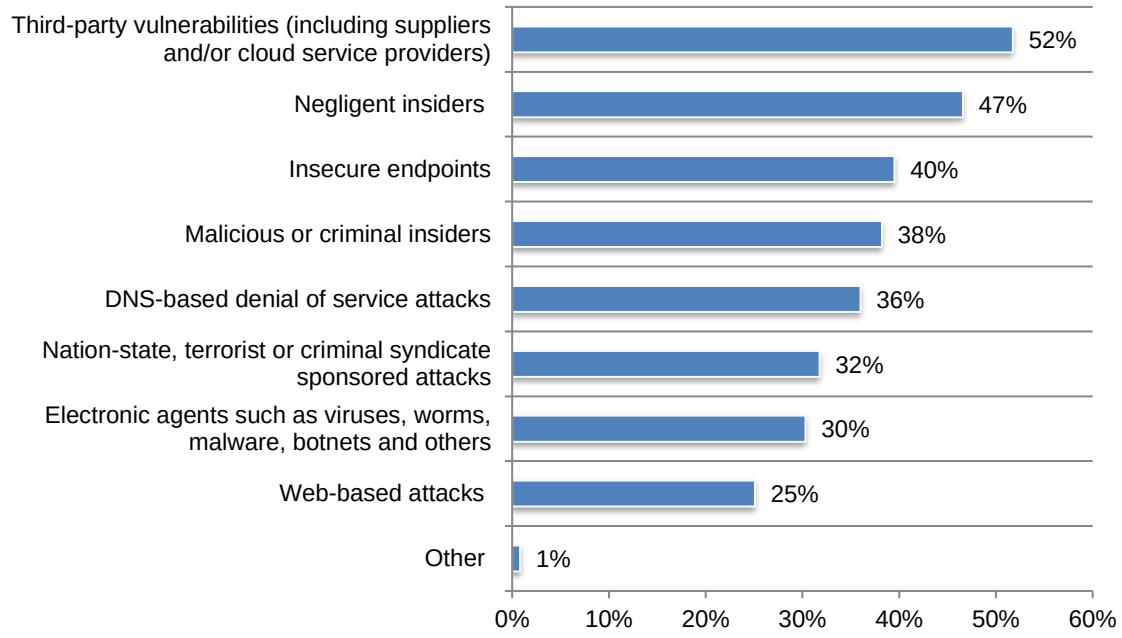
Negligent insiders and third-party vulnerabilities are the top security threats affecting their organization. As shown in Figure 12, 55 percent of respondents say their organizations prefer security updates as they are available rather than cumulative updates and 53 percent of respondents say their organizations use state-of-the-art technologies to minimize security risks.

Figure 12. Preferences about minimizing security threats
Strongly agree and Agree responses combined



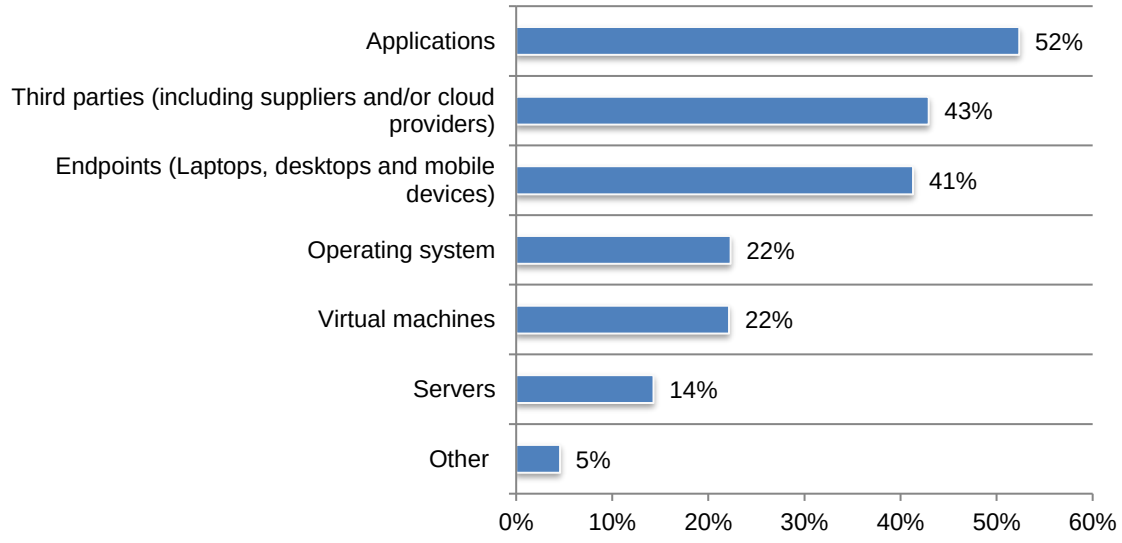
As shown in Figure 13, organizations believe third-party vulnerabilities from such sources as suppliers and cloud service providers are the biggest security threat (52 percent of respondents), followed by negligent insiders (47 percent of respondents) and insecure endpoints (40 percent of respondents).

Figure 13. What are the top security threats that affect your organization?
Three responses permitted



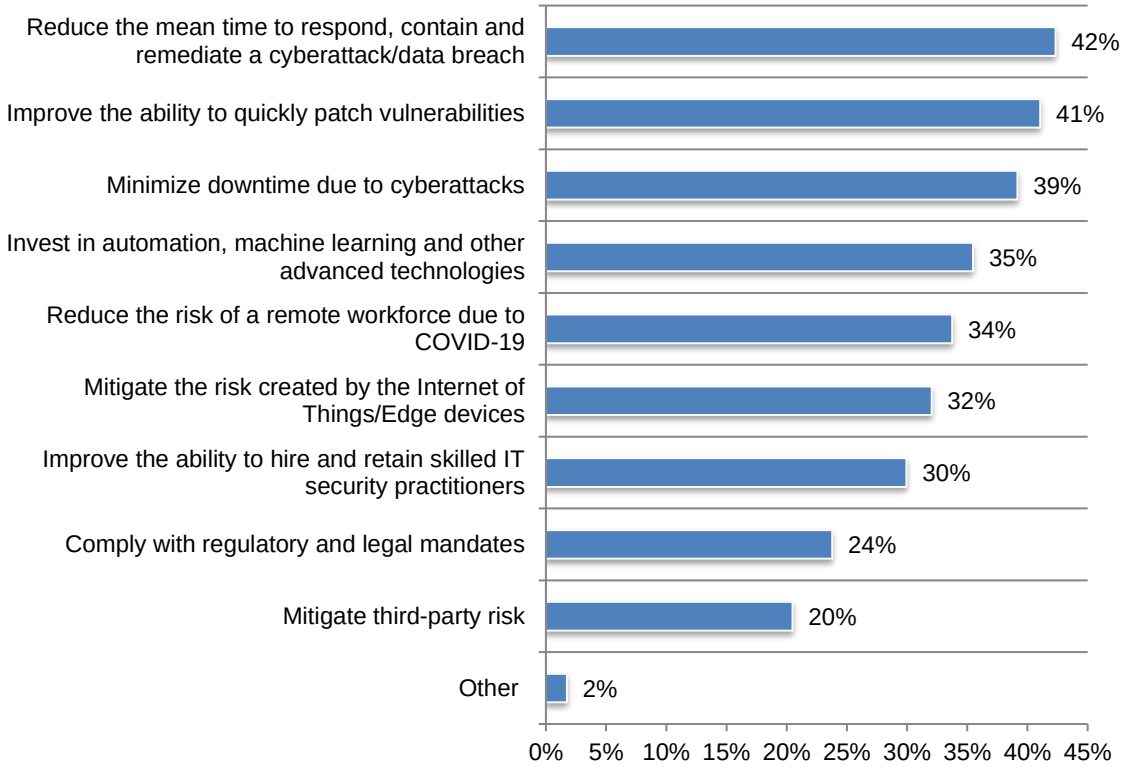
Data in use is the most important data to protect. The data most susceptible to loss, theft, misuse or other security compromise is located in applications, with third parties and on endpoints, as shown in Figure 14.

