

---

# The Evolving Role of CISOs

## and their Importance to the Business

August 2017



Independently conducted by Ponemon Institute LLC  
Sponsored by F5 Networks

# What's inside

Executive Summary	2
<b>Section 1: Key Takeaways</b>	3
Introduction	4
Key Takeaways	5
There is a shift toward security as a business priority	5
Key approaches for securing business operations despite the increasing severity and frequency of cyber exploits and data breaches	7
<b>Section 2: Key Findings</b>	9
The role and responsibilities of CISOs	10
Third-party risks	19
The evolution of the IT security function	23
Budgets and spending	34
<b>Section 3: Methods and Caveats</b>	36
Caveats	41
Appendix: Detailed survey results	42
Part 1: IT security ecosystem	42
Part 2: Controls, governance and technologies	56
Part 3: Budget, funding and investment decisions	58
Part 4: The CISO role	61
Part 5: Third parties and supply chain issues	61
Part 6: Security threats and issues	62
Part 7: Demographics and organizational characteristics	63

## Executive Summary

---

The realization is growing in the C-Suite that just one serious security incident or data breach could derail the growth and profitability of their companies because of the cost to remediate, fines and legal fees, and customer loss. As a result of this awareness, the role of the CISO is growing in importance, as is the need to have an enterprise-wide IT security strategy that supports the company's mission and goals.

<sup>1</sup>Countries represented in this research are: the United States, the United Kingdom, Germany, Brazil, Mexico, India, and China.

This research on the evolution and influence of the CISO is based on in-depth interviews with senior-level IT professionals (those with CISO level role and responsibility) at 184 companies in seven countries<sup>1</sup> to represent a global footprint. This report presents the consolidated global findings to better understand the nature of the CISO role and reveal insights, challenges, and approaches to security strategy in today's global threat landscape.

Participants in this research agree that as cyber attacks and other threats increase in frequency and sophistication, the CISO role will become more critical, especially in managing enterprise risk, deploying security analytics, and ensuring the security of Internet of Things (IoT) devices. However, to play a bigger role in their organizations, it is essential not only that CISOs have the necessary technical expertise and leadership skills, but also that they understand their companies' operations and be able to articulate IT security priorities from a business perspective.

SECTION

# 01

---



## Key Takeaways



## Introduction

---

What is a CISO, and what do they do? As the leader of cyber defense for an organization, the Chief Information Security Officer is rapidly becoming indispensable for an organization's survival. Hacks and malware infections were once uncommon occurrences that were isolated to just office automation IT processes.

But now, the drizzle and drops of sophisticated hacking attacks have grown to a hammering torrent of constant zero-day exploits and global malware pandemics. Combine this with our utter dependence on powerful but still embryonic and fragile technology like the IoT, cloud computing, and mobile-everything have transformed the Internet age into a period of cruel miracles for security professionals. New compliance regimes, like General Data Protection Regulation (GDPR), are challenging the status quo of many new IT processes, especially considering how much regulated data is entrenched in normal business processes. How CISOs make decisions and what influence they have is more important than ever.

But what do we know about CISOs? We know there are not enough of them and that is obvious. What do our CISOs look like? Traditionally CISOs have come from IT but that seems to be changing. How do they work? How much budget do they control? Do they focus on network security or application security? Is the CISO role part of the IT department or outside of IT? What challenges do they face? Does the rest of the business listen to them? How are supply chain and third party risks addressed? What do they see as the top and emerging threats?

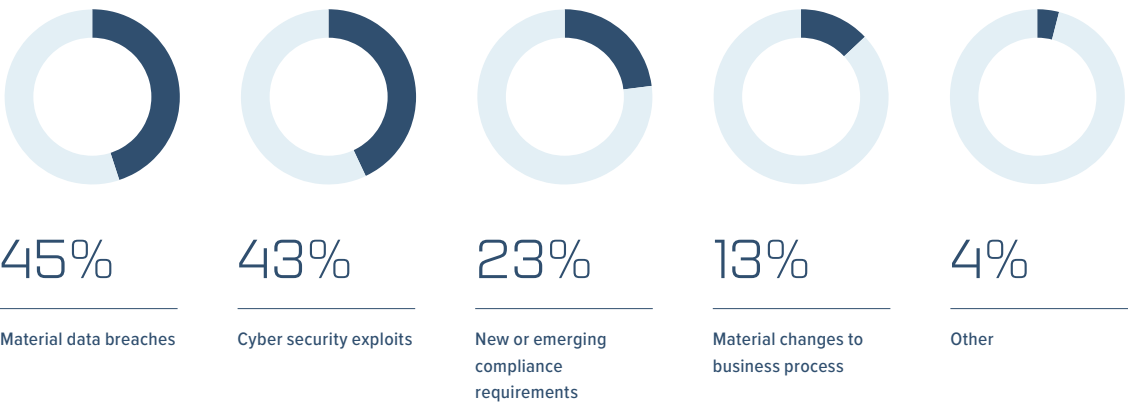
Given the mounting need for security expertise, knowing how CISOs work, what they are doing, and where they should reside within the organization is key to strengthening their capability, improving their effectiveness, and expanding their numbers. To that end, F5 Networks and the Ponemon Institute collaborated to help answer these questions.

## Key Takeaways

### There is a shift toward security as a business priority


**The relationship between an organization’s business priorities and its security posture is shifting.** According to 60 percent of respondents, material data breaches and cyber security exploits are driving change in organizations’ attitudes about their security programs, and 60 percent of respondents believe their organizations consider security to be a business priority. As shown in Figure 1, when asked what big developments are changing respondents’ attitudes about their organizations’ IT security programs, material data breach (45 percent) and cybersecurity exploit (43 percent) were the top two.

**FIGURE 1** EVENTS THAT CAUSE SECURITY TO BE TAKEN MORE SERIOUSLY BY THE C-SUITE  
(MORE THAN ONE RESPONSE ALLOWED.)



**There is a need for more opportunities to regularly report to the CEO and board of directors.** Today, it usually takes a data breach or serious security incident before the CISO is asked to present to the CEO and board of directors. Sixty percent of respondents say they have a direct channel to the CEO in the event of a serious security incident. However, only 19 percent of respondents say they report all data breaches to the CEO and board of directors.

Only 45 percent of respondents say they have an emergency fund to deal with a serious security incident that may require additional resources to resolve. As part of their responsibility to report on new threats, CISOs should be able to explain the cost impact of cyber crime and data breaches and the importance of having an appropriate budget.



According to one CISO, the IT security function will transform from a cost center to a revenue center; hence the CISO will be more involved in brand and reputation protection.

IT security should be enterprise-wide and capable of addressing new global regulations. The EU's GDPR, which will go into effect in May 2018, is a significant concern, as it will require many companies to change their business processes in order to be compliant. Because the regulation requires specific security practices to be implemented, the role of the CISO will be critical in ensuring the business can continue to confidently operate overseas.

The importance of preserving customer trust and reputation should be recognized. As shown in this study, ensuring the availability of IT services ranks much higher than preserving customer trust. However, there is more evidence that the loss of trust and reputation in the aftermath of a data breach has serious financial consequences.<sup>2</sup> Consequently, CISOs should communicate the steps taken to preserve the sensitive and confidential information of customers and business partners to minimize customer and reputational loss following a security incident.

By demonstrating the ability to reduce the risk of customer churn through practices that both secure confidential information and protect privacy, CISOs may gain the support of senior management. According to one CISO, the IT security function will transform from a cost center to a revenue center; hence the CISO will be more involved in brand and reputation protection.

<sup>2</sup> 2017 Cost of Data Breach Study: Global Overview, conducted by Ponemon Institute and sponsored by IBM Security, June 2017

---

**It's important to achieve alignment between IT security and lines of business.**

According to 58 percent of respondents, IT security is a standalone function and not integrated with other business functions. As a consequence, most companies in this study do not have an IT security strategy that spans the entire enterprise. Moreover, 57 percent of respondents say their security strategy is not reviewed, approved, and supported by C-level executives and 45 percent say their security function does not have clearly defined lines of responsibility.

Seventy-five percent of respondents say that due to the lack of integration, turf and silo issues have either a significant influence (36 percent) or some influence (39 percent) on IT security tactics and strategies. Thus, it is important for CISOs to work toward the integration of security in all business processes and to have direct influence over an enterprise-wide IT security strategy.

---

**Key approaches for securing business operations despite the increasing severity and frequency of cyber exploits and data breaches**

To strengthen the security posture of organizations, CISOs stress the importance of:

**An executive-level security leader with enterprise-wide responsibility**

The IT security leaders in this study believe enterprise-wide responsibility is the most important governance practice. Specifically, the appointment of an executive-level security leader with enterprise-wide responsibility is the number-one governance practice (69 percent of respondents).

