mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
#selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob

Separating the Truths from the Myths in Cybersecurity

Sponsored by BMC

Independently conducted by Ponemon Institute LLC

Publication Date: June 2018

Ponemon Institute© Research Report

Separating the Truths from the Myths in Cybersecurity

Prepared by Ponemon Institute, June 2018

Part 1. Introduction

Ponemon Institute, with sponsorship from BMC, conducted the study on *Separating the Truths from the Myths in Cybersecurity* to better understand the security myths that can be barriers to a more effective IT security function and to determine the truths that should be considered important for the overall security posture. In the context of this survey, cybersecurity truths are based on the actual experience of participants in this research. In contrast, cybersecurity myths are based on their perceptions, beliefs and gut feel.

More than 1,300 IT and IT security professionals in North America (NA), United Kingdom (UK) and EMEA who have various roles in IT operations and security were surveyed. All respondents are knowledgeable about their organizations' IT security strategies.

Separating the truths from the myths in cybersecurity

Following are statements about cybersecurity technologies, personnel and governance practices. Participants in this research were asked if these statements are considered truthful or if they are based solely on conjecture or gut feel (i.e. myth). Specifically, respondents rated each statement on a five-point scale from -2 = absolute myth, -1 = mostly myth, 0 = can't be determined, +1 = mostly truth and + 2 = absolute truth. The number shown next to each statement represents the average index value compiled from all responses in this study. As can be seen, all myths and truths are not equal and range from -1.04 to +0.78.

Drawing upon nonparametric statistical methods, we separated those statements that had a statistically significant positive value that was above 0 (i.e. truth) from those statements that had a statistically significant negative value at or below 0 (i.e. myth).[1]

Truth – The test statistic confirms the following statements are mostly believed to be a fact

1. There is a skills gap in the IT security field. +0.78
2. Security patches can cause greater risk of instability than the risk of a data breach +0.52
3. The cloud is cost effective because it is easier and faster to deploy new software and applications than on-premises +0.52
4. Greater visibility into al applications, data and devices and how they are connected lowers and organization's security risk. +0.45
5. Malicious or criminal attacks are the root cause of most data breaches. +0.42
6. A strong security posture enables companies to innovate and take risks that can lead to greater profitability. +0.33
7. IT security and IT operations work closely to make sure resolution and remediation of security problems are completed successfully. +0.22
8. Many organizations are suffering from investments in disjointed, non-integrated security products that increase cost and complexity. +0.09

Myth – test statistic confirms the following statements are mostly a myth

1. Too much security diminishes productivity. -1.04
2. A strong security posture does not affect consumer trust. (In other words, a strong security posture is considered beneficial to improving consumers' trust in the organization.) -0.87
3. Automation is going to reduce the need for IT security expertise. -0.55
4. Artificial intelligence and machine learning will reduce the need for IT security expertise. -0.50

[1] See: Wilcoxon-Mann-Whitney test as a nonparametric alternative to the t-test.

5. It is difficult or impossible to allocate the time and resources to patching vulnerabilities because it leads to costly business disruptions and downtime. -0.41
6. Insider threats are costlier to detect and contain than external attacks. -0.27
7. Nation state attacks are mainly a threat for government organizations. -0.24
8. Security intelligence tools provide too much information to be effective in investigating threats. -0.21

Part 2. Key takeaways

Current state of cybersecurity

Senior management believes in the importance of the IT security function. Sixty-one percent of respondents say their senior management **does not think** IT security is strictly a tactical activity that reduces its importance in the eyes of senior management. Respondents concur that IT security in their organization is considered a strategic imperative.

Companies face a shortage of skilled and competent in-house staff. According to another Ponemon Institute study[2] , 70 percent of chief information security officers and other IT security professionals surveyed say a lack of competent in-house staff is what they worry about most when trying to defend their companies against cyberattacks. Further, 65 percent of these respondents say the top reason they are likely to have a data breach is because they have inadequate in-house expertise.

Are tensions between the IT and IT security function diminishing the security of organizations? Fifty-six percent of respondents agree that there is tension between IT security and IT operations because of a lack of alignment of their different priorities. Specifically, IT operations is more concerned with the organization's business objectives and IT security is focused on securing the enterprise from cybersecurity threats.

However, many respondents believe that despite this tension, IT security and IT operations work closely to make sure resolution and remediation of security problems are completed successfully. Collaboration between these two groups can be improved through the use of tools that bring these two functions closer together and foster teamwork which will benefit the organization as a whole.

Investments in security technologies should be aligned with the overall IT strategy and not lead to complexity. While the priorities of IT security and IT operations are often not in alignment, investments in technologies are consistent with their organizations' overall IT strategy, according to 60 percent of respondents. However, respondents believe many organizations are suffering from investments in disjointed, non-integrated security products that increase cost and complexity.

Technology investments are often motivated by well-publicized data breaches. Fifty percent of respondents say data breaches that are widely reported in media can influence the decisions to purchase security technologies. While companies may purchase cyber insurance to manage the financial consequences of a data breach, only 34 percent of respondents say such a policy would reduce their investments in security technologies.

Creating a strong security posture

Visibility is important to creating a strong security posture. Investing in visibility and discovery solutions is an opportunity to reduce cybersecurity risks. However, more than half of all respondents (55 percent) say their organizations are not purchasing such solutions. Further, the lack of visibility into sensitive data, applications and platforms is why many companies are concerned about the security of both public and private clouds. Fifty-one percent of respondents say the public cloud is less secure than on-premises and 44 percent of respondents say the private cloud is less secure than on-premises.

[2] "What CISOs Worry about in 2018", a research study conducted by Ponemon Institute and sponsored by Opus, January 2018.

Compliance with privacy and security regulations is believed to improve the cybersecurity posture of organizations. The benefits of a strong cybersecurity posture include an increase in consumer trust and the ability to innovate and take risks that can lead to greater profitability.

A well-informed and involved CEO and board of directors strengthens a company's security posture. Fifty-five percent of respondents say a well-informed and involved CEO and board of directors is critical to a strong security posture. Respondents believe it is a myth that the CEO and board of directors are too far removed from day-to-day security events to provide effective oversight and compliance.

Automation improves cybersecurity posture but does not reduce the need for in-house expertise. Sixty-two percent of respondents say automation, artificial intelligence and machine learning is **not** going to reduce the need for IT expertise but will enhance the productivity and effectiveness of skilled staff. The combination of a cybersecurity skills shortage and the adoption of advanced technologies is influencing how job candidates are recruited and hired. Sixty percent of respondents believe that when hiring IT security personnel, it is more important for the candidate to have the proper training and credentials than to have the aptitude to be trained.

Preventing and remediating risks

Prevention of security incidents is very hard to accomplish. Sixty percent of respondents say their organizations tend to focus on rapid response to security incidents because prevention of these incidents is too hard to accomplish. However, most companies represented in this research do not believe they have an incident response plan that enables them to respond to a data breach in a timely and cost-effective manner.

An integrated, automated solution for vulnerability management is a proactive strategy for preventing and minimizing the risk of a data breach. Only 19 percent of respondents rate their organizations' ability to minimize or mitigate IT security risks as very high. One reason is that instead of focusing on prevention, 53 percent of respondents say their organizations' approach to dealing with threats is reactive.

Poor patch management practices need to be improved because poor patching can lead to a data breach. Sixty-eight percent of respondents believe that data breaches occur because patch management is poorly executed. In another Ponemon Institute study, [3] 57 percent of respondents who reported their companies had one or more data breaches in the past year say these breaches could have occurred because a patch was available for a known vulnerability but not applied.

To improve the patch management process, companies should consider replacing manual processes with automated solutions that will not lead to costly business disruptions and downtime. In the same Ponemon Institute study on patching vulnerabilities[4], 61 percent of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use manual processes and 55 percent of respondents agree that IT security spends more time navigating manual processes than responding to vulnerabilities which leads to an insurmountable response backlog. The study also estimates that the downtime companies experience because of patching vulnerabilities can average 23 hours per week.

The findings above are consistent with this study. Forty-five percent of respondents believe patching vulnerabilities is difficult because it often requires companies to disrupt business practices which causes downtime. Fifty-three percent of respondents believe when patching is

[3] "Today's State of Vulnerability Response: Patchwork Demands Attention," conducted by Ponemon Institute and sponsored by ServiceNow, April 2018.
[4] Ibid

not properly executed security patches can cause a greater risk of instability than the risk of a data breach.