Figure 14. Where is data most susceptible to loss, theft, misuse or other security compromise?
Two responses permitted



Improving the ability to deal effectively with a data breach or cyberattack is the top goal of the IT function. According to Figure 15, reduction of the mean time to respond, contain and remediation of a cyberattack or data breach and the ability to quickly patch vulnerabilities are the top security objectives of organizations.

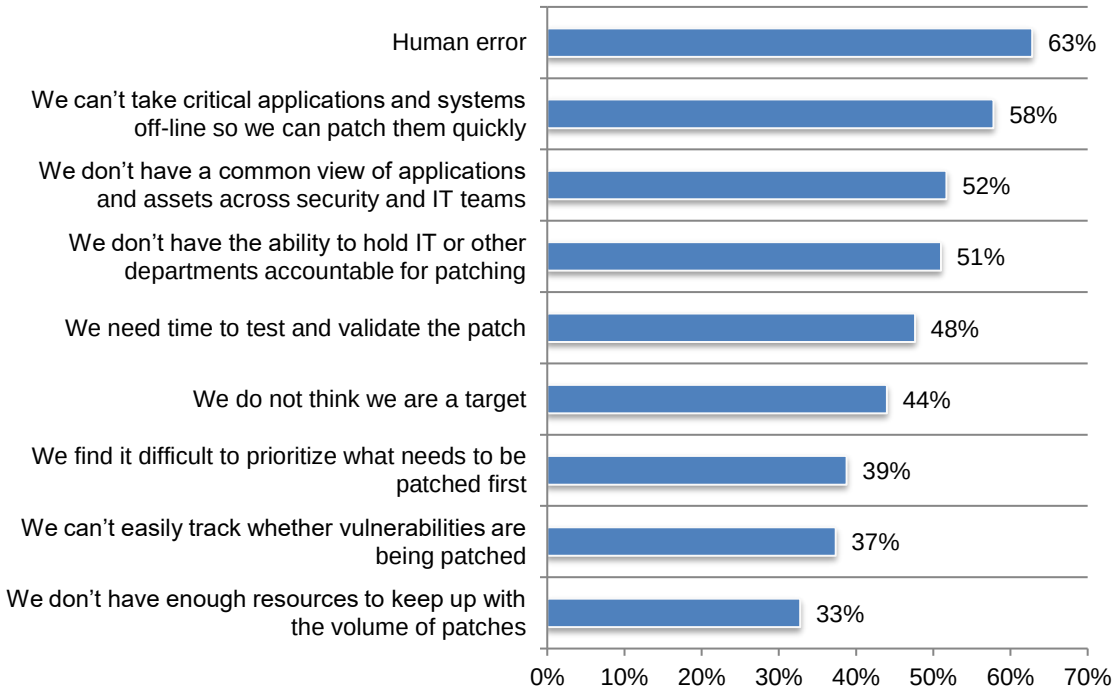
Figure 15. What does the IT function consider the top security objectives for the organization?
Three responses permitted



Organizations are at risk because of the inability to quickly address vulnerabilities. As discussed, a top goal of the IT function is to improve the ability to quickly address vulnerabilities. Thirty-six percent of respondents say they only scan every month or more than once a month.

While 30 percent of respondents say their organizations can patch critical or high priority vulnerabilities in a week or less, on average, it takes almost six weeks to patch a vulnerability once it is detected. As shown in Figure 16, the delays in patching are mainly caused by human error (63 percent of respondents), the inability to take critical applications and systems off-line in order to patch quickly (58 percent of respondents) and not having a common view of applications and assets across security and IT teams (52 percent of respondents).

Figure 16. Which factors cause delays in your vulnerability patching process?
More than one response permitted

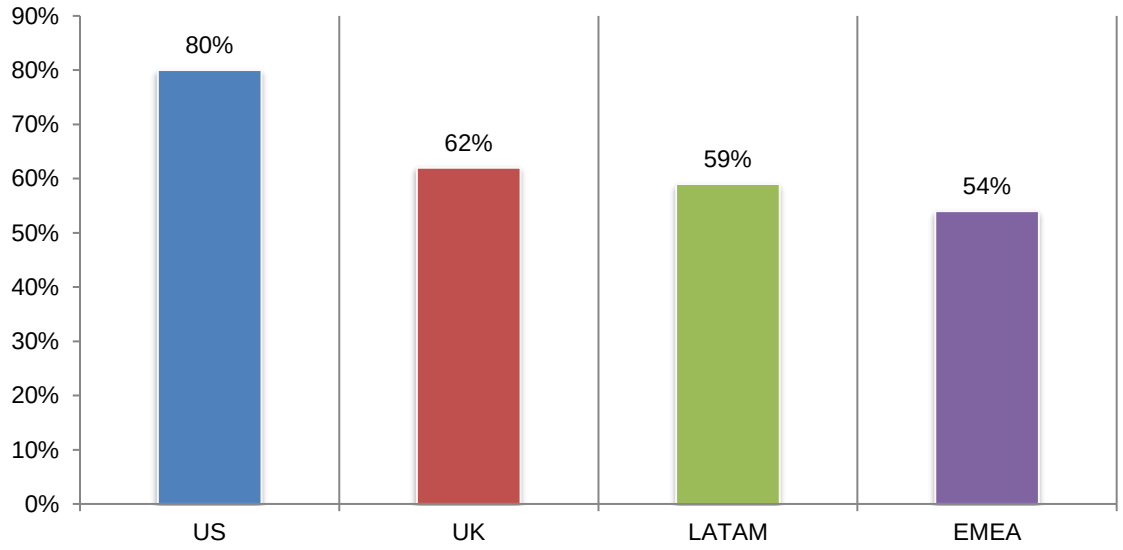


Country and regional differences

In this section we present the most salient differences among the countries and regions represented in this research: United States (623 respondents), United Kingdom (412) EMEA (485 respondents) and LATAM (355 respondents).