**Strict enforcement of policies that protect the organization from insider negligence**

Although many companies represented in this study have guidelines and policies for minimizing malicious and negligent insider risk, only 35 percent of respondents say employees and immediate supervisors are held accountable for IT security infractions and non-compliance.

**Assessing the risks created by the Internet of Things**

Eighty percent of respondents say the IoT will cause significant or some change to their practices and requirements. However, most companies are not hiring or engaging IoT security experts and purchasing and deploying new security technologies to deal with potential new risks (41 percent and 32 percent of respondents, respectively).



---

**Holding third parties to a higher standard of security**

According to one CISO, third-party cyber risks will significantly increase, requiring closer collaboration between the CISO and lines of business leaders. Not all companies represented in this research have a process for evaluating the IT security capabilities of business partners, vendors, contractors, and other third parties, nor do they monitor third parties to ensure continued compliance with contractually required security requirements. Respondents say outsourcing security functions is considered an important option but creates risk. Almost half of respondents say outsourced services are never or only sometimes held to the same standard as on-premises security operations.

**Investing in technologies that enable the move from protecting the perimeter to endpoints, applications and data**

According to the findings, in the past two years, organizations' IT security posture has shifted from being dependent on network security to being dependent on application security. In the next two years, the IT security posture will be dependent on application and endpoint security.

SECTION

# 02

---



## Key Findings

## Key Findings

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

- The role and responsibilities of CISOs
- The importance of an enterprise-wide IT security strategy
- Third-party risks
- The evolution of the security function
- Budgets and spending

### The role and responsibilities of CISOs

Although today CISOs have varying degrees of influence among upper management in their organizations, most CISOs are influential in managing their companies’ cybersecurity risks, and it’s clear that their influence is growing.

FIGURE 2 CISOs’ INFLUENCE IN THE ORGANIZATION  
(MORE THAN ONE RESPONSE ALLOWED.)





# 68%

68 percent of respondents  
say CISOs have the final say  
in all IT security spending

### Most CISOs control the IT security staffing and spending in their organizations.

Sixty-eight percent of respondents say CISOs have the final say in all IT security spending, while a slightly smaller number (64 percent) say they have direct influence and authority over all security expenditures in their organizations. Sixty-seven percent are responsible for setting their organization's security strategy and related initiatives.

In terms of hiring, 66 percent of respondents say CISOs are responsible for overcoming the shortage of personnel with critical security skills and 62 percent say the CISO has direct influence over the hiring and firing of security personnel.

Fifty percent of respondents say risk management practices are incorporated in the evaluation of their organization's security programs, and 70 percent say risk informs their organization's security culture.

FIGURE 3

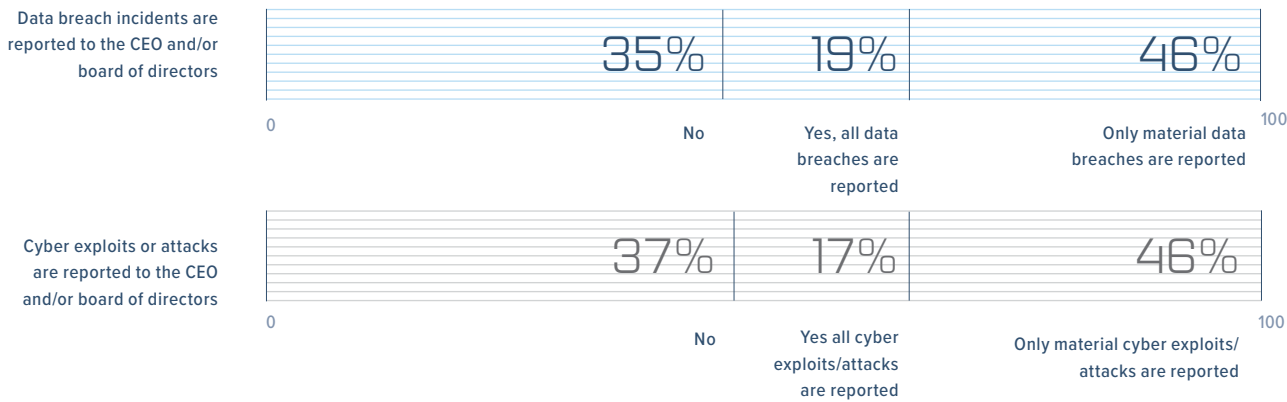
### HOW MUCH DOES RISK INFORM YOUR ORGANIZATION'S SECURITY CULTURE?



CISOs should not wait until a crisis to inform the CEO and board of directors about potential threats to the organization.

Although 65 percent of respondents say they report to senior executives, most often it is to report a crisis. As shown in Figure 4, 46 percent of respondents said only material data breaches and material cyber attacks are reported to the CEO and/or board of directors. 35 percent of respondents say no data breaches and 37 percent of respondents say no material cyber attacks are reported to the board.

FIGURE 4 CISOS COMMUNICATION WITH THE CEO AND BOARD OF DIRECTORS

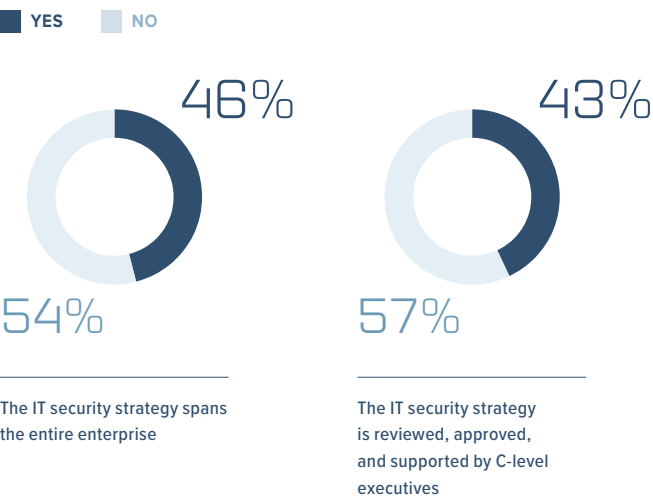




The importance of an enterprise-wide IT security strategy.

The belief that more organizations need to have an IT security strategy that extends throughout the enterprise and is supported by the C-suite is growing among senior IT professionals.

FIGURE 5 IS THE SECURITY STRATEGY ENTERPRISE-WIDE AND SUPPORTED BY C-LEVEL EXECUTIVES?



IT security is not integrated with other business functions or physical security operations, and in many cases there are no clearly defined lines of responsibility.

Only 22 percent of respondents say their organizations' security function is integrated with other business functions and 50 percent say IT security is not integrated with physical security operations. Furthermore, 45 percent of respondents say their security function does not have clearly defined lines of responsibility.

FIGURE 6 IS IT SECURITY CONSIDERED A STANDALONE FUNCTION?



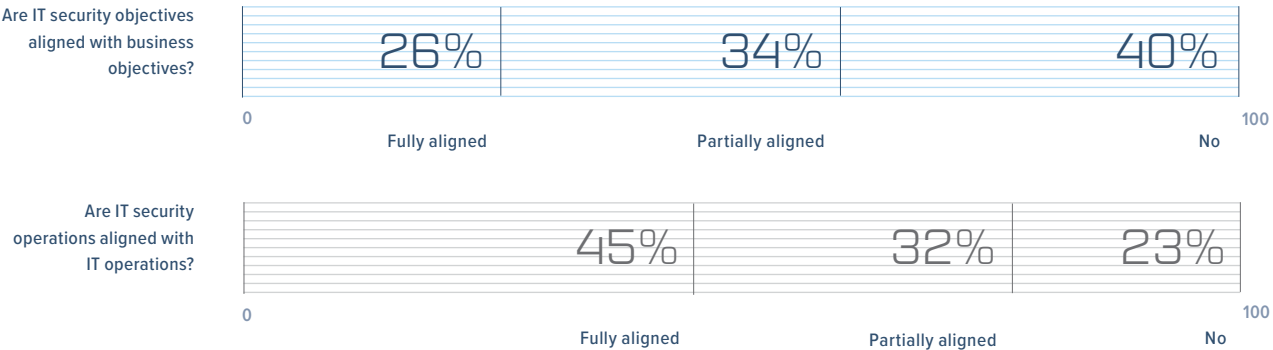
**An IT security strategy that is aligned with lines of business will help CISOs address turf and silo issues.**  
Seventy-five percent of respondents say turf and silo issues have a significant influence or some influence on IT security tactics and strategies, as shown in Figure 7.

**FIGURE 7** DO TURF AND SILO ISSUES INFLUENCE YOUR ORGANIZATION'S IT SECURITY TACTICS AND STRATEGY?



**IT security and IT operations have achieved alignment in most organizations.**  
Whereas 77 percent of respondents say their IT security operations are aligned with IT operations, fewer respondents (60 percent) say they have achieved alignment of IT security operations with business objectives.