Response to threats and security incidents is reactive. Instead of focusing on prevention, 53 percent of respondents say their organizations' approach to dealing with threats is reactive, focusing on the immediate threat or “hack du jour”. This underscores the need to automate vulnerability management and the patching of server and network devices. In addition, automation can increase the efficiency of staff and improve the quality of patch rollouts.

Part 3. Findings

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

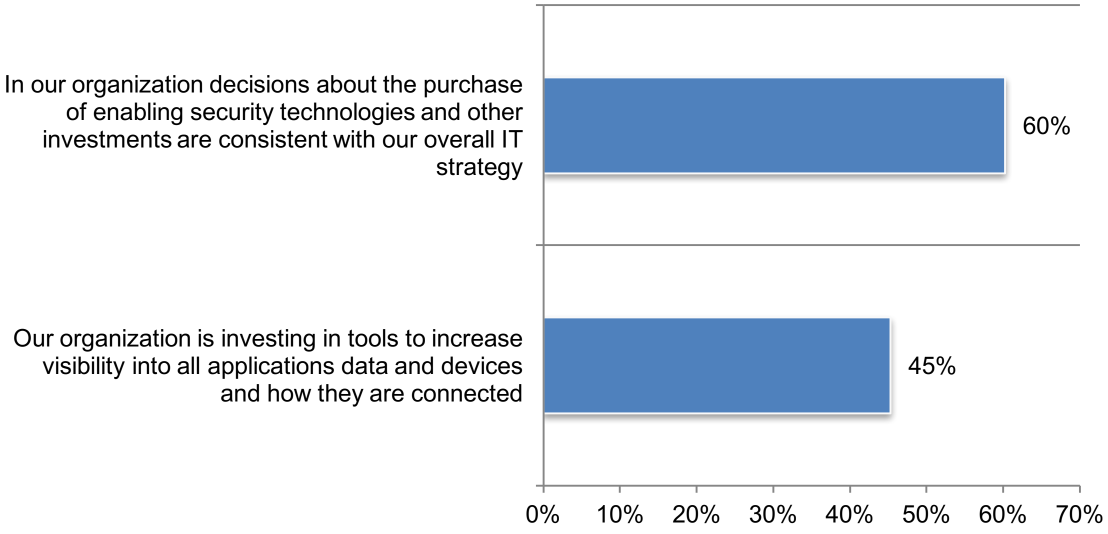
- What influences investments in technologies?
- Can the lack of proper patch management cause data breaches?
- What practices strengthen or diminish the security posture?
- What are the conflicts between IT operations and IT security?

What influences investments in technologies?

Despite the risk, many companies are not investing in technologies that increase visibility into applications, data and devices. As shown in Figure 1, only 45 percent of respondents say their organizations are investing in tools to increase visibility into all applications, data and devices and how they are connected. However, respondents believe it is a fact that greater visibility into all applications, data and devices and how they are connected lowers an organization's security risk.

Investments in security technologies are aligned with the overall IT strategies and tactics. While the priorities of IT security and IT operations are not in alignment, investments in technologies are consistent with the overall IT strategy, according to 60 percent of respondents.

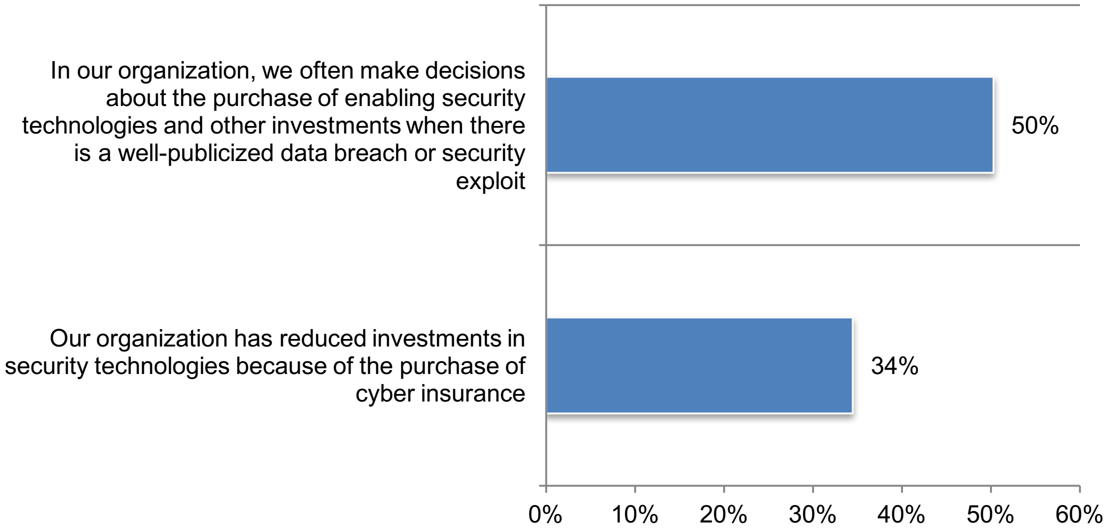
Figure 1. What influences investments in security technologies
Strongly Agree and Agree responses combined



Technology investments are often motivated by well-publicized data breaches. As shown in Figure 2, 50 percent of respondents say data breaches that are widely reported in media can influence the decisions to purchase security technologies. While companies may purchase cyber insurance to manage the financial consequences of a data breach, only 34 percent of respondents say such a policy would reduce their investments in security technologies.

When purchasing a technology are companies vetting the claims made by vendors or relying on a brochure? Almost half of respondents (49 percent) say marketing collateral is important when deciding whether or not to purchase a solution. On average, 28 percent of these purchases end up as shelfware and many organizations are suffering from investments in disjointed, non-integrated security products that increase cost and complexity.

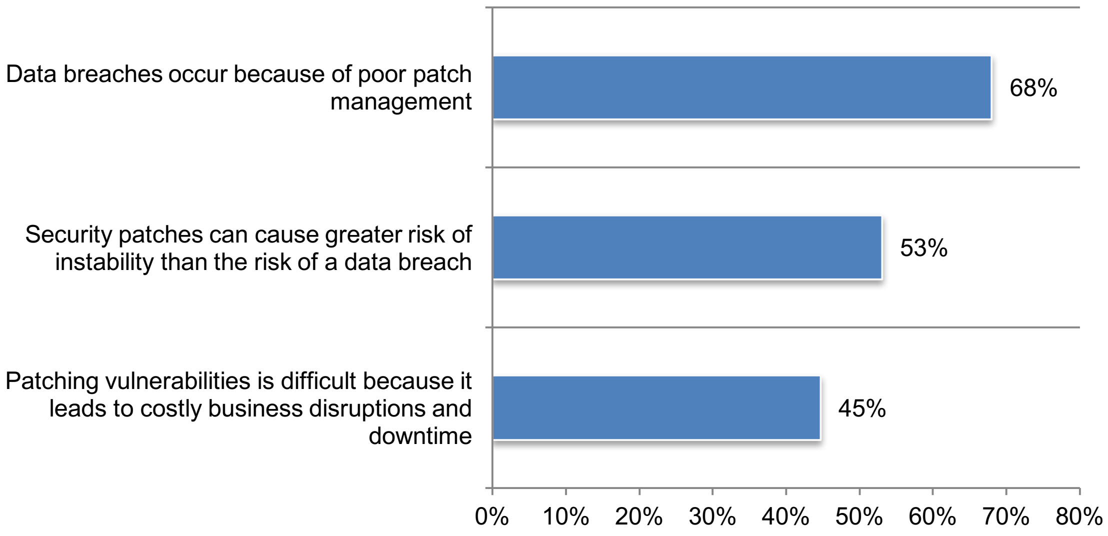
Figure 2. How purchasing decisions are made in security technologies
Strongly Agree and Agree responses combined



Can problems with patching lead to a data breach?

Poor patch management practices need to be improved because poor patching can lead to a data breach. According to Figure 3, 68 percent of respondents believe that data breaches occur because patch management is poorly executed. Companies should consider replacing manual processes with automated solutions that will not lead to costly business disruptions and downtime. As shown below, 45 percent of respondents believe patching vulnerabilities is difficult because it often requires companies to disrupt business practices which causes downtime. Fifty-three percent of respondents believe when patching is not properly executed security patches can cause a greater risk of instability than the risk of a data breach.