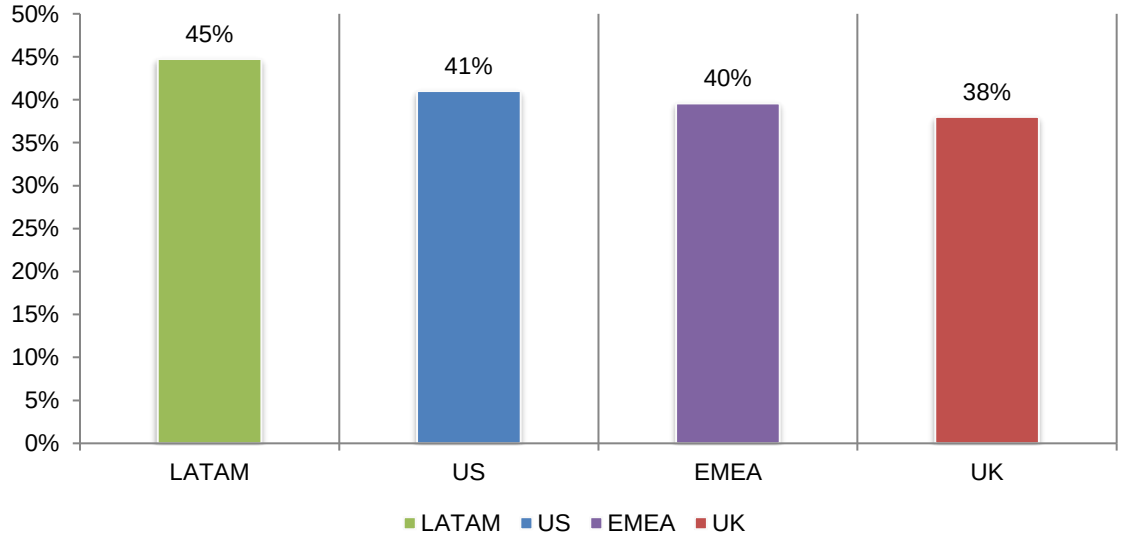
According to Figure 17, US respondents (80 percent) are more likely to say that it is highly important for technology providers to have the capability to adapt to a changing threat landscape and EMEA respondents (54 percent) are less likely to believe it is highly important.

Figure 17. The importance of technology providers' capability to adapt to the changing threat landscape
On a scale from 1 = not important to 10 = highly important, 7+ responses



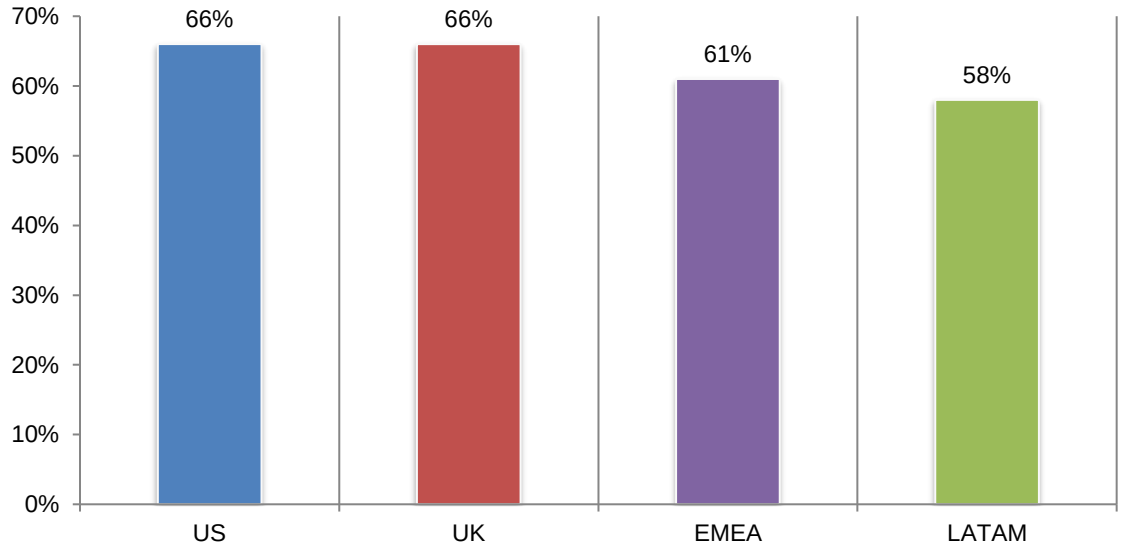
Only 38 percent of UK respondents say their technology provider has this capability, as shown in Figure 18.

Figure 18. Does your current technology provider have this capability?
Yes responses presented



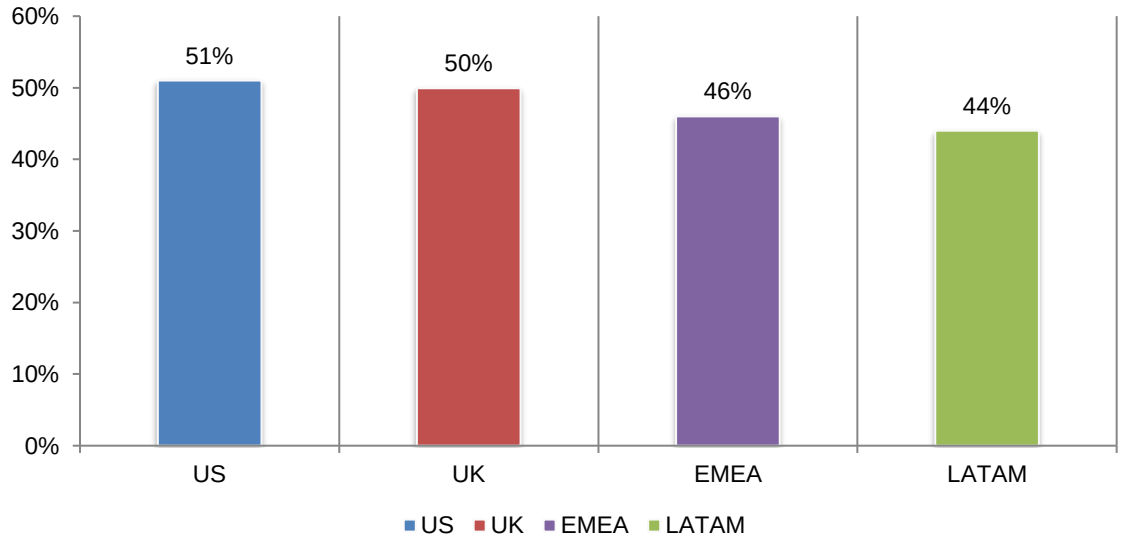
Sixty-six percent of US and UK respondents say transparency about security updates and mitigations is highly important, according to Figure 19.