**FIGURE 8** ARE IT SECURITY OBJECTIVES ALIGNED WITH BUSINESS AND IT OPERATIONS?



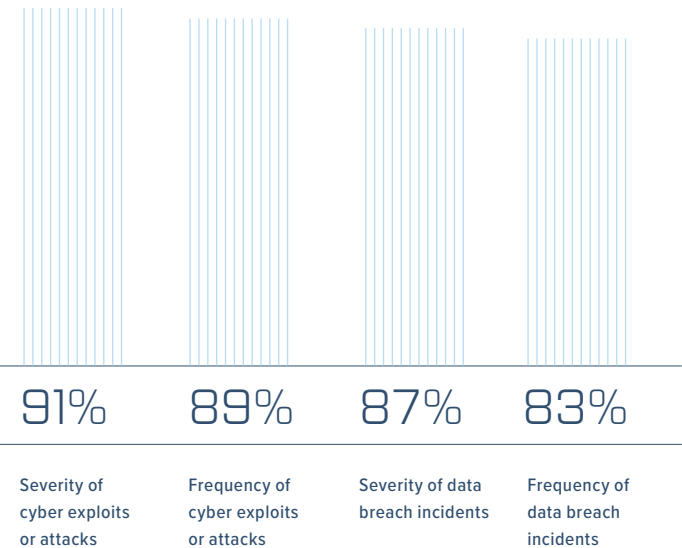
**Data breach and cyber incidents will not decrease in frequency or severity.**

As mentioned previously, material data breaches and cyber security exploits are making security a business priority and, as shown in Figure 9, the frequency and severity of cyber incidents will continue to plague companies.

On average, organizations represented in this study experienced two data breaches in the past 24 months. Eighty-three percent of respondents say the frequency of data breach will increase (39 percent) or stay the same (44 percent) and 87 percent say the severity of data breach incidents will increase (41 percent) or stay the same (46 percent).

Eighty-nine percent of respondents say cyber exploits will increase (40 percent) or stay the same (49 percent). Ninety-one percent say the severity of cyber exploits or attacks will increase (46 percent) or stay the same (45 percent). In interviews, participants predicted that new, dangerous forms of malware will emerge and ransomware attacks will morph into more costly forms of cyber extortion.

**FIGURE 9** WHAT WILL HAPPEN WITH THE FREQUENCY AND SEVERITY OF DATA BREACHES AND CYBER INCIDENTS OVER THE NEXT 24 MONTHS?  
(INCREASE AND STAY THE SAME RESPONSES ARE COMBINED.)



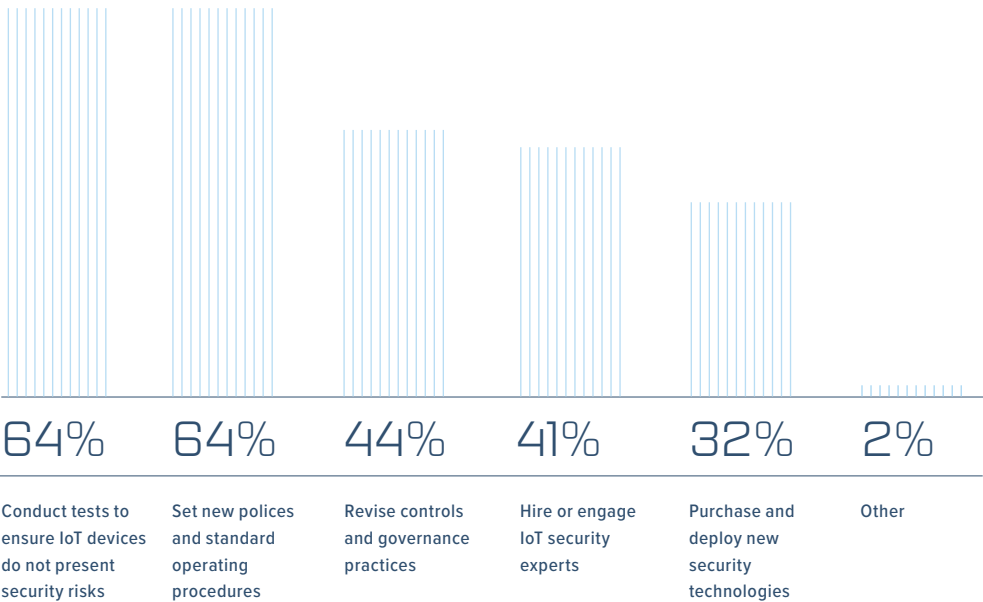
CISOs recognize that the IoT will affect their IT security practices or requirements.

In the context of this research, IoT is defined as the network of physical objects or “things” embedded with electronics, software, sensors, and network connectivity, which enables them to collect, monitor, and exchange data. Examples of IoT devices in the workplace include network-connected printers and building automation solutions.

Eighty percent of respondents say IoT will cause significant change (49 percent) or some change (31 percent) to their practices and requirements. However, only 22 percent say their organizations are evaluating the risk of IoT devices and applications before they are deployed throughout the organization.

As shown in Figure 10, the most significant changes are include setting new policies and standard operating procedures and conducting tests to ensure IoT devices do not present security risks. Only 32 percent of respondents say they have purchased and deployed new security technologies.

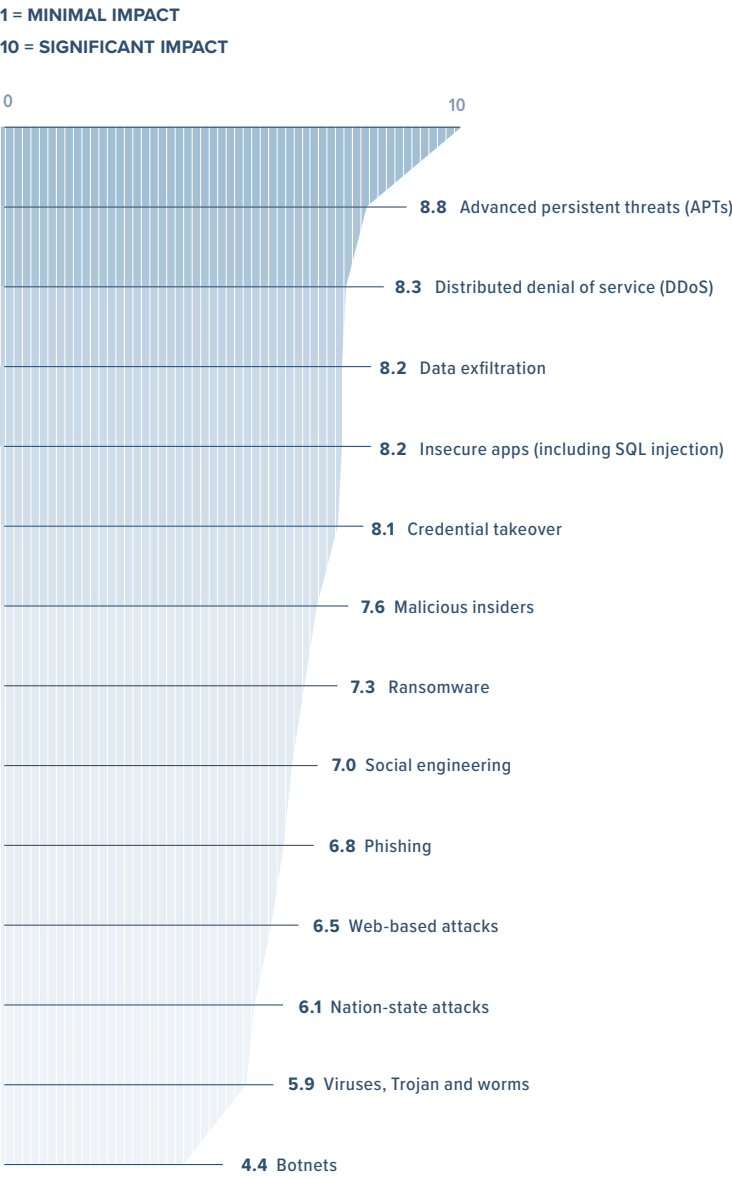
FIGURE 10 CHANGES COMPANIES ARE MAKING TO ADDRESS POTENTIAL RISKS CREATED BY THE IOT (MORE THAN ONE RESPONSE ALLOWED.)



**APTs and DDoS attacks are considered more serious than viruses and botnets.**

In the current threat landscape, advanced persistent threats (APTs) and distributed denial-of-service (DDoS) attacks top the list of threats respondents are concerned about.