Figure 3. Patching vulnerabilities
Strongly Agree and Agree responses combined

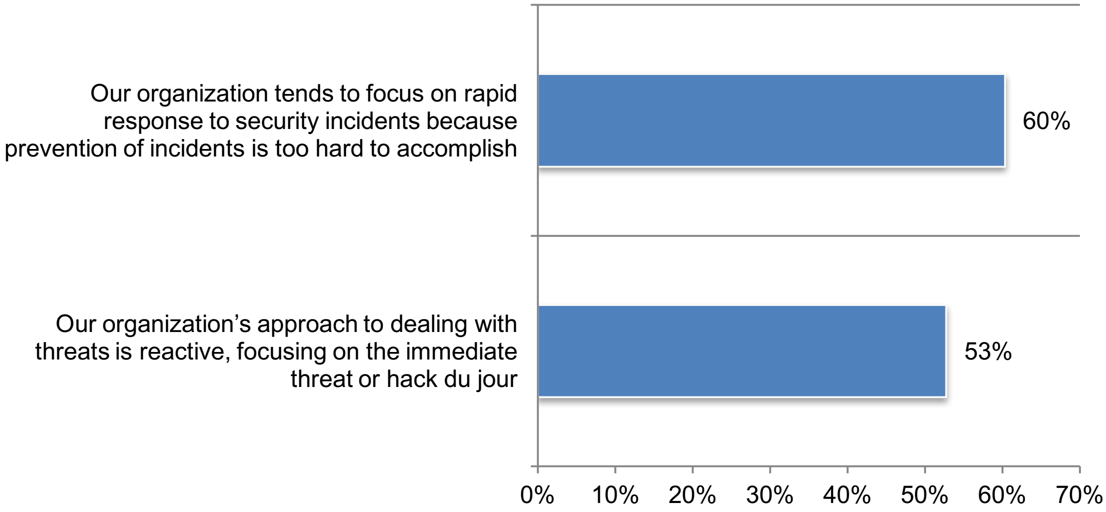


What practices strengthen or diminish an organization's security posture?

Response to threats and security incidents is reactive. Only 42 percent of respondents rate their organizations' ability to minimize or mitigate IT security risk as high. One reason for the lack of ability to more effectively address threats is shown in Figure 4. That is, instead of focusing on prevention, 53 percent of respondents say their organizations' approach to dealing with threats is reactive, focusing on the immediate threat or "hack du jour".

In addition, 60 percent of respondents say their organizations tend to focus on rapid response to security incidents because prevention of incidents is too hard to accomplish. However, such response efforts may not be effective because most companies do not have an incident response plan that enables them to respond to a data breach in a timely and cost-effective manner. These findings suggest that organizations need tools and technologies that help prevent breaches and incident response plans when such an incident occurs.

Figure 4. How organizations are preventing, detecting and responding to threats
Strongly Agree and Agree responses combined



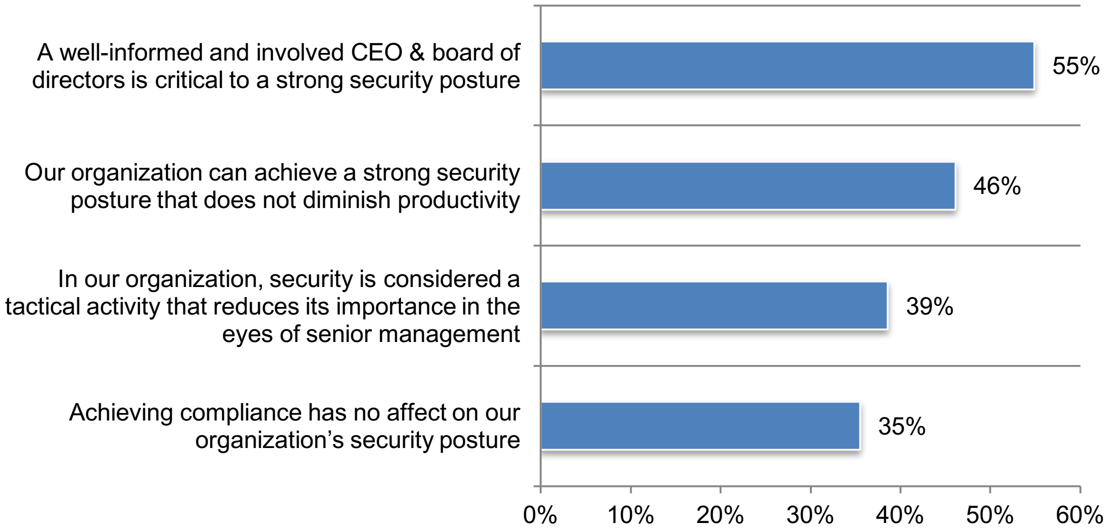
Replacing manual processes with automation helps companies achieve both a strong security posture without diminishing workplace productivity. The desire to have a strong security posture without affecting workplace productivity is difficult to accomplish. As shown in Figure 5, only 46 percent of respondents say their organization can achieve a strong security posture that does not diminish productivity. However, respondents believe organizations do not have to sacrifice productivity to have a strong security posture. This finding suggests the need for automation.

A strong security posture supports innovation and consumer trust. Respondents agree that a strong security posture enables companies to innovate and take risks that can lead to greater profitability. It also can increase consumer trust.

A well-informed and involved CEO and board of directors strengthens a company's security posture. Fifty-five percent of respondents say a well-informed and involved CEO and board of directors are critical to a strong security posture, as shown in Figure 5. Respondents believe the CEO and board of directors can provide effective oversight and guidance. Compliance with external and internal regulations is also important to achieving a stronger security posture (65 percent of respondents).

Senior management believes the IT security function is strategic and not tactical. Only 39 percent of respondents say their senior management thinks security is strictly a tactical activity that reduces its importance in the eyes of senior management. Respondents concur that it is a fact that IT security in their organization is considered a strategic imperative.

Figure 5. Perceptions about governance practices
Strongly Agree and Agree responses combined

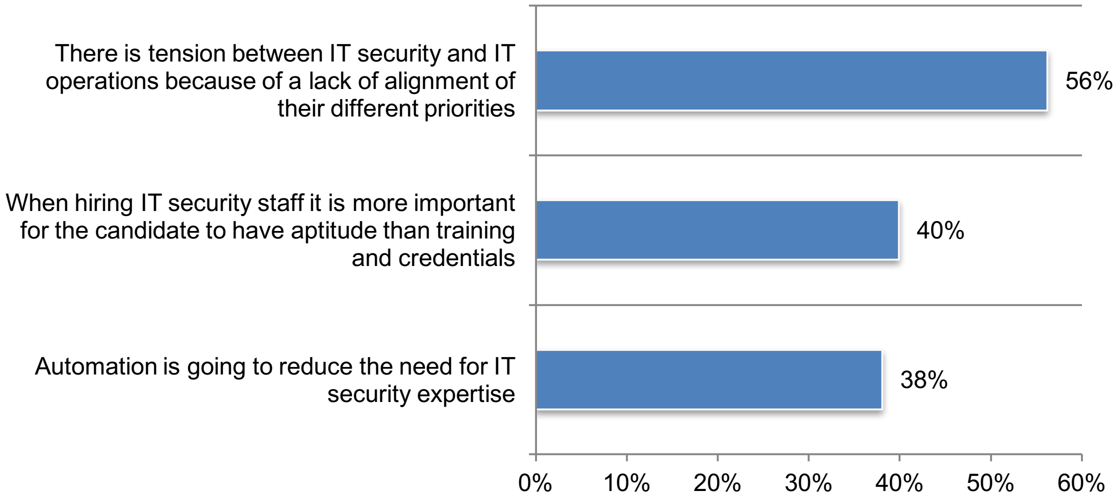


Automation improves cybersecurity posture but does not reduce the need for in-house expertise. Sixty-two percent of respondents say automation, artificial intelligence and machine learning is **not** going to reduce the need for IT expertise. Instead, organizations will benefit from having both automation and in-house expertise to improve their ability to prevent, detect and respond to security threats.

The combination of a skills shortage and the adoption of advanced technologies is influencing how job candidates are recruited and hired. Sixty percent of respondents believe that when hiring IT security personnel, it is more important for the candidate to have the proper training and credentials than to have the aptitude to be trained.