Figure 19. The importance of technology providers to be transparent about security updates and mitigations that are available
On a scale from 1 = not important to 10 = highly important, 7+ responses



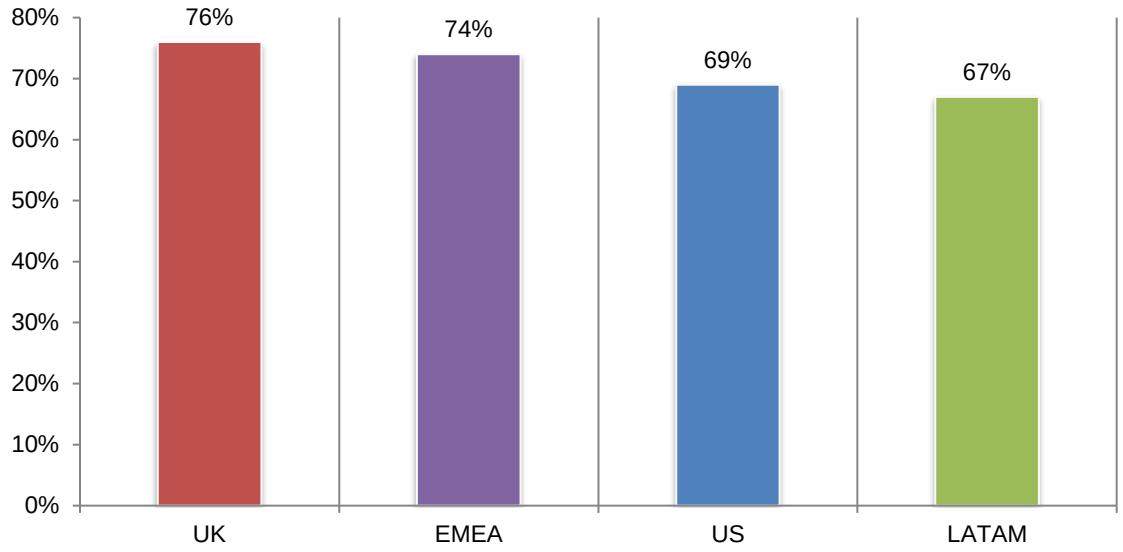
Only 46 of EMEA respondents and 44 percent of respondents say their technology provider has this capability, as shown in Figure 20.

Figure 20. Does your technology provider have this capability?
Yes responses presented



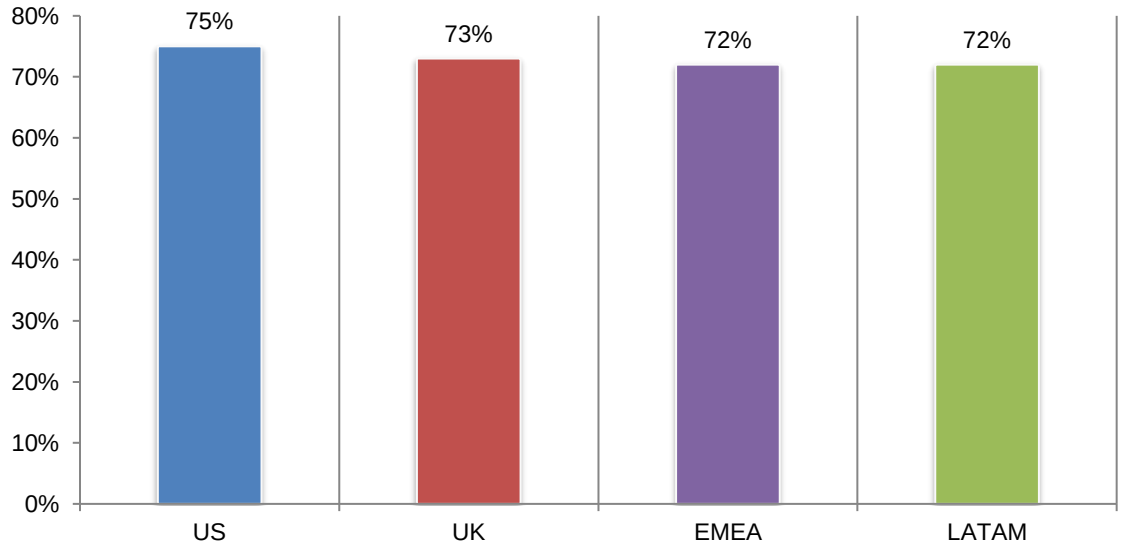
According to Figure 21, more UK and EMEA respondents (76 percent and 74 percent, respectively) rate the capability of offering ongoing security assurances as highly important.

Figure 21. The importance of offering ongoing security assurances
On a scale from 1 = not important to 10 = highly important, 7+ responses



According to Figure 22, respondents in all country and regions believe applying ethical hacking practices to proactively identify and address vulnerabilities as highly important.

Figure 22. The importance of applying ethical hacking practices to proactively identify and address vulnerabilities
On a scale from 1 = not important to 10 = highly important, 7+ responses



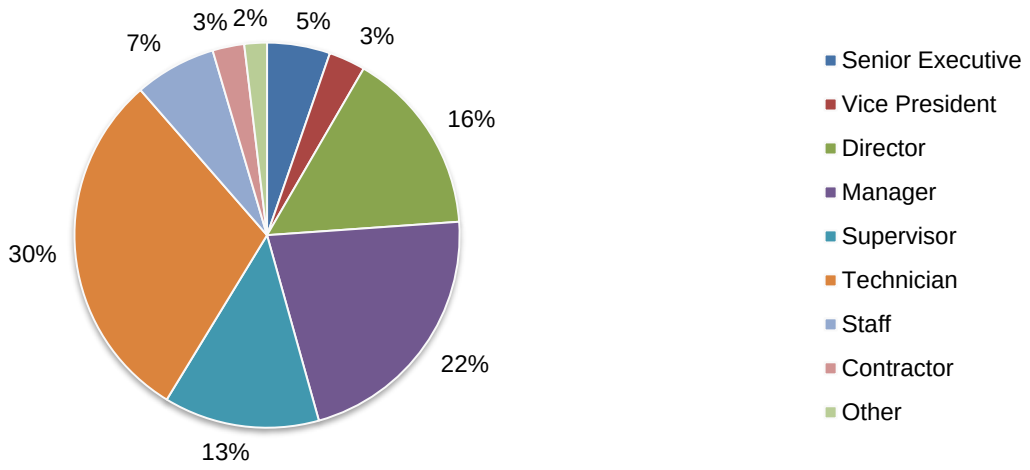
Part 4. Methodology

A sampling frame of 49,707 individuals in the US, UK, EMEA and Latin America who are involved in securing or overseeing the security of their organization's information systems or IT infrastructure were selected as participants to this survey. Table 1 shows 2,062 total returns. Screening and reliability checks required the removal of 187 surveys. Our final sample consisted of 1,875 surveys or a 3.8 percent response.