**FIGURE 11**      **RESPONDENTS RANKED THE TOP THREATS TO THEIR SECURITY ECOSYSTEM**

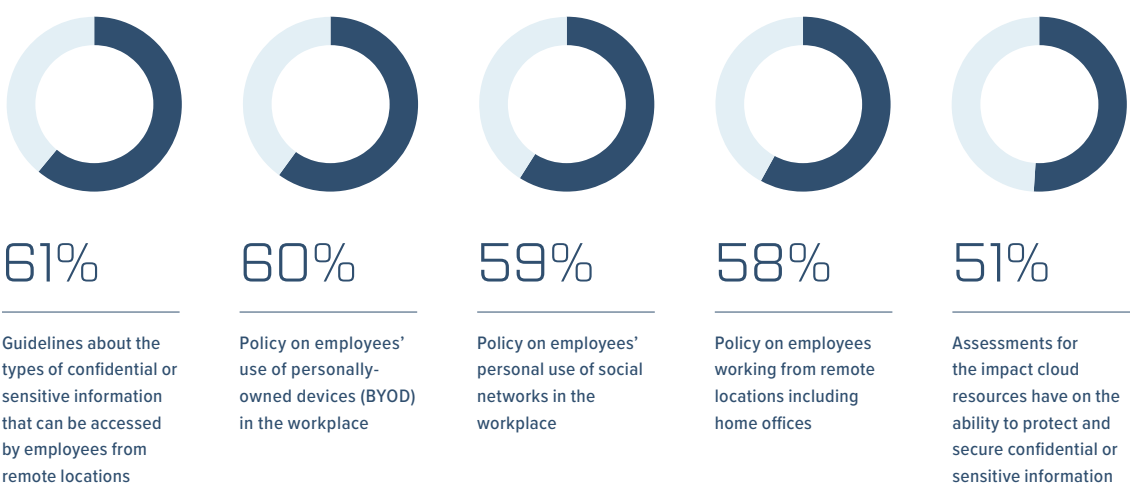




Organizations have established policies and guidelines for employees to address emerging threats to their IT security ecosystem, including use of personally owned devices (BYOD), personal use of social networks in the workplace, and employees' working from remote locations, including home offices.

More than half of respondents have guidelines as to the types of confidential or sensitive information that can be accessed by employees from remote locations, and 51 percent of respondents say their organization assesses the impact of cloud resources on their ability to protect and secure confidential or sensitive information.

**FIGURE 12**    **RESPONDENTS NOTED WHICH POLICIES AND GUIDELINES THEY USE TO ADDRESS NEGLIGENCE AND MALICIOUS INSIDER THREATS**  
(MORE THAN ONE RESPONSE ALLOWED.)



**Policies to minimize insider risks are not enforced.**

IT security policies are monitored for compliance by 63 percent of respondents. However, only 35 percent of respondents say employees and their immediate supervisors are held strictly accountable for IT security infractions or non-compliance with the company's policies. Thirty-two percent say employees and supervisors are held accountable but with exceptions, and 33 percent say they are not held accountable at all.



Third-party risks

CISOs admit their organizations’ business partners, vendors, and other third parties are not always held to high security standards.

Unfortunately, third parties such as business partners and vendors are not often held to high security standards, exposing organizations to risk of a data breach.

FIGURE 13

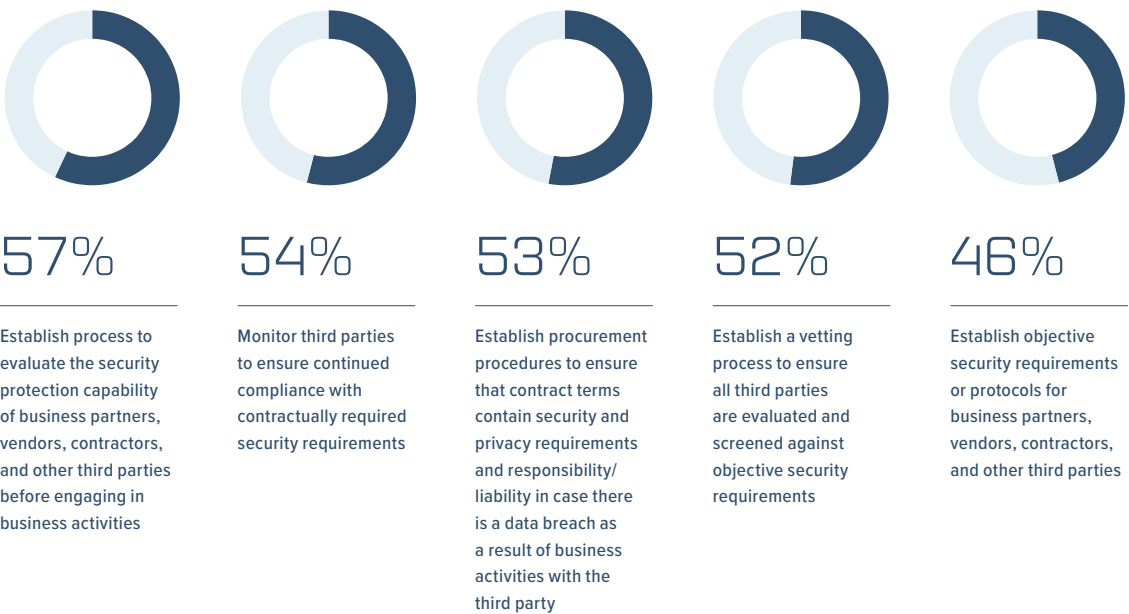
ARE YOUR ORGANIZATION’S BUSINESS PARTNERS, VENDORS, AND OTHER THIRD PARTIES HELD TO HIGH SECURITY STANDARDS?



Many organizations have a process for evaluating the IT security capabilities of business partners, vendors, contractors, and other third parties.

More than half monitor third parties to ensure continued compliance with contractually required security requirements. Still, CISOs admit that despite these activities, third parties are not held to a high security standard.

FIGURE 14 TOP IT SECURITY ACTIVITIES RESPONDENTS USE TO MINIMIZE THIRD-PARTY RISKS  
(MORE THAN ONE RESPONSE ALLOWED.)



Respondents acknowledged a number of other processes for minimizing third-party risk that are more stringent than those in Figure 14, but less frequently deployed.

**FIGURE 15** OTHER IT SECURITY ACTIVITIES RESPONDENTS USE TO MINIMIZE THIRD-PARTY RISKS  
(MORE THAN ONE RESPONSE ALLOWED.)



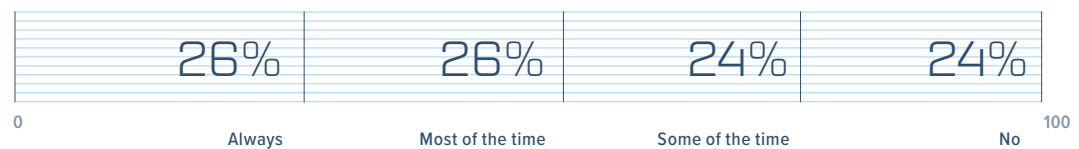


69% of respondents consider the appointment of an executive-level security leader with enterprise-wide responsibility as an organization's most important governance practice.

Additionally, the ability to outsource security functions is considered an important option but it also creates risks, as outsourced functions may not be held to the same standards as on-premises security operations (Figure 16).

FIGURE 16

ARE OUTSOURCED SERVICES HELD TO THE SAME STANDARDS AS ON-PREMISES SECURITY OPERATIONS?





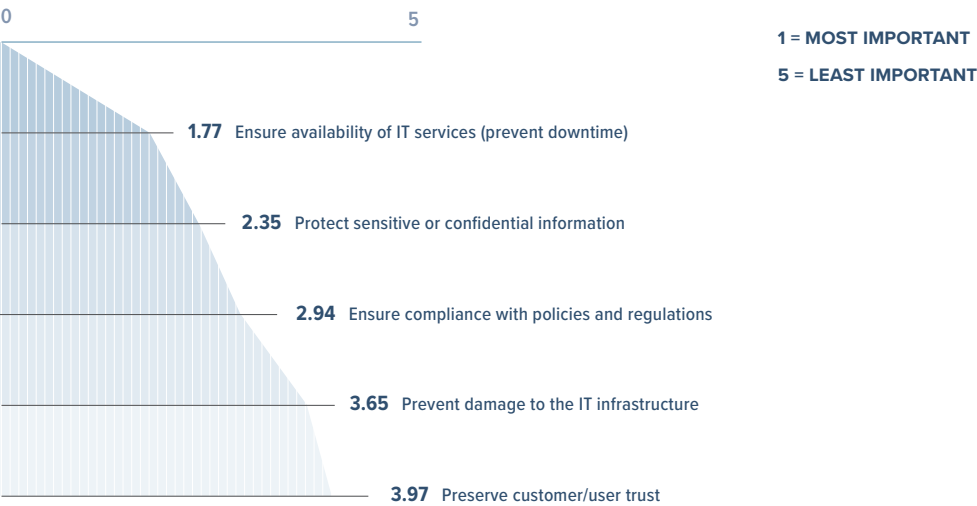
## The evolution of the IT security function

**The most important mission of IT security is to ensure availability of IT services.**

To gain the support of senior management, CISOs need to recognize the importance of preserving customer and user trust. This can be achieved by demonstrating the ability to reduce the risk of customer churn through practices that both secure confidential information and protect privacy.