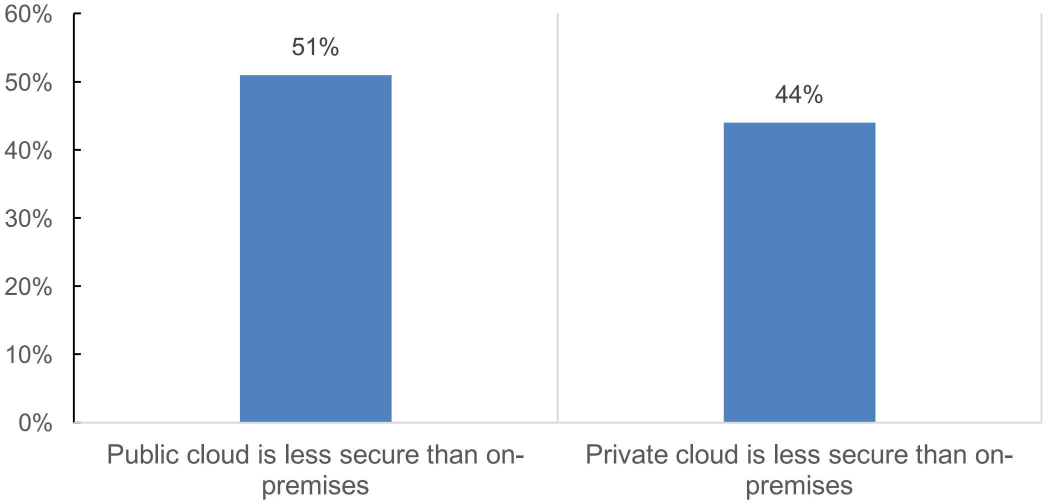
Are tensions between the IT and IT security functions diminishing the security of organizations? Fifty-six percent of respondents agree that there is tension between IT security and IT operations because of a lack of alignment of their different priorities. However, many respondents believe that despite this tension, IT security and IT operations work closely to make sure resolution and remediation of security problems are completed successfully.

Figure 6. Staffing issues in IT security
Strongly Agree and Agree responses combined



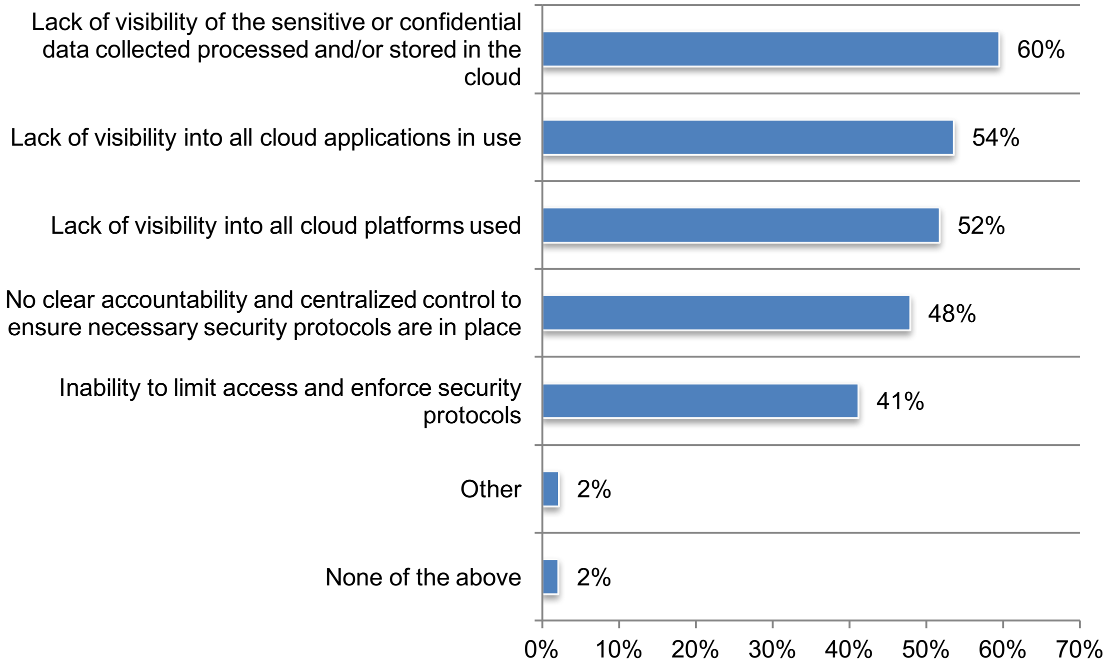
More respondents the public cloud is less secure than on-premises. As shown in Figure 7, 51 percent of respondents say the public cloud is less secure than on-premises and 44 percent of respondents say the private cloud is less secure than on-premises.

Figure 7. Are public and private clouds considered less secure than on-premises?
Yes response



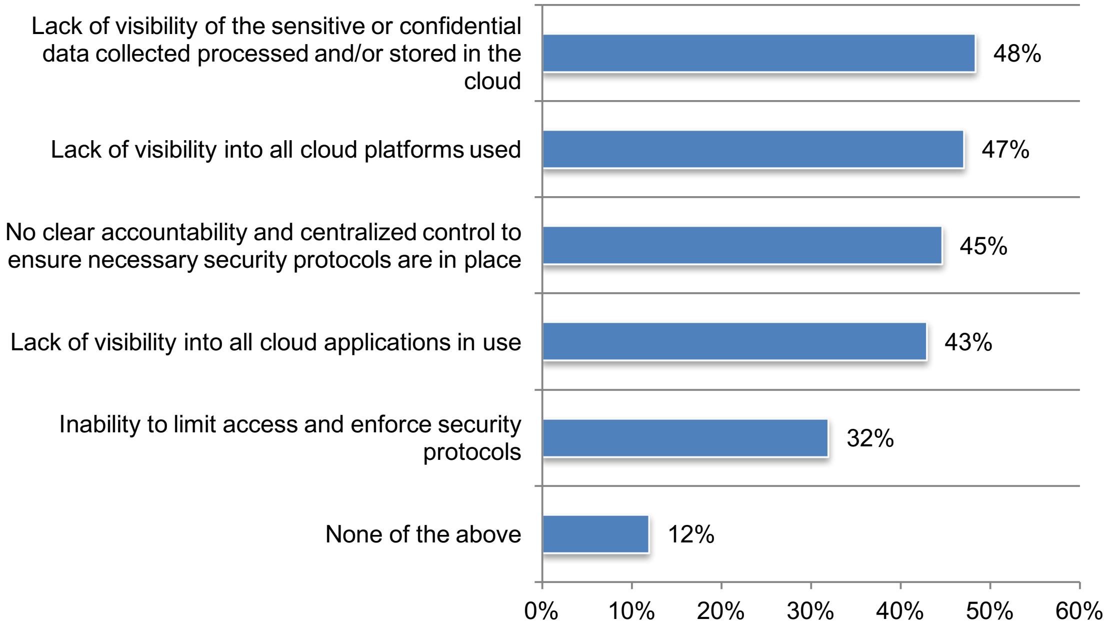
Lack of visibility is the barrier to a more secure public cloud. As shown above, more than half of respondents (51 percent) believe the public cloud is less secure than on-premises. Of these respondents, 60 percent say the lack of visibility of the sensitive or confidential data collected, processed and/or stored in the cloud. More than half say lack of visibility into all cloud applications and cloud platforms are used (54 percent and 52 percent, respectively).

Figure 8. Why is the public cloud less secure than on-premises?
More than one response permitted



Lack of visibility also makes the private cloud less secure than on-premises. Forty-four percent of respondents believe the private cloud is less secure than on-premises cloud. As shown in Figure 9, the two top reasons are the lack of visibility of the sensitive or confidential data collected, processed and/or stored in the cloud and into all cloud platforms used (48 percent and 47 percent respondents, respectively). Forty-five percent of respondents say security risks to the cloud are caused by no clear accountability and centralized controls to ensure necessary security protocols are in place.

Figure 9. Why is the private cloud less secure than on-premises?
More than one response permitted



Differences between IT operations and IT security put organizations at risk?

To understand the differences between IT operations and IT security that may be contributing to tensions between these groups, we did an analysis of how they responded to the survey questions. IT operations represents 50 percent of respondents and IT security represents 26.5 percent of respondents. Following are the most salient differences in how IT operations and IT security respondents perceive the importance of people, processes and technologies in IT security.