Table 1. Sample response	US	UK	EMEA	LATAM	Overall
Sampling frame	16,993	10,800	11,963	9,951	49,707
Total returns	675	455	534	398	2,062
Rejected or screened surveys	52	43	49	43	187
Final sample	623	412	485	355	1,875
Response rate	3.7%	3.8%	4.1%	3.6%	3.8%

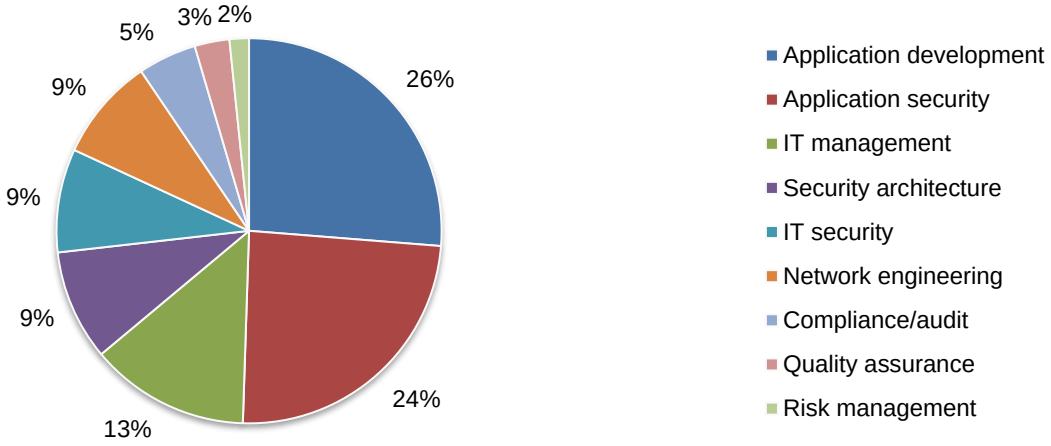
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (59 percent of respondents) are at or above the supervisory level. The largest organizational position is technician (30 percent of respondents) followed by manager (22 percent of respondents).

Pie Chart 1. Current position within the organization



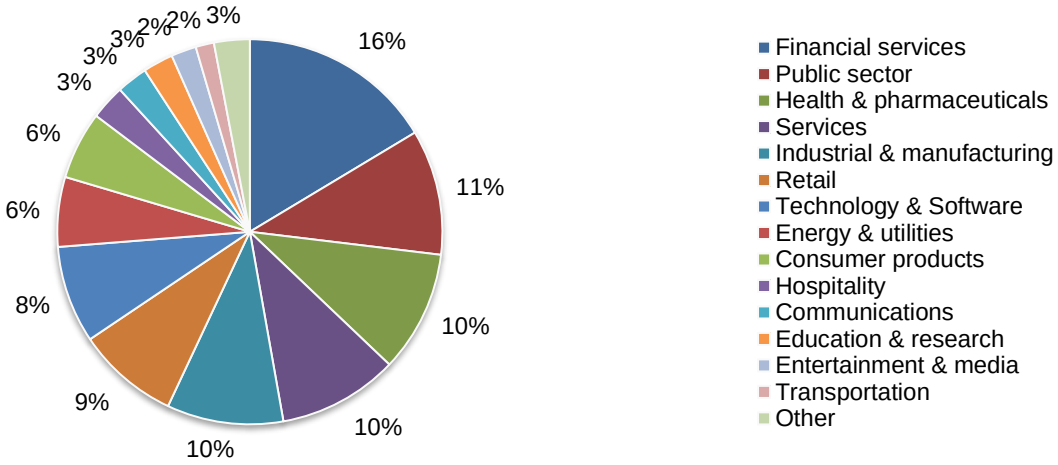
Pie Chart 2 identifies the respondents primary role within the organization. Twenty-six percent of respondents identified application development and twenty-four percent of respondents identified application security as their primary role. Another 13 percent of respondents indicated their primary role is in IT management.

Pie Chart 2. Distribution of respondents according to primary role in the organization



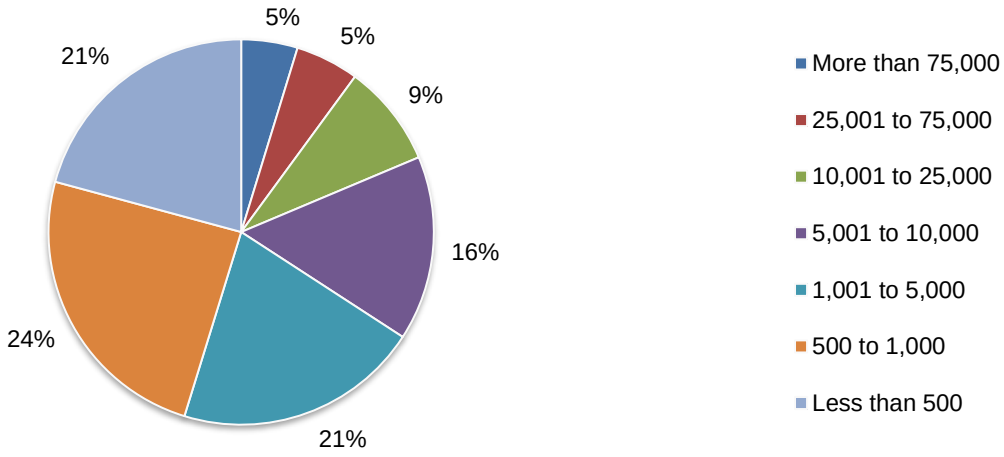
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (16 percent of respondents) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by public sector (11 percent of respondents), health and pharmaceuticals (10 percent of respondents), services (10 percent of respondents), and industrial and manufacturing (10 percent of respondents).

Pie Chart 3. Primary industry focus



As shown in Pie Chart 4, 56 percent of respondents are from organizations with a global headcount of more than 1,000 employees. The largest segment at 24 percent of respondents are from organizations with a global headcount between 500 and 1,000 employees.

Pie Chart 4. Global employee headcount



Part 5. 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 involved in securing or overseeing the security of their organization's information systems or IT infrastructure. We also acknowledge that the results may be biased by external events such as media coverage. Finally, 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, 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 December 21, 2020 and January 7, 2021.