Respondents felt that CISOs’ most critical responsibility is downtime prevention (see Figure 17). It is also important to protect sensitive or confidential information and ensure compliance with policies and regulations.

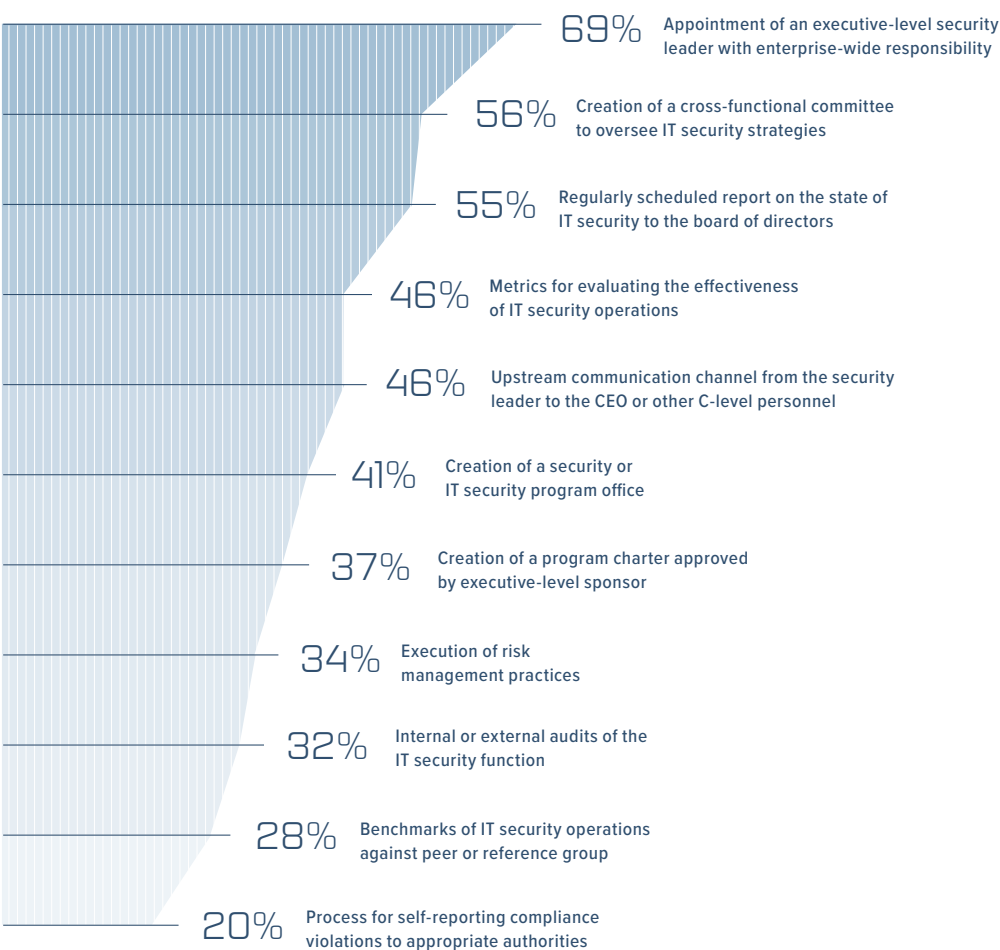
FIGURE 17 WHAT IS THE CISO’S MOST IMPORTANT MISSION?



**CISOs believe in the importance of an executive-level security leader with enterprise-wide responsibility.**

The IT security leaders in this study believe an enterprise-wide strategy is the most important governance practice. Specifically, respondents consider the appointment of an executive-level security leader with enterprise-wide responsibility as an organization’s most important governance practice (69 percent of respondents), as shown in Figure 18.

**FIGURE 18** SECURITY CONTROLS AND GOVERNANCE PRACTICES CONSIDERED MOST IMPORTANT  
(MORE THAN ONE RESPONSE ALLOWED.)



**Computer learning and artificial intelligence might help solve staffing shortages.**

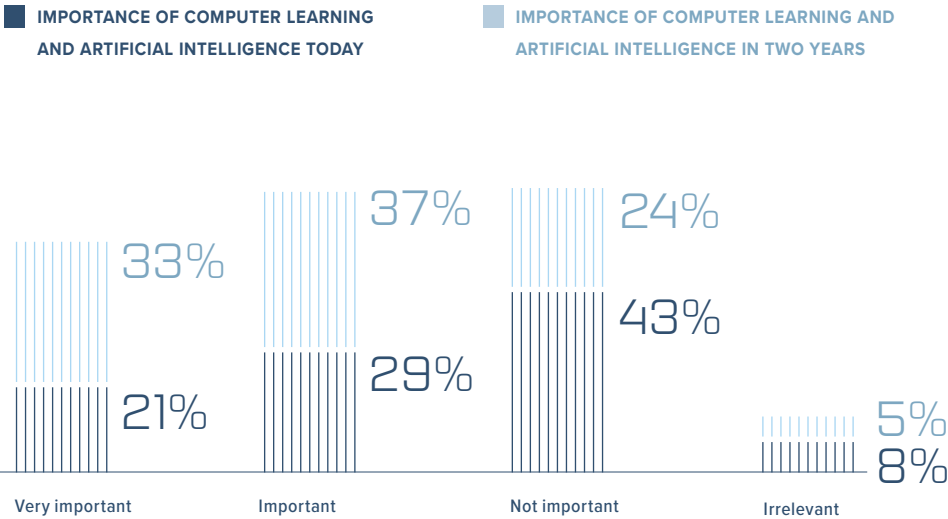
The biggest challenge to having adequate staffing and expertise is identifying and recruiting qualified candidates (56 percent of respondents), followed by the inability to offer a market-level salary (48 percent of respondents).

The average headcount of IT security personnel will increase from 19 to 32 full-time (or equivalent) employees. Slightly more than half (51 percent) say they have adequate headcount for meeting their organization’s security mission and/or strategy but 42 percent say their staffing is not adequate.

As shown in Figure 19, 50 percent of respondents believe computer learning and artificial intelligence are considered important today to address staffing shortages, and 70 percent of respondents say these technologies will be important to their IT security functions in two years.

FIGURE 19

**HOW IMPORTANT ARE COMPUTER LEARNING AND ARTIFICIAL INTELLIGENCE FOR RESPONDENTS’ ORGANIZATIONS?**



Global cultural and regulatory differences influence 72 percent of organizations' local security requirements.

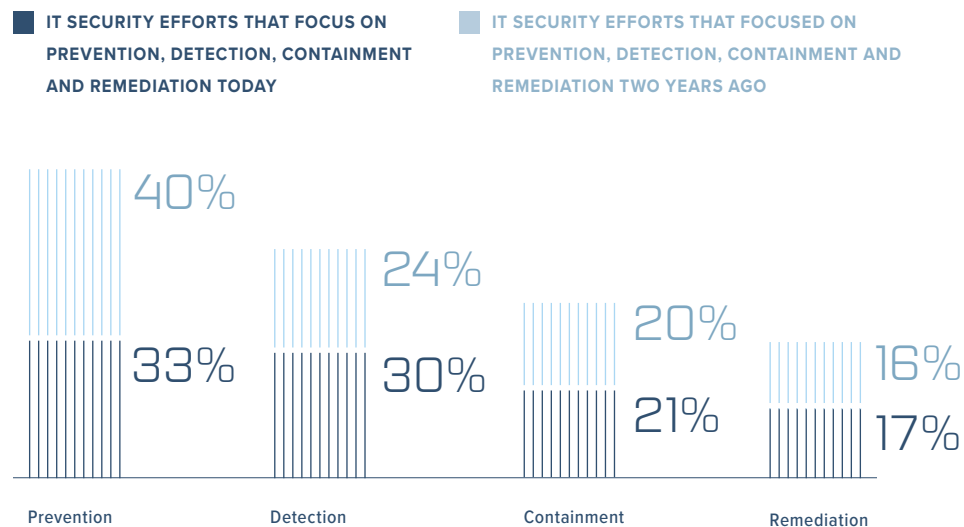


**Security efforts are shifting from prevention to detection.**

Two years ago, 40 percent of respondents focused on prevention and 24 percent focused on detection. Today, that gap is significantly smaller: 33 percent focus on prevention, while 30 percent focus on detection.