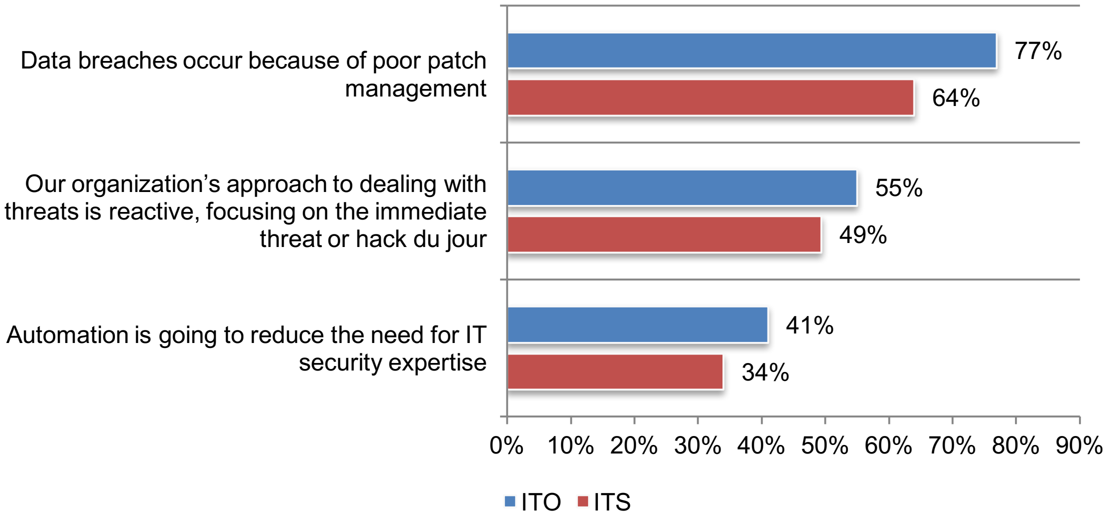
IT operations respondents are more likely to believe the following:

Data breaches occur because of poor patch management. Seventy-seven percent of IT operations believe patching should be properly managed to avoid a data breach.

Their companies' approach to dealing with threats is reactive. Fifty-five percent of IT operations say their organizations tend to focus on the immediate threat or "hack du jour". In contrast, less than half of IT security respondents (49 percent) say their organizations are more reactive than proactive when responding to threats.

Automation is going to reduce the need for IT security expertise. Forty-one percent of IT operations say headcount can be reduced because of automation. Only 34 percent of respondents in IT security believe this to be true.

Figure 10. IT operations perceptions
Strongly agree and Agree responses combined



IT security respondents are more likely to believe the following:

Well-publicized data breaches influence the purchase of enabling security technologies. More than half of IT security respondents (53 percent) say decisions about the purchase of enabling security technologies and other investments are made when there is a well-publicized data breach or security exploit. In contrast, only 37 percent of IT operations say media coverage of a data breach would affect investment decisions.

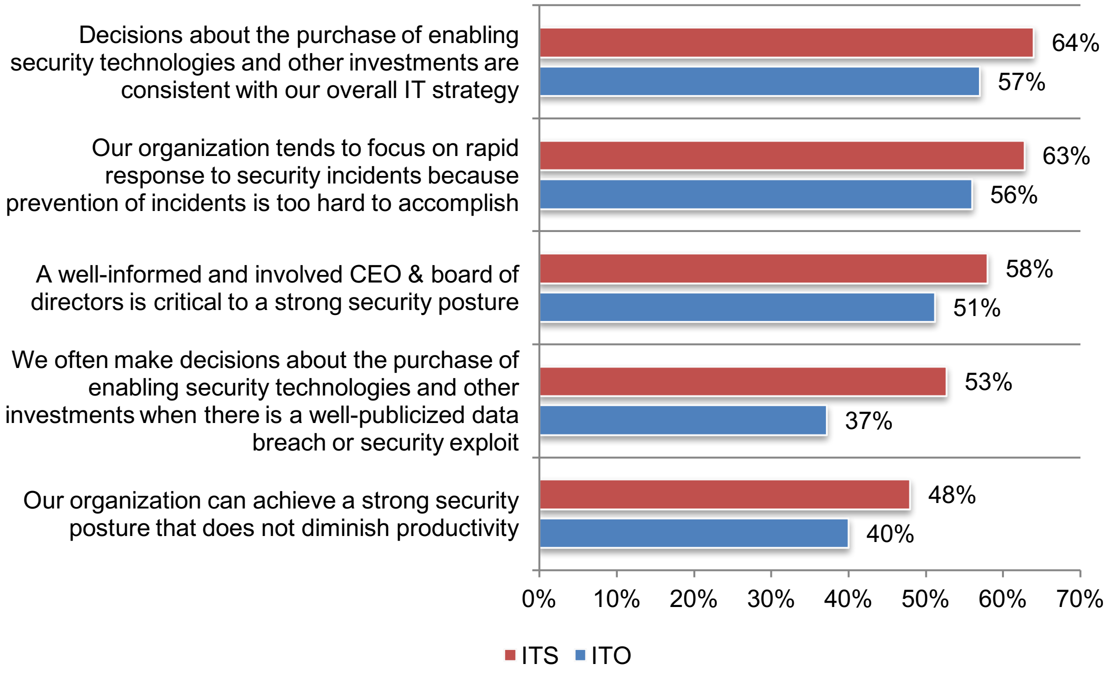
A strong security posture does not mean productivity is diminished. Almost half of IT security respondents (48 percent) believe productivity does not have to be sacrificed in order to have a strong security posture. Forty percent of IT operations are less confident in the ability to have both productivity and a strong security posture. Operations needs automated tools for vulnerability management.

Organizations focus on rapid response to security incidents. Sixty-three percent of IT security respondents say their organization tends to focus on rapid response to security incidents because prevention of incidents is too hard to accomplish. While 56 percent of IT operations believe this is the case.

A well-informed and involved CEO and board of directors improves the security posture of companies. Fifty-eight percent of IT security respondents believe involvement and an engaged CEO and board of directors is critical to a strong security posture.

Decisions about the purchase of enabling security technologies are aligned with the overall IT strategy. IT security respondents are more likely to believe that the investments made in security technologies are consistent with the companies' overall IT strategy.

Figure 11. Perceptions of IT security
Strongly agree and Agree responses combined



Agreement between IT operations respondents and IT security respondents:

There is tension between IT security and IT operations because of different priorities. Both groups acknowledge that tension exists because of a lack of alignment in their priorities. Fifty-five percent of IT operations and 60 percent of IT security respondents believe that because of different priorities there is tension between these two functions.

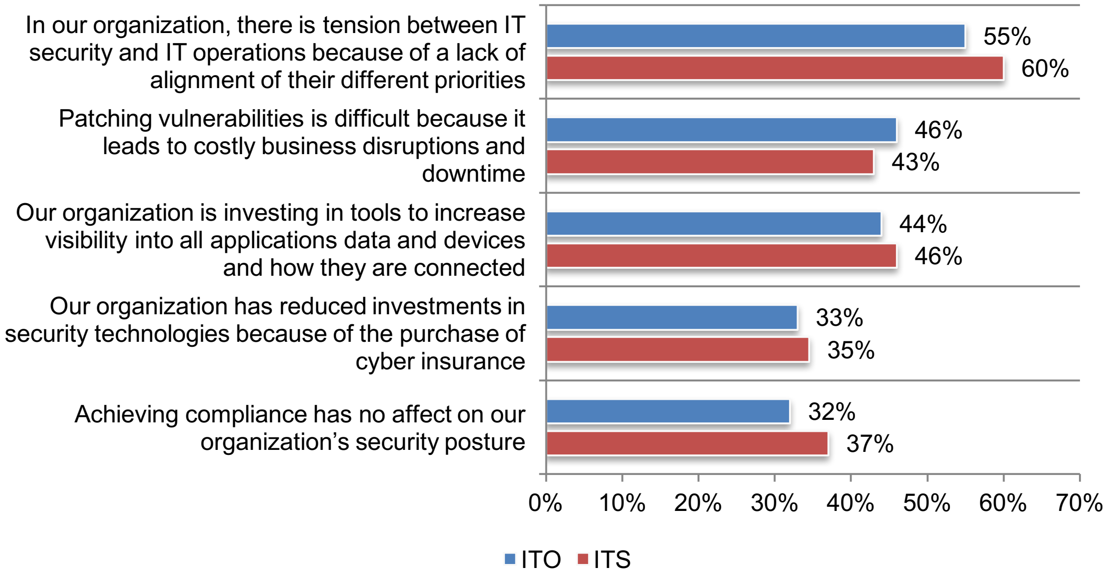
Patching vulnerabilities is difficult. Forty-three percent of IT security and 46 percent of IT operations agree that patching vulnerabilities is difficult because it leads to costly business disruptions and downtime. Another factor is the sheer volume of patches that need to be deployed.