Survey response	US	UK	EMEA	LATAM	Overall
Total sampling frame	16,993	10,800	11,963	9,951	49,707
Total returns	675	455	534	398	2,062
Rejected surveys	52	43	49	43	187
Final sample	623	412	485	355	1,875
Response rate	3.7%	3.8%	4.1%	3.6%	3.8%

Part 1. Screening

S1. Does your job involve securing or overseeing the security of your organization's information systems or IT infrastructure? Please mark yes even if your job is only partially involved in the security function.	US	UK	EMEA	LATAM	Overall
Yes	100%	100%	100%	100%	100%
No (stop)	0%	0%	0%	0%	0%
Total	100%	100%	100%	100%	100%

S2. Please check all the activities that you see as part of your job or role.	US	UK	EMEA	LATAM	Overall
Managing budgets	46%	44%	47%	51%	47%
Evaluating vendors	43%	32%	31%	34%	36%
Setting priorities	41%	35%	30%	31%	35%
Securing systems	64%	50%	49%	54%	55%
Ensuring compliance	40%	46%	47%	43%	44%
Ensuring system availability	46%	40%	45%	42%	44%
Patching vulnerabilities	55%	49%	43%	48%	49%
Responding to cyber attacks	74%	70%	69%	71%	71%
None of the above (stop)	0%	0%	0%	0%	0%
Total	409%	366%	362%	373%	381%

S3. How familiar are you with your organization's purchase of IT security technologies and services?	US	UK	EMEA	LATAM	Overall
Very familiar	45%	41%	40%	52%	44%
Familiar	37%	34%	36%	32%	35%
Somewhat familiar	18%	25%	24%	16%	21%
Not familiar (stop)	0%	0%	0%	0%	0%
Total	100%	100%	100%	100%	100%

Part 2. Attributions: Strongly agree and Agree response combined.	US	UK	EMEA	LATAM	Overall
Q1a. My organization makes IT investment decisions based on continued product assurance and support.	51%	61%	49%	61%	55%
Q1b My organization is more likely to purchase technologies and services from companies that are finding, mitigating and communicating security vulnerabilities proactively.	76%	74%	72%	66%	73%
Q1c. My organization uses state-of-the-art technologies to minimize security risks.	60%	51%	49%	47%	53%
Q1d. My organization prefers security updates as they are available rather than cumulative updates.	54%	57%	60%	45%	55%

Q2a. How important is it for your technology provider to have the capability to adapt to the changing threat landscape on a scale from 1 = not important to 10 = highly important?	US	UK	EMEA	LATAM	Overall
1 or 2	2%	8%	9%	10%	7%
3 or 4	4%	9%	8%	9%	7%
5 or 6	14%	22%	29%	21%	21%
7 or 8	37%	24%	22%	33%	30%
9 or 10	43%	38%	32%	26%	36%
Total	100%	100%	100%	100%	100%
Extrapolated value	7.80	7.02	6.73	6.61	7.13

Q2b. Does your current technology provider have this capability?	US	UK	EMEA	LATAM	Overall
Yes	41%	38%	40%	45%	41%
No	54%	58%	53%	51%	54%
Unsure	5%	4%	7%	4%	5%
Total	100%	100%	100%	100%	100%

Q3a. How important is it for your technology provider to identify vulnerabilities in its own products and mitigate them from 1 = not important to 10 = highly important?	US	UK	EMEA	LATAM	Overall
1 or 2	3%	6%	5%	5%	5%
3 or 4	6%	10%	14%	10%	10%
5 or 6	20%	21%	20%	16%	20%
7 or 8	24%	30%	24%	32%	27%
9 or 10	47%	33%	37%	37%	39%
Total	100%	100%	100%	100%	100%
Extrapolated value	7.62	6.96	6.96	7.24	7.23

Q3b. Does your current technology provider have this capability?	US	UK	EMEA	LATAM	Overall
Yes	49%	42%	47%	46%	46%
No	45%	54%	47%	50%	48%
Unsure	6%	4%	6%	4%	5%
Total	100%	100%	100%	100%	100%

Q4a. How important is it for your technology provider to be transparent about security updates and mitigations that are available from 1 = not important to 10 = highly important?	US	UK	EMEA	LATAM	Overall
1 or 2	3%	5%	4%	5%	4%
3 or 4	4%	7%	8%	9%	7%
5 or 6	27%	23%	26%	28%	26%
7 or 8	25%	25%	27%	26%	26%
9 or 10	41%	41%	34%	32%	38%
Total	100%	100%	100%	100%	100%
Extrapolated value	7.44	7.30	7.09	6.92	7.22

Q4b. Does your current technology provider have this capability?	US	UK	EMEA	LATAM	Overall
Yes	51%	50%	46%	44%	48%
No	45%	43%	49%	50%	47%
Unsure	4%	7%	4%	6%	5%
Total	100%	100%	100%	100%	100%

Q5a. How important is it for your technology provider to offer ongoing security assurance and evidence that the components are operating in a known and trusted state from 1 = not important to 10 = highly important?	US	UK	EMEA	LATAM	Overall
1 or 2	5%	6%	6%	5%	5%
3 or 4	9%	5%	9%	10%	8%
5 or 6	17%	13%	11%	18%	15%
7 or 8	29%	32%	28%	29%	29%
9 or 10	40%	44%	46%	38%	42%
Total	100%	100%	100%	100%	100%
Extrapolated value	7.30	7.54	7.50	7.19	7.38

Q5b. How important is it for your technology provider to have the capability to apply ethical hacking practices to proactively identify and address vulnerabilities in its own products from 1 = not important to 10 = highly important?	US	UK	EMEA	LATAM	Overall
1 or 2	4%	3%	4%	6%	4%
3 or 4	9%	9%	10%	10%	9%
5 or 6	12%	14%	14%	11%	13%
7 or 8	36%	32%	37%	37%	36%
9 or 10	39%	41%	35%	35%	38%
Total	100%	100%	100%	100%	100%
Extrapolated value	7.44	7.47	7.24	7.21	7.35

Q6a. How important is it for your technology provider to offer mechanisms to protect distributed workloads from 1 = not important to 10 = highly important?	US	UK	EMEA	LATAM	Overall
1 or 2	5%	4%	5%	8%	5%
3 or 4	8%	7%	6%	10%	8%
5 or 6	14%	13%	13%	18%	14%
7 or 8	30%	34%	44%	30%	34%
9 or 10	43%	42%	32%	34%	38%
Total	100%	100%	100%	100%	100%
Extrapolated value	7.46	7.56	7.32	6.94	7.35