FIGURE 20

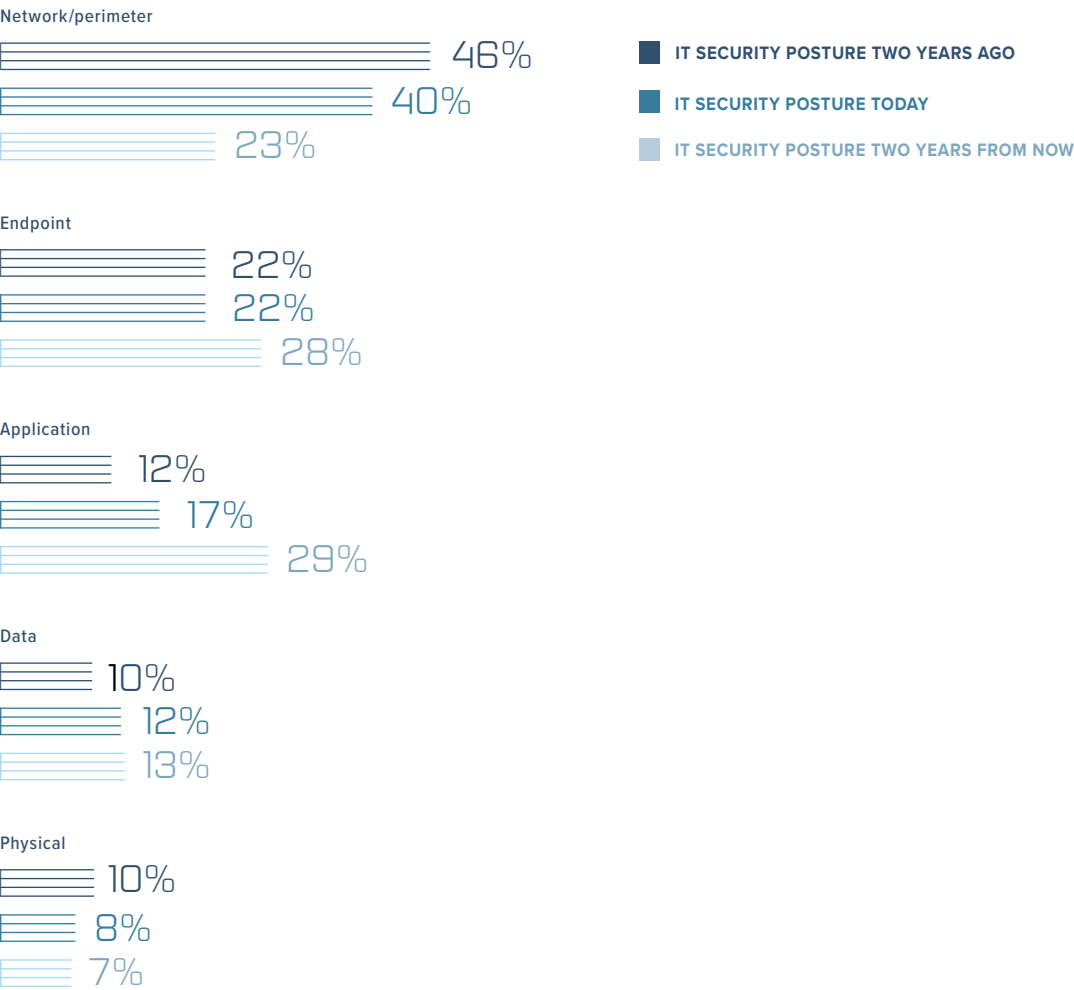
**WHAT DO ORGANIZATIONS FOCUS THEIR IT SECURITY EFFORTS ON?**



Security efforts are evolving from protecting the network and the traditional network perimeter to protecting applications and endpoints.

In the past two years, IT security postures have shifted from being dependent on network security to application security. In the next two years, IT security postures will be dependent on application and endpoint security, as shown in Figure 21.

FIGURE 21 HOW MUCH HAS (AND WILL) IT'S SECURITY POSTURE DEPEND ON NETWORK SECURITY, ENDPOINT SECURITY, APPLICATION SECURITY, DATA SECURITY, AND PHYSICAL SECURITY?





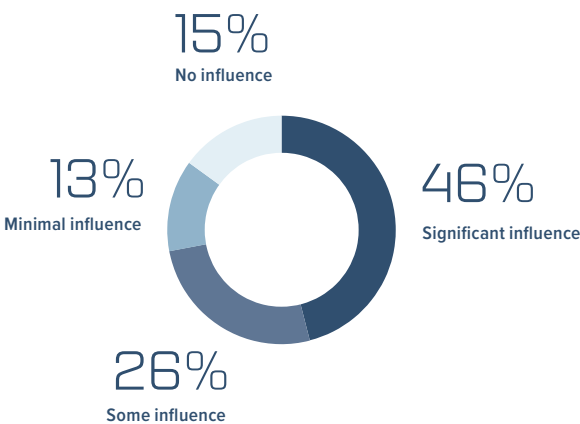
**Global cultural and regulatory differences, including the General Data Protection Regulation (GDPR), are affecting the IT security function.**

The reach of the new regulation is more expansive than that of previous regulations. Specifically, any company outside of the EU that is targeting consumers in the EU will be subject to the GDPR. As shown in Figure 22, 72 percent of respondents say cultural differences among people and business operations around the globe influence their organizations' local security requirements.

The most difficult security requirement to meet is the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident. The pseudonymization and encryption of personal data is also difficult.<sup>3</sup>

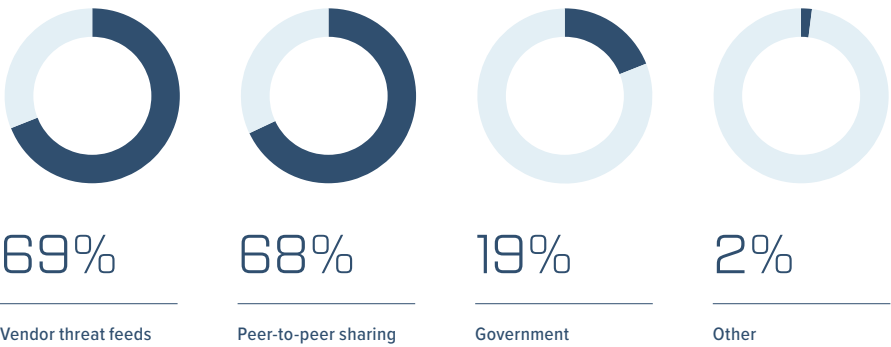
<sup>3</sup> See Data Protection Risk & Regulations in the Global Economy, conducted by Ponemon Institute and sponsored by Experian Data Breach Resolution, June 2017

**FIGURE 22** DO GLOBAL CULTURAL DIFFERENCES INFLUENCE YOUR ORGANIZATION'S SECURITY REQUIREMENTS?



**CISOs value threat intelligence about their organization or industry (52 percent of respondents).**  
They overwhelmingly favor vendor threat feeds and peer-to-peer sharing as information sources.

**FIGURE 23** SOURCES OF THREAT INTELLIGENCE THAT CISOS CONSUME  
(MORE THAN ONE RESPONSE ALLOWED.)



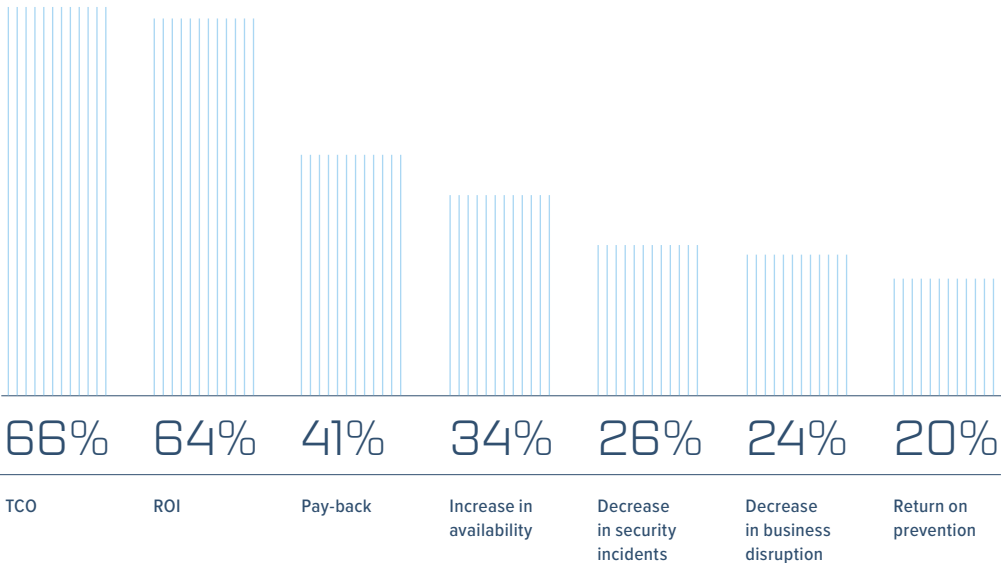


The need to reduce operational complexity will result in the consolidation of IT security vendors and tools, according to one CISO.