Organizations are not investing in tools to increase visibility. Only 44 percent of IT operations and 46 percent of IT security respondents say their organizations are investing in tools to increase visibility into all applications, data and devices and how they are connected.

Cyber insurance is not reducing investment in security technologies. Only one-third of IT operations and 35 percent of IT security respondents say the purchase of cyber insurance has not reduced the need to invest in security technologies.

Compliance improves security posture. Less than one-third of IT operations (32 percent) and 37 percent of IT security respondents believe that achieving compliance has no effect on their companies' security posture.

Figure 12. IT operations and IT security areas of agreement
Strongly agree and Agree responses combined



Part 3. Methods

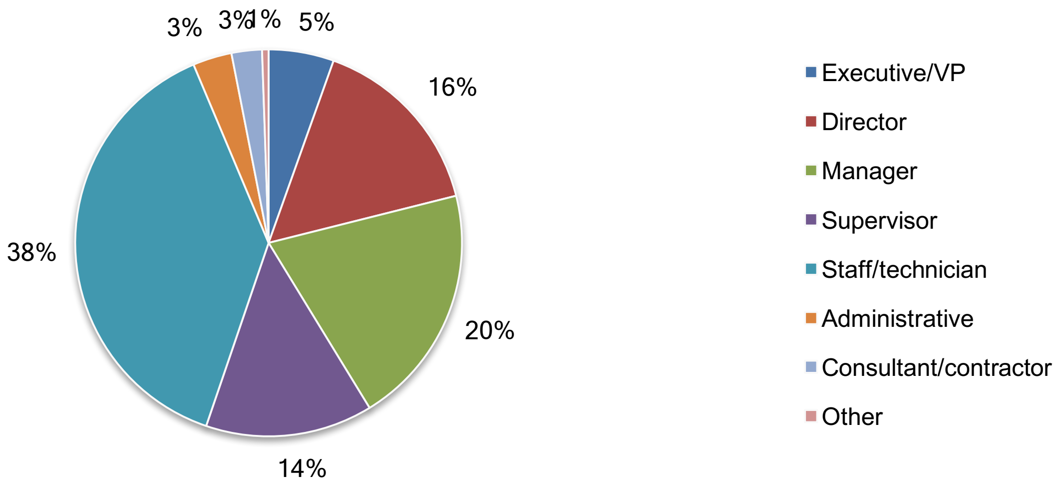
The sampling frame was composed of 40,194 IT and IT security practitioners located in North America, the United Kingdom and the EMEA region and who have various roles in IT operations and security. As shown in Table 1, 1,517 respondents completed the survey. Screening removed 191 surveys. The final sample was 1,326 surveys (or a 3.3 percent response rate).

Table 1. Sample response	NA	UK	EMEA*	Global
Total sampling frame	17,500	10,093	12,601	40,194
Total returns	679	402	436	1,517
Rejected or screened surveys	74	57	60	191
Final sample	605	345	376	1,326
Response rate	3.5%	3.4%	3.0%	3.3%

*The EMEA cluster sample does not contain UK respondents.

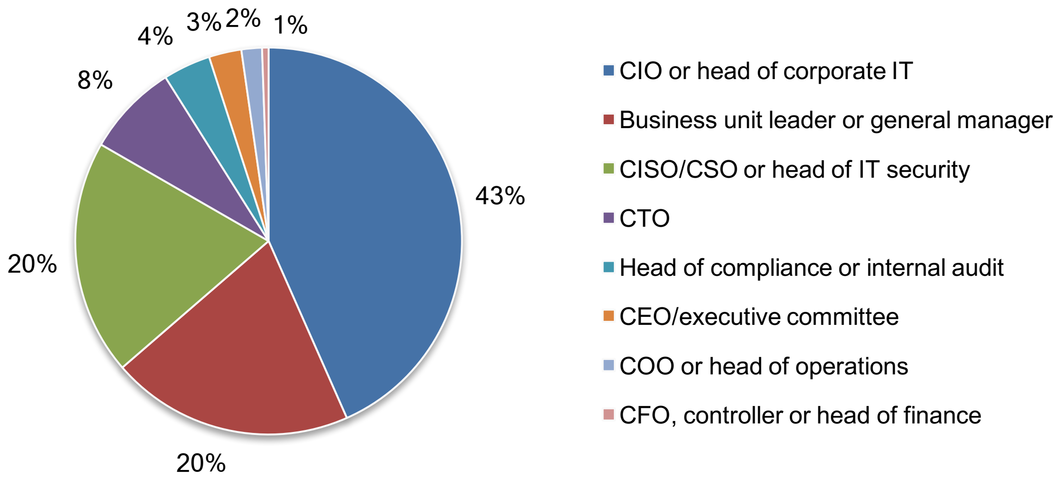
Pie Chart 1 reports the current position or organizational level of the respondents. Slightly more than half of respondents (55 percent) reported their current position as supervisory or above.

Pie Chart 1. Distribution of respondents according to position level



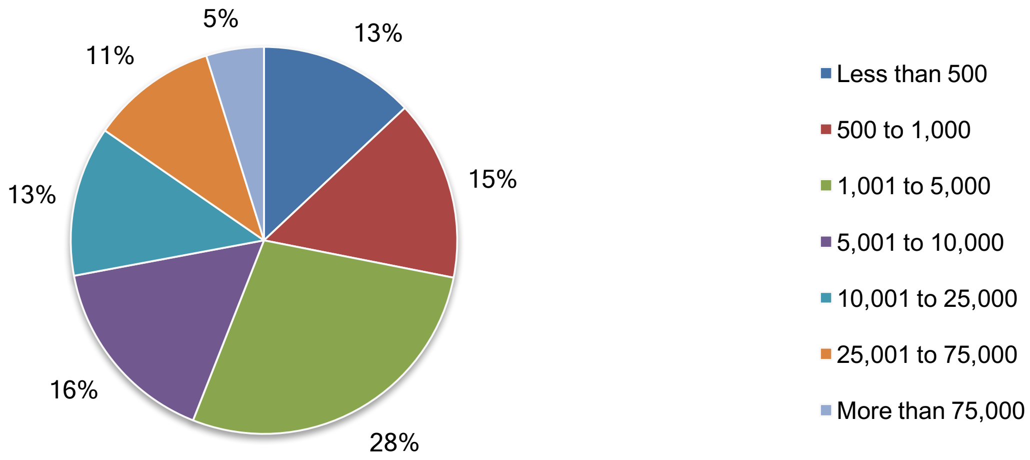
Pie Chart 2 identifies the primary person the respondent reports to within the organization. Forty-three percent of respondents identified the chief information officer or head of corporate IT as the person they report to. Another 20 percent of respondents indicated they report directly to the line of business unit leader or general manager, and 20 percent of respondents report to the chief information security officer/chief security officer or head of IT security.