Q6b. How important is it for you to protect customer data from insider threats within your organization?	US	UK	EMEA	LATAM	Overall
1 or 2	0%	0%	0%	0%	0%
3 or 4	2%	2%	2%	2%	2%
5 or 6	18%	19%	20%	18%	19%
7 or 8	30%	39%	23%	30%	30%
9 or 10	50%	40%	55%	50%	49%
Total	100%	100%	100%	100%	100%
Extrapolated value	8.06	7.89	8.11	8.04	8.03

Q6c. How important is it for your technology provider to offer hardware-assisted capabilities to mitigate software exploits from 1 = not important to 10 = highly important?	US	UK	EMEA	LATAM	Overall
1 or 2	4%	9%	4%	8%	6%
3 or 4	7%	11%	6%	10%	8%
5 or 6	10%	13%	8%	11%	10%
7 or 8	38%	29%	40%	30%	35%
9 or 10	41%	39%	42%	41%	41%
Total	100%	100%	100%	100%	100%
Extrapolated value	7.60	7.08	7.74	7.20	7.45

Part 3. Perceptions about cybersecurity risks to their organizations

Q7. What are the top security threats that affect your organization? Check only the top three choices.	US	UK	EMEA	LATAM	Overall
Negligent insiders	48%	42%	47%	48%	47%
Malicious or criminal insiders	40%	32%	36%	46%	38%
Web-based attacks	25%	25%	24%	27%	25%
Insecure endpoints	37%	42%	36%	46%	40%
Third-party vulnerabilities (including suppliers and/or cloud service providers)	50%	63%	50%	45%	52%
DNS-based denial of service attacks	36%	41%	39%	26%	36%
Electronic agents such as viruses, worms, malware, botnets and others	31%	23%	33%	34%	30%
Nation-state, terrorist or criminal syndicate sponsored attacks	33%	32%	35%	25%	32%
Other (please specify)	0%	0%	1%	3%	1%
Total	300%	300%	300%	300%	300%

Q8. What does the IT function consider the top security objectives for the organization? Check only the top three choices.	US	UK	EMEA	LATAM	Overall
Reduce the mean time to respond, contain and remediate a cyberattack/data breach	44%	49%	38%	38%	42%
Minimize downtime due to cyberattacks	40%	38%	44%	33%	39%
Comply with regulatory and legal mandates	23%	22%	28%	22%	24%
Mitigate third-party risk	20%	20%	19%	23%	20%
Mitigate the risk created by the Internet of Things/Edge devices	31%	34%	31%	32%	32%
Reduce the risk of a remote workforce due to COVID-19	34%	31%	32%	38%	34%
Improve the ability to hire and retain skilled IT security practitioners	30%	28%	28%	35%	30%
Invest in automation, machine learning and other advanced technologies	37%	37%	35%	31%	35%
Improve the ability to quickly patch vulnerabilities	39%	36%	44%	46%	41%
Other (please specify)	2%	3%	0%	2%	2%
Total	300%	300%	300%	300%	300%

Q9. In your organization, how do you prioritize protecting data (information assets)? Please rate in order of 1 = highest priority to 3 = lowest priority.	Avg rank	UK	EMEA	LATAM	Overall
At rest (inactive data)	2.78	2.92	3.02	2.55	2.83
In transit (moving from one location to another)	2.15	2.03	2.04	1.91	2.05
In use (active data)	1.60	2.01	2.00	1.28	1.73

Q10. In your organization, where is data (information assets) most susceptible to loss, theft, misuse or other security compromise? Please select the top two choices.	US	UK	EMEA	LATAM	Overall
Operating system	23%	24%	19%	24%	22%
Applications	53%	54%	46%	59%	52%
Servers	16%	12%	14%	15%	14%
Virtual machines	20%	25%	21%	24%	22%
Endpoints (Laptops, desktops and mobile devices)	43%	36%	47%	36%	41%
Third parties (including suppliers and/or cloud providers)	40%	45%	47%	40%	43%
Other (please specify)	5%	4%	6%	3%	5%
Total	200%	200%	200%	200%	200%

Q11. Who is **most responsible** for ensuring IT security objectives are achieved within your organization? Please select only one choice.	US	UK	EMEA	LATAM	Overall
CEO	7%	7%	7%	9%	7%
Board of Directors	5%	5%	5%	4%	5%
COO/CFO	3%	3%	3%	4%	3%
CIO/CTO	19%	19%	21%	14%	19%
IT security leader (CISO)	21%	24%	22%	18%	21%
Security leader (CSO)	4%	4%	5%	7%	5%
Compliance/legal	8%	10%	6%	10%	8%
Business unit leader	19%	13%	18%	19%	17%
Operations leader	5%	5%	4%	6%	5%
No one role has overall responsibility	9%	8%	10%	9%	9%
Other (please specify)	0%	1%	0%	1%	0%
Total	100%	100%	100%	100%	100%

Q12. How often does your organization scan for vulnerabilities?	US	UK	EMEA	LATAM	Overall
Daily	14%	13%	16%	13%	14%
Between 2 and 3 times per week	10%	11%	9%	8%	9%
Every week	9%	10%	9%	7%	9%
Every 2 weeks	6%	6%	5%	6%	6%
Every 3 weeks	9%	10%	9%	9%	9%
Every month	17%	13%	14%	18%	16%
More than once a month	20%	17%	20%	21%	20%
We don’t scan	15%	20%	19%	18%	18%
Total	100%	100%	100%	100%	100%

Q13. Once you detect a **critical or high priority** vulnerability, how long on average does it take to patch?	US	UK	EMEA	LATAM	Overall
3 days	16%	13%	12%	9%	13%
1 week	17%	18%	14%	18%	17%
2-3 weeks	25%	27%	29%	29%	27%
4-5 weeks	23%	18%	24%	24%	22%
6-7 weeks	12%	13%	11%	12%	12%
up to 6 months	6%	5%	6%	4%	6%
7 months to 1 year	1%	3%	3%	2%	2%
More than 1 year	0%	2%	1%	2%	1%
Total	100%	100%	100%	100%	100%
Extrapolated value (weeks)	4.6	6.4	6.0	5.9	5.6

Q14. Which factors below cause delays in your vulnerability patching process? Please select all that apply.	US	UK	EMEA	LATAM	Overall
Human error	62%	62%	62%	66%	63%
We need time to test and validate the patch	46%	41%	50%	56%	48%
We can't take critical applications and systems off-line so we can patch them quickly	57%	51%	62%	62%	58%
We can't easily track whether vulnerabilities are being patched	38%	32%	36%	44%	37%
We find it difficult to prioritize what needs to be patched first	41%	43%	34%	36%	39%
We don't have enough resources to keep up with the volume of patches	34%	32%	27%	39%	33%
We don't have a common view of applications and assets across security and IT teams	52%	54%	48%	54%	52%
We do not think we are a target	43%	43%	49%	40%	44%
We don't have the ability to hold IT or other departments accountable for patching	51%	59%	47%	48%	51%
Total	424%	416%	415%	444%	424%