**CISOs take into account multiple factors when selecting security solutions and tools to address threats.**

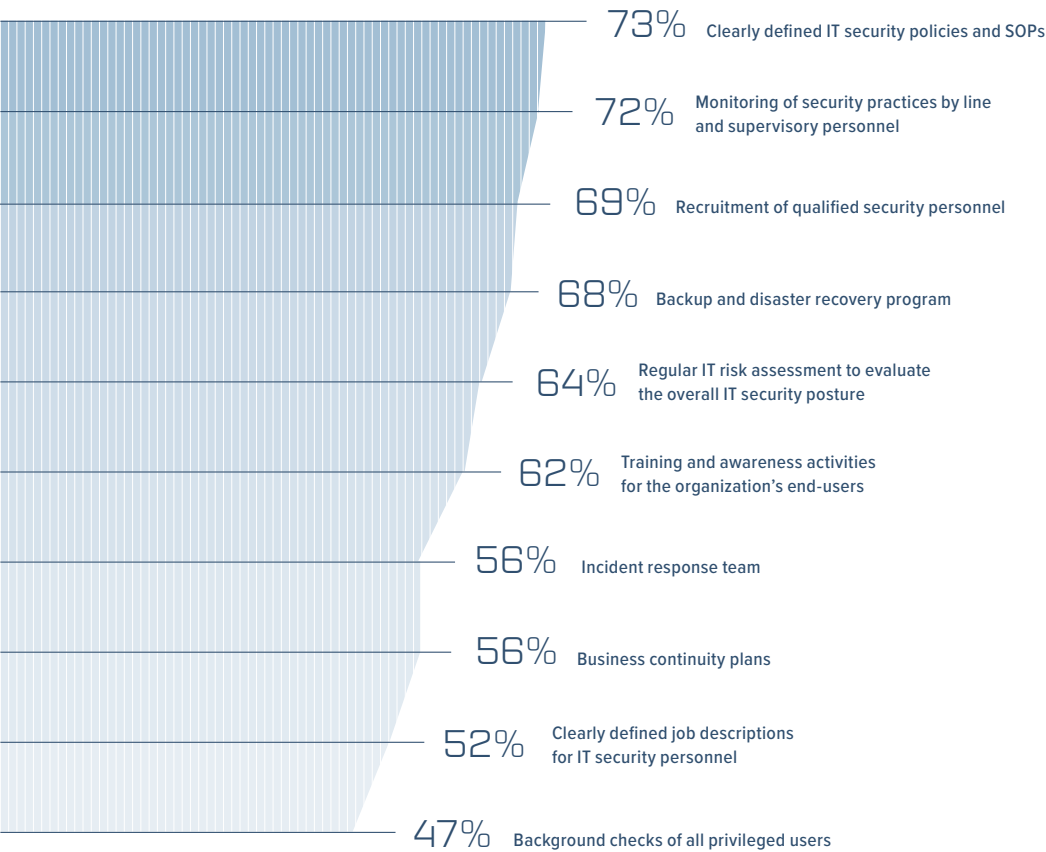
Forty-two percent of respondents say third-party analyst reviews are very important (18 percent) or important (24 percent) to choosing effective security solutions. As shown in Figure 24, TCO and ROI are the most important factors in investment evaluation.

**FIGURE 24**    **HOW ARE INVESTMENTS IN IT SECURITY EVALUATED?**  
(MORE THAN ONE RESPONSE ALLOWED.)



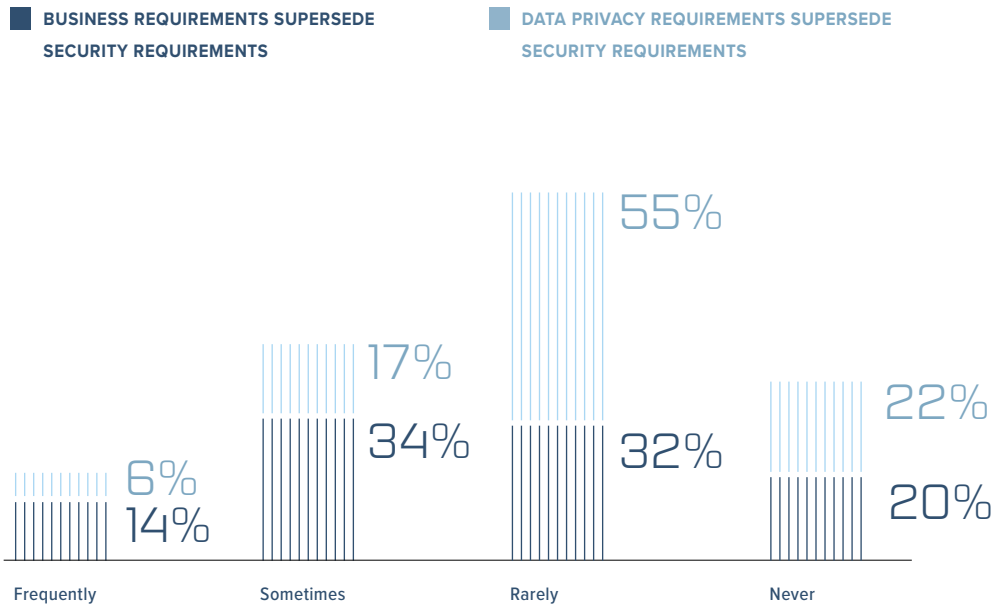
CISOs consider a wide range of security controls when planning their overall security posture. These controls range from policy definition to hiring and retention of qualified personnel.

FIGURE 25 WHAT ARE THE MOST IMPORTANT SECURITY CONTROLS?  
(MORE THAN ONE RESPONSE ALLOWED.)



As shown in Figure 26, almost half of respondents say business requirements supersede security requirements frequently or sometimes. Only 23 percent of respondents say data privacy requirements supersede security requirements frequently or sometimes. More organizations prioritize external threats over internal threats.

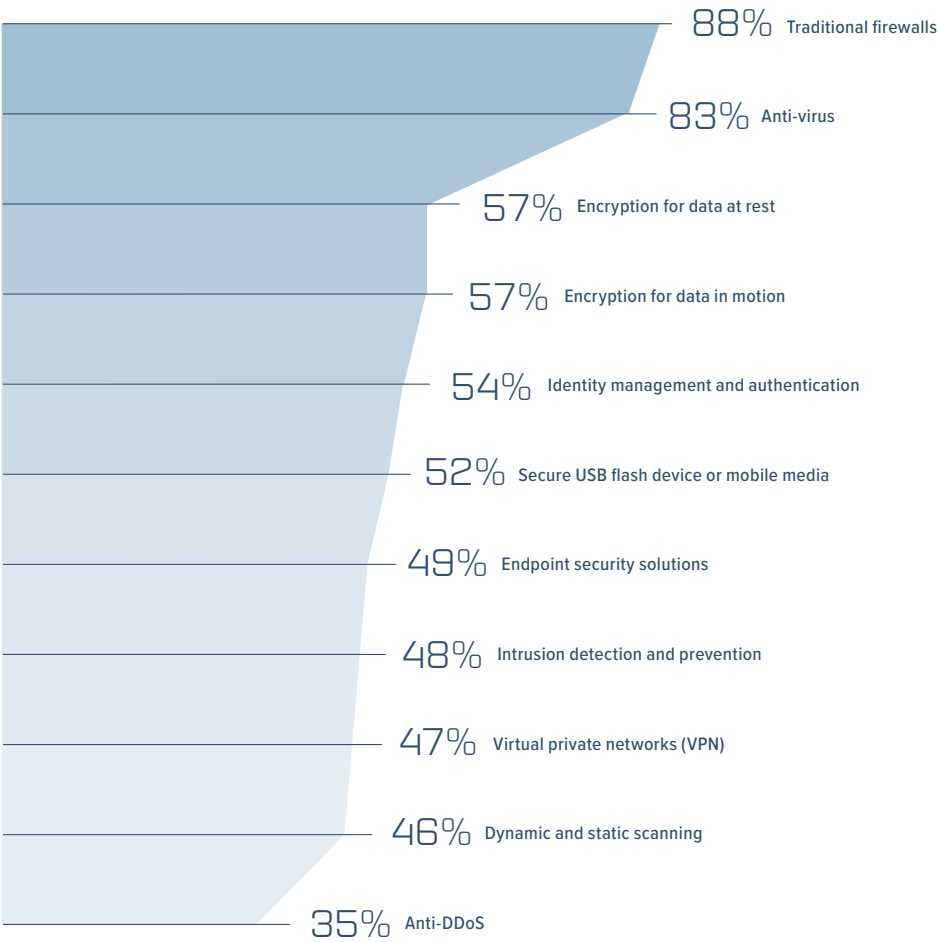
FIGURE 26 DO BUSINESS AND PRIVACY REQUIREMENTS SUPERSEDE SECURITY REQUIREMENTS?