Pie Chart 2. Distribution of respondents according to reporting channel



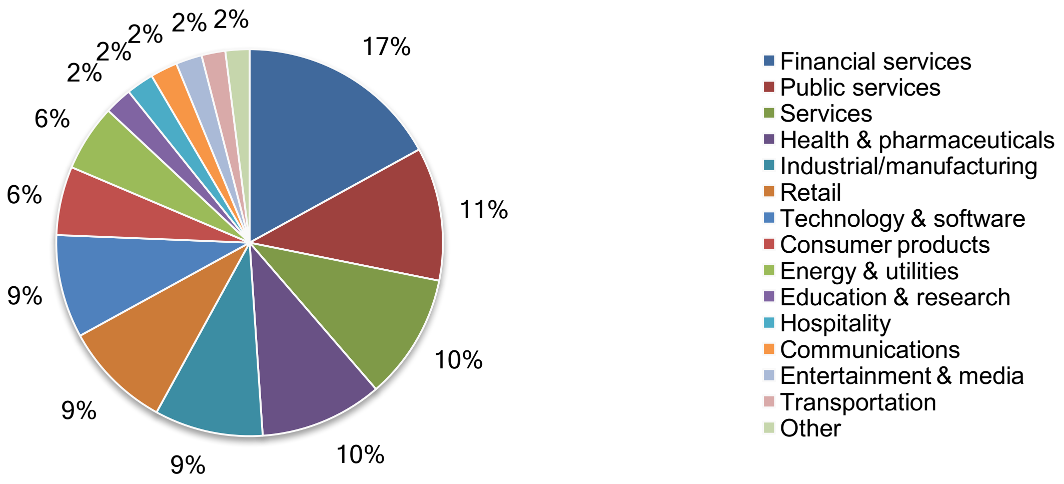
According to Pie Chart 3, more than half of the respondents (72 percent) are from organizations with a global head count of more than 1,000 employees.

Pie Chart 3. Distribution of respondents according to organizational head count



Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services as the largest segment (17 percent of respondents), followed by public services (11 percent of respondents), services sector (10 percent of respondents), health and pharmaceuticals (10 percent of respondents), industrial/manufacturing (9 percent of respondents), retail (9 percent of respondents) and technology and software (9 percent of respondents).

Pie chart 4. Distribution of respondents according to primary industry classification



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 various organizations in North America, the United Kingdom and the EMEA region. 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 in March 12 to March 26, 2018.

Survey response	Total
Total sampling frame	40,194
Total returns	1,517
Rejected surveys	191
Final sample	1,326
Response rate	3.3%
Sample weights	1.00

Part 1. Screening

S1. What best describes your role within your organization's IT or IT security department? Please select all that apply.	Total
Security leadership (CSO/CISO)	29%
IT management	38%
IT operations	53%
Security management	38%
Security monitoring and response	38%
Data administration	38%
Compliance administration	27%
Applications development	32%
Data Protection Office	10%
I'm not involved in my organization's IT or IT security function (stop)	0%
Total	304%

S2. How knowledgeable are you about your organization's IT security strategy and tactics?	Total
Very knowledgeable	30%
Knowledgeable	45%
Somewhat knowledgeable	25%
Slightly knowledgeable (stop)	0%
No knowledge (stop)	0%
Total	100%

S3. Please check all the activities that you see as part of your job or role.	Total
Managing budgets	36%
Evaluating vendors	45%
Setting priorities	36%
Securing systems	64%
Ensuring compliance	47%
Ensuring system availability	58%
None of the above (stop)	0%
Total	286%

Part 2. Facts and myths about technology, personnel and governance

Please rate the following statements using the five-point scale provided below each item. **Strongly Agree and Agree responses combined.**

Technology	Total
Q1a. The cloud is diminishing the need for on-premise IT security.	56%
Q1b. The cloud is cost effective because it is easier and faster to deploy new software and applications than on-premise.	74%
Q1c. As organizations re-write their apps to be cloud-enabled they are less secure than on-premises apps.	51%
Q1d. Data breaches occur because of poor patch management.	68%
Q1e. Security patches can cause greater risk of instability than the risk of a data breach.	53%
Q1f. Patching vulnerabilities is difficult because it leads to costly business disruptions and downtime.	45%
Q1g. Our organization is investing in tools to increase visibility into all applications data and devices and how they are connected.	45%

Governance	Total
Q1h. In our organization, security is considered a tactical activity that reduces its importance in the eyes of senior management.	39%
Q1i. Our organization can achieve a strong security posture that does not diminish productivity.	46%
Q1j. Our organization’s approach to dealing with threats is reactive, focusing on the immediate threat or hack du jour.	53%
Q1k. Our organization tends to focus on rapid response to security incidents because prevention of incidents is too hard to accomplish.	60%
Q1l. Achieving compliance has no affect on our organization’s security posture.	35%
Q1m. Our organization has reduced investments in security technologies because of the purchase of cyber insurance.	34%
Q1n. A well-informed and involved CEO & board of directors is critical to a strong security posture.	55%
Q1o. In our organization decisions about the purchase of enabling security technologies and other investments are consistent with our overall IT strategy.	60%
Q1p. In our organization, we often make decisions about the purchase of enabling security technologies and other investments when there is a well-publicized data breach or security exploit.	50%

Personnel	Total
Q1q. Automation is going to reduce the need for IT security expertise.	38%
Q1r. When hiring IT security staff it is more important for the candidate to have aptitude than training and credentials.	40%
Q1s. In our organization, there is tension between IT security and IT operations because of a lack of alignment of their different priorities.	56%

Part 3. Background

Q2. Using the following 10-point scale, please rate your organization's ability to minimize or mitigate IT security risk. 1 = low ability to 10 = high ability	Total
1 or 2	11%
3 or 4	19%
5 or 6	28%
7 or 8	23%
9 or 10	19%
Total	100%
Extrapolated value	5.91

Q3. Does your organization take a fact-based approach when deciding which investments in enabling security technologies are most appropriate?	Total
Mostly fact-based	52%
A combination of facts and informal indicators such as word-of-mouth or gut feel	37%
Mostly informal indicators such as word-of-mouth and gut feel	12%
Total	100%

Q4. Does your organization take a fact-based approach when deciding which investments to make in personnel?	Total
Mostly fact-based	53%
A combination of facts and informal indicators such as word-of-mouth or gut feel	38%
Mostly informal indicators such as word-of-mouth and gut feel	9%
Total	100%

Q5. Does your organization take a fact-based approach when making strategic decisions?	Total
Mostly fact-based	61%
A combination of facts and informal indicators such as word-of-mouth and gut feel	32%
Mostly informal indicators such as word-of-mouth and gut feel	7%
Total	100%

Q6. How important is marketing collateral when deciding on investments in enabling security technologies?	Total
Very important	24%
Important	25%
Somewhat important	17%
Not important	28%
Irrelevant	5%
Total	100%

Q7. What percentage of your organization's investments in enabling security technologies has not met expectations (e.g. shelfware)?	Total
None	4%
Less than 5%	10%
5 to 10%	16%
11 to 25%	31%
26 to 50%	21%
51 to 75%	12%
76 to 100%	7%
Total	100%
Extrapolated value	28.3%

Q8a. Is the public cloud less secure than on-premises?	Total
Yes	51%
No	49%
Total	100%

Q8b. If yes, why is the public cloud less secure? Please select all that apply.	Total
Lack of visibility into all cloud applications in use	54%
Lack of visibility into all cloud platforms used	52%
No clear accountability and centralized control to ensure necessary security protocols are in place	48%
Lack of visibility of the sensitive or confidential data collected processed and/or stored in the cloud	60%
Inability to limit access and enforce security protocols	41%
Other	2%
None of the above	2%
Total	258%

Q9a. Is the private cloud less secure than on-premises?	Total
Yes	44%
No	56%
Total	100%

Q9b. If yes, why is the private cloud less secure? Please select all that apply.	Total
Lack of visibility into all cloud applications in use	43%
Lack of visibility into all cloud platforms used	47%
No clear accountability and centralized control to ensure necessary security protocols are in place	45%
Lack of visibility of the sensitive or confidential data collected processed and/or stored in the cloud	48%
Inability to limit access and enforce security protocols	32%
Other	0%
None of the above	12%
Total	227%

Part 4. Is it fact or myth?

Following are statements about IT security technologies, personnel and governance practices. Based on your experience, please indicate how true the statements are (e.g. fact) or if they are based solely on conjecture (e.g. myth). Please rate each statement using the following five-point scale: -2=absolute myth, -1=mostly myth, 0=scale mean (denoting can't determine), +1=mostly fact and +2=absolute fact.