Q15a. When making **endpoint** (PCs, workstations) IT purchase decisions, what features are most important? Please rank the following from 1= most important to 5 = least important	Avg rank	UK	EMEA	LATAM	Overall
Improved productivity	1.68	1.54	1.57	1.83	1.65
Interoperability	2.55	2.43	3.14	2.59	2.68
Ongoing product assurance and security updates	4.51	4.50	4.83	5.29	4.74
Data and workload protection	3.94	3.13	4.05	4.61	3.92
Supply chain traceability	2.93	2.46	2.77	2.89	2.78

Q15b. When making **network/infrastructure** IT purchase decisions, how do you prioritize the following, please rank the following from 1 = most important to 5 = least important	US	UK	EMEA	LATAM	Overall
Improved productivity	2.36	2.76	2.46	2.36	2.47
Interoperability	1.89	1.53	2.04	2.29	1.93
Ongoing product assurance and security updates	4.58	4.68	4.67	4.25	4.56
Data and workload protection	4.24	4.00	4.36	4.60	4.29
Supply chain traceability	3.36	3.30	2.89	2.93	3.14

Q16. Is the IT security budget part of or separate from the overall IT budget?	US	UK	EMEA	LATAM	Overall
Part of overall IT budget	51%	47%	57%	56%	53%
Separate budget	49%	53%	43%	44%	47%
Total	100%	100%	100%	100%	100%

Q17. What best describes the adequacy of the IT budget to achieve a strong security posture within your organization?	US	UK	EMEA	LATAM	Overall
More than adequate	12%	15%	16%	12%	14%
Adequate	40%	47%	56%	38%	45%
Less than adequate	48%	39%	28%	50%	41%
Total	100%	101%	100%	100%	100%

Q18a. Does your organization use metrics to evaluate the economic benefits of enabling security technologies deployed by your organization?	US	UK	EMEA	LATAM	Overall
Yes	54%	48%	45%	36%	47%
No	46%	52%	55%	64%	53%
Total	100%	100%	100%	100%	100%

Q18b. If yes, what metrics are used to evaluate the economic benefits? Please select all that apply.	US	UK	EMEA	LATAM	Overall
Return on investment (ROI)	68%	57%	55%	48%	58%
Total cost of ownership (TCO)	51%	45%	43%	40%	46%
Increase in threat prevention rates	35%	25%	32%	38%	33%
Increase in threat detection rates	34%	26%	30%	30%	30%
Decrease in false positive rates	57%	49%	43%	39%	48%
Increase speed in threat detection	33%	29%	27%	26%	29%
Increase speed in threat containment	29%	25%	25%	27%	27%
Increase speed in threat remediation	24%	21%	20%	19%	21%
Other (please specify)	3%	1%	4%	2%	3%
Total	334%	278%	278%	269%	295%

Q19. What factors does your organization consider when deploying security technologies? Please select all that apply.	US	UK	EMEA	LATAM	Overall
The licensing cost	57%	50%	47%	49%	51%
The maintenance cost	63%	48%	46%	44%	52%
Installation costs	61%	58%	56%	57%	58%
System performance issues (degradation)	49%	38%	39%	27%	40%
System effectiveness issues (high false positive)	52%	49%	47%	45%	49%
System complexity issues	63%	57%	60%	41%	57%
Personnel issues (lack of in-house expertise)	34%	46%	44%	49%	42%
Interoperability issues	67%	60%	63%	58%	63%
Scalability issues	61%	50%	51%	47%	53%
Vendor support issues	59%	57%	56%	46%	55%
Other (please specify)	3%	2%	0%	3%	2%
Total	569%	515%	509%	466%	522%

Part 4. Your Role & Organization Characteristics

D1. What organizational level best describes your current position?	US	UK	EMEA	LATAM	Overall
Senior Executive	6%	5%	4%	6%	5%
Vice President	3%	3%	2%	5%	3%
Director	15%	15%	15%	17%	16%
Manager	21%	24%	23%	18%	22%
Supervisor	14%	13%	12%	13%	13%
Technician	29%	28%	33%	29%	30%
Staff	7%	7%	6%	8%	7%
Contractor	3%	3%	2%	3%	3%
Other	2%	3%	2%	0%	2%
Total	100%	100%	100%	100%	100%

D2. What best describes your primary role in the organization?	US	UK	EMEA	LATAM	Overall
Application development	26%	23%	30%	25%	26%
Application security	24%	24%	25%	23%	24%
Security architecture	10%	9%	7%	11%	9%
IT management	12%	15%	12%	15%	13%
IT security	9%	10%	8%	8%	9%
Quality assurance	3%	3%	3%	3%	3%
Compliance/audit	5%	4%	5%	6%	5%
Risk management	2%	1%	2%	1%	2%
Network engineering	9%	8%	9%	8%	9%
Other	0%	2%	0%	0%	0%
Total	100%	100%	100%	100%	100%

D3. What industry best describes your organization's industry focus?	US	UK	EMEA	LATAM	Overall
Agriculture & food services	1%	2%	1%	2%	1%
Communications	2%	3%	3%	2%	3%
Consumer products	6%	5%	6%	5%	6%
Defense & aerospace	1%	0%	0%	2%	1%
Education & research	2%	3%	4%	2%	3%
Energy & utilities	5%	6%	6%	7%	6%
Entertainment & media	2%	2%	3%	1%	2%
Financial services	18%	16%	15%	16%	16%
Health & pharmaceuticals	11%	8%	11%	10%	10%
Hospitality	2%	3%	4%	3%	3%
Industrial & manufacturing	9%	12%	8%	11%	10%
Public sector	10%	12%	11%	9%	11%
Retail	9%	8%	8%	9%	9%
Services	10%	8%	10%	12%	10%
Technology & Software	9%	8%	8%	7%	8%
Transportation	2%	1%	2%	1%	2%
Other	1%	2%	0%	0%	1%
Total	100%	100%	100%	100%	100%

D4. What is the worldwide headcount of your organization?	US	UK	EMEA	LATAM	Overall
Less than 500	15%	21%	25%	25%	21%
500 to 1,000	21%	27%	27%	24%	24%
1,001 to 5,000	22%	20%	19%	21%	21%
5,001 to 10,000	17%	16%	15%	13%	16%
10,001 to 25,000	10%	8%	7%	9%	9%
25,001 to 75,000	7%	5%	3%	6%	5%
More than 75,000	8%	3%	4%	2%	5%
Total	100%	100%	100%	100%	100%

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

Ponemon Institute

Advancing Responsible Information Management

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

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