**APTs and DDoS attacks are considered the biggest threats, but are the technologies deployed minimizing these risks?**

As shown in Figure 27, top security technologies are: traditional firewalls (88 percent of respondents), anti-virus (83 percent of respondents), encryption for data at rest and in motion (57 percent of respondents), identity management and authentication (54 percent of respondents) and secure USB flash device or mobile media (52 percent of respondents).

**FIGURE 27** WHAT SECURITY TECHNOLOGIES DO RESPONDENTS CONSIDER IMPORTANT?  
(MORE THAN ONE RESPONSE ALLOWED.)



Budgets and spending

IT security budgets are increasing or staying the same.

Eighty-seven percent of respondents say the IT security budget has increased significantly (18 percent), increased some (29 percent), or has not changed (40 percent). The average annual IT budget of companies represented in this research is \$167 million, and 11 percent of this total budget is allocated to IT security.

On average, 55 percent of the annual IT security budget is dedicated to operating costs and 41 percent is dedicated to capital investments. As shown in Table 1, on average, 8 percent of the IT security is dedicated to training of users, 23 percent is allocated to the procurement of managed security services and 24 percent is dedicated to compliance and audit activities.

TABLE 1 AVERAGE SPENDING ON IT SECURITY\*

	Percent	Calculus
Average total annual IT budget		\$167,000,000
Average of the total annual IT budget spent on security	11%	\$18,370,000
Average of the total annual security budget spent on training	8%	\$1,469,600
Average of the total annual security budget spent on managed security services	23%	\$4,225,100
Average of the total annual security budget spent on compliance and audit activities	24%	\$4,408,800

\* Averages compiled from 184 companies participating in this research



As shown in Figure 28, 53 percent of respondents say these funding levels are adequate but 37 percent say they are inadequate. Those who do not say their budget is adequate say the funding deficit averages 22 percent.

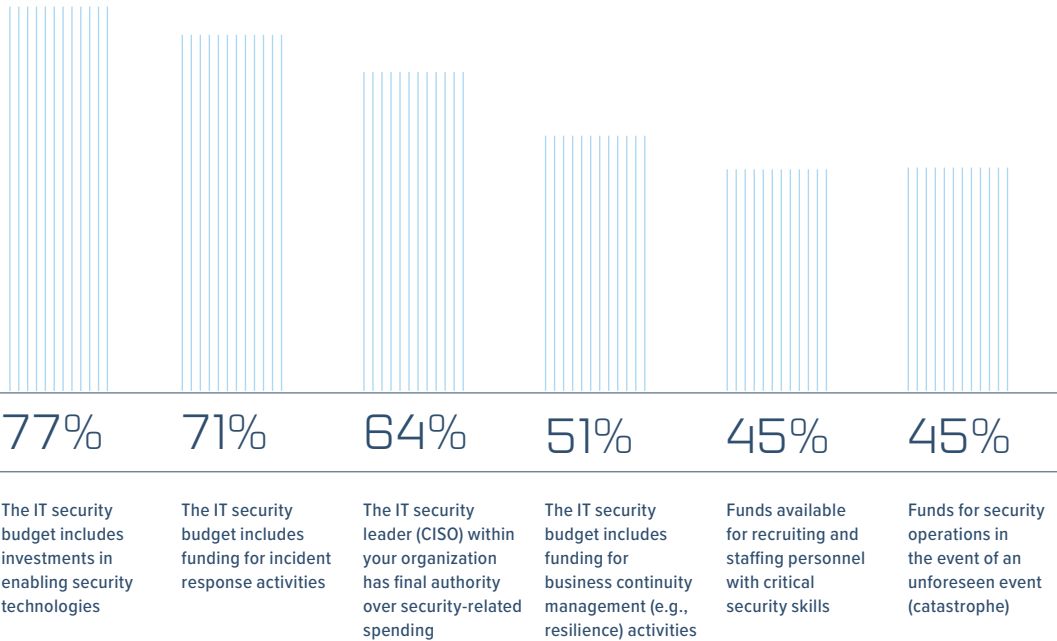
FIGURE 28 ARE IT SECURITY BUDGETS ADEQUATE?



Would organizations have the funds to deal with a crisis?

As shown in Figure 29, fewer than half of organizations allocate special funds for security operations to address an unforeseen event. Rather, the majority of companies focus their budgets on investments in enabling security technologies and funding for incident response activities.

FIGURE 29 HOW IT SECURITY FUNDS ARE ALLOCATED



SECTION

# 03

---



## Methods and Caveats

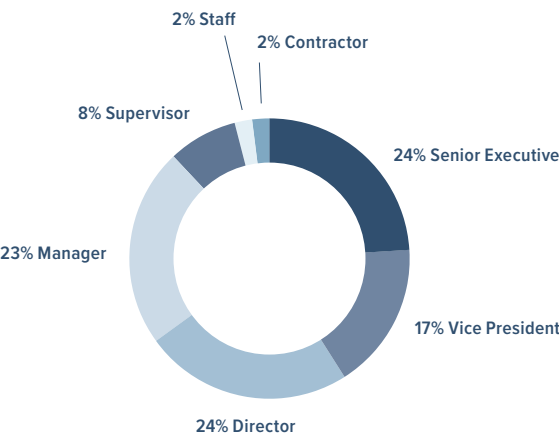
# Methods and Caveats

In this study, the sampling frame consisted of 184 organizations in the United States, the United Kingdom, Germany, Brazil, Mexico, India and China. Approximately 3.6 interviews with senior level IT professionals were conducted at each organization.

	SAMPLE SIZE BY COUNTRY	COUNTRY PERCENTAGE	INTERVIEWS PER COMPANY
United States	49	27%	181
United Kingdom	26	14%	93
Germany	26	14%	78
Brazil	21	11%	71
Mexico	22	12%	75
India	23	13%	94
China	17	9%	68
	184	100%	660

By design, more than half of the respondents (65 percent) are at or above the director level. Approximately 90 percent of respondents held full-time employment status.

FIGURE 30 RESPONDENTS' JOB ROLES WITHIN THE ORGANIZATION



Sixty-seven percent of respondents report directly to a C-level executive, with 49 percent reporting to the CIO.

FIGURE 31 DIRECT REPORTING CHANNEL

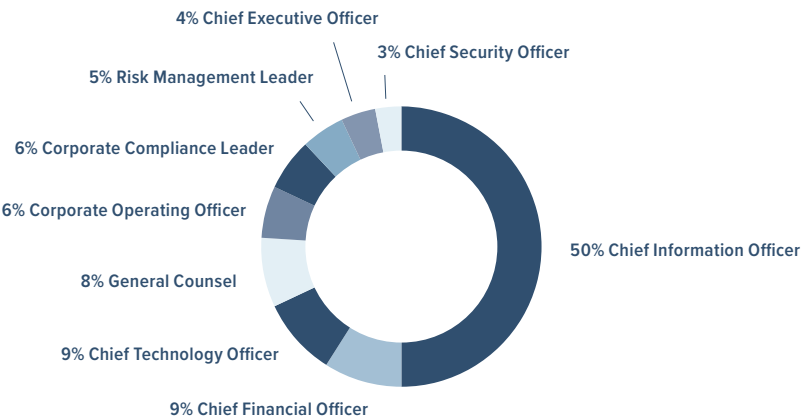
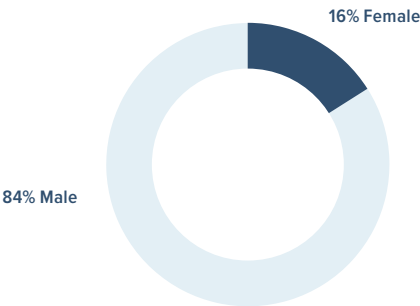
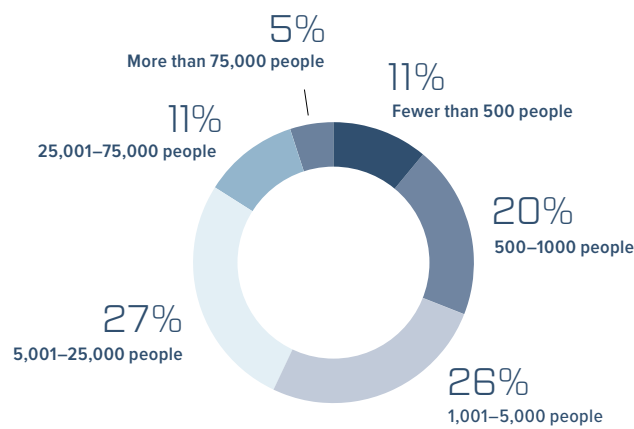


FIGURE 32 RESPONDENTS' GENDER