Technology

Q10. The cloud is diminishing the need for on-premise IT security.	Total
-2 [Absolute myth]	0.17
-1 [Mostly myth]	0.33
0 [Can't determine]	0.15
+1 [Mostly fact]	0.18
+2 [Absolute fact]	0.17
Total	1.00
Extrapolated value	(0.17)

Q11. The cloud is cost effective because it is easier and faster to deploy new software and applications than on-premise.	Total
-2 [Absolute myth]	0.08
-1 [Mostly myth]	0.14
0 [Can't determine]	0.17
+1 [Mostly fact]	0.39
+2 [Absolute fact]	0.22
Total	1.00
Extrapolated value	0.52

Q12. Security patches can cause greater risk of instability than the risk of a data breach.	Total
-2 [Absolute myth]	0.08
-1 [Mostly myth]	0.14
0 [Can't determine]	0.17
+1 [Mostly fact]	0.39
+2 [Absolute fact]	0.22
Total	1.00
Extrapolated value	0.52

Q13. Most data breaches are caused by failure to patch vulnerabilities in a timely manner.	Total
-2 [Absolute myth]	0.23
-1 [Mostly myth]	0.21
0 [Can't determine]	0.18
+1 [Mostly fact]	0.25
+2 [Absolute fact]	0.14
Total	1.00
Extrapolated value	(0.15)

Q14. It is difficult or impossible to patch because it leads to costly business disruptions and downtime.	Total
-2 [Absolute myth]	0.24
-1 [Mostly myth]	0.29
0 [Can't determine]	0.22
+1 [Mostly fact]	0.14
+2 [Absolute fact]	0.11
Total	1.00
Extrapolated value	(0.41)

Q15. Greater visibility into all applications, data and devices and how they are connected lowers an organization's security risk.	Total
-2 [Absolute myth]	0.10
-1 [Mostly myth]	0.10
0 [Can't determine]	0.21
+1 [Mostly fact]	0.40
+2 [Absolute fact]	0.18
Total	1.00
Extrapolated value	0.45

Q16. Most security intelligence tools provide too much information to be effective in investigating threats.	Total
-2 [Absolute myth]	0.26
-1 [Mostly myth]	0.24
0 [Can't determine]	0.12
+1 [Mostly fact]	0.19
+2 [Absolute fact]	0.18
Total	0.99
Extrapolated value	(0.21)

Q17. A strong security posture enables companies to innovate and take risks that can lead to greater profitability.	Total
-2 [Absolute myth]	0.13
-1 [Mostly myth]	0.20
0 [Can't determine]	0.16
+1 [Mostly fact]	0.24
+2 [Absolute fact]	0.27
Total	1.00
Extrapolated value	0.33

Q18. IT security is mostly tactical rather than a strategic imperative.	Total
-2 [Absolute myth]	0.25
-1 [Mostly myth]	0.20
0 [Can't determine]	0.12
+1 [Mostly fact]	0.22
+2 [Absolute fact]	0.21
Total	1.00
Extrapolated value	(0.06)

Q19. Insider threats are more costly to detect and contain than external attacks.	Total
-2 [Absolute myth]	0.29
-1 [Mostly myth]	0.21
0 [Can't determine]	0.13
+1 [Mostly fact]	0.23
+2 [Absolute fact]	0.14
Total	1.00
Extrapolated value	(0.27)

Q20. Malicious or criminal attacks are the root cause of most data breaches.	Total
-2 [Absolute myth]	0.12
-1 [Mostly myth]	0.15
0 [Can't determine]	0.22
+1 [Mostly fact]	0.21
+2 [Absolute fact]	0.30
Total	1.00
Extrapolated value	0.42

Q21. Too much security diminishes productivity.	Total
-2 [Absolute myth]	0.46
-1 [Mostly myth]	0.33
0 [Can't determine]	0.09
+1 [Mostly fact]	0.06
+2 [Absolute fact]	0.07
Total	1.00
Extrapolated value	(1.04)

Personnel

Q22. Nation state attacks are mainly a threat for government organizations.	Total
-2 [Absolute myth]	0.29
-1 [Mostly myth]	0.21
0 [Can't determine]	0.13
+1 [Mostly fact]	0.21
+2 [Absolute fact]	0.16
Total	1.00
Extrapolated value	(0.24)

Q23. A strong security posture does not affect consumer trust.	Total
-2 [Absolute myth]	0.43
-1 [Mostly myth]	0.27
0 [Can't determine]	0.11
+1 [Mostly fact]	0.12
+2 [Absolute fact]	0.07
Total	1.00
Extrapolated value	(0.87)

Q24. Many organizations are suffering from investments in disjointed, non-integrated security products that increase cost and complexity.	Total
-2 [Absolute myth]	0.20
-1 [Mostly myth]	0.18
0 [Can't determine]	0.18
+1 [Mostly fact]	0.19
+2 [Absolute fact]	0.24
Total	1.00
Extrapolated value	0.09

Q25. IT security and IT operations work closely to make sure resolution and remediation of security problems are completed successful.	Total
-2 [Absolute myth]	0.16
-1 [Mostly myth]	0.16
0 [Can't determine]	0.23
+1 [Mostly fact]	0.21
+2 [Absolute fact]	0.24
Total	1.00
Extrapolated value	0.22

Q26. Many companies are at risk because IT security and IT operations have conflicting objectives.	Total
-2 [Absolute myth]	0.18
-1 [Mostly myth]	0.23
0 [Can’t determine]	0.24
+1 [Mostly fact]	0.18
+2 [Absolute fact]	0.17
Total	1.00
Extrapolated value	(0.08)

Q27. Automation is going to reduce the need for IT security expertise.	Total
-2 [Absolute myth]	0.34
-1 [Mostly myth]	0.18
0 [Can’t determine]	0.25
+1 [Mostly fact]	0.12
+2 [Absolute fact]	0.10
Total	1.00
Extrapolated value	(0.55)

Q28. AI/machine learning is going to reduce the need for IT security expertise.	Total
-2 [Absolute myth]	0.33
-1 [Mostly myth]	0.19
0 [Can’t determine]	0.25
+1 [Mostly fact]	0.13
+2 [Absolute fact]	0.11
Total	1.00
Extrapolated value	(0.50)

Q29. There is a skills gap in the IT security field.	Total
-2 [Absolute myth]	0.08
-1 [Mostly myth]	0.11
0 [Can’t determine]	0.15
+1 [Mostly fact]	0.28
+2 [Absolute fact]	0.38
Total	1.00
Extrapolated value	0.78

Governance

Q30. Most companies have an incident response plan that enables them to respond to a data breach in a timely and cost-effective manner.	Total
-2 [Absolute myth]	0.24
-1 [Mostly myth]	0.19
0 [Can’t determine]	0.21
+1 [Mostly fact]	0.20
+2 [Absolute fact]	0.16
Total	1.00
Extrapolated value	(0.15)

Q31. The purchase of cyber insurance reduces the need to invest in security solutions.	Total
-2 [Absolute myth]	0.22
-1 [Mostly myth]	0.20
0 [Can't determine]	0.23
+1 [Mostly fact]	0.15
+2 [Absolute fact]	0.20
Total	1.00
Extrapolated value	(0.10)

Q32. The CEO and board of directors are too far removed from day-to-day security events to provide effective oversight and guidance.	Total
-2 [Absolute myth]	0.23
-1 [Mostly myth]	0.21
0 [Can't determine]	0.19
+1 [Mostly fact]	0.22
+2 [Absolute fact]	0.15
Total	1.00
Extrapolated value	(0.13)

Part 5. Organization and respondents' demographics

D1. What best describes your position level within the organization?	Total
Executive/VP	5%
Director	16%
Manager	20%
Supervisor	14%
Staff/technician	38%
Administrative	3%
Consultant/contractor	3%
Other	1%
Total	100%

D2. What best describes your direct reporting channel?	Total
CEO/executive committee	3%
COO or head of operations	2%
CFO, controller or head of finance	1%
CIO or head of corporate IT	43%
CTO	8%
Business unit leader or general manager	20%
Head of compliance or internal audit	4%
CISO/CSO or head of IT security	20%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Total
Less than 500	13%
500 to 1,000	15%
1,001 to 5,000	28%
5,001 to 10,000	16%
10,001 to 25,000	13%
25,001 to 75,000	11%
More than 75,000	5%
Total	100%

D4. What best describes your organization's primary industry classification?	Total
Agriculture & food services	1%
Communications	2%
Consumer products	6%
Defense & aerospace	0%
Education & research	2%
Energy & utilities	6%
Entertainment & media	2%
Financial services	17%
Health & pharmaceuticals	10%
Hospitality	2%
Industrial/manufacturing	9%
Public services	11%
Retail	9%
Services	10%
Technology & software	9%
Transportation	2%
Other	1%
Total	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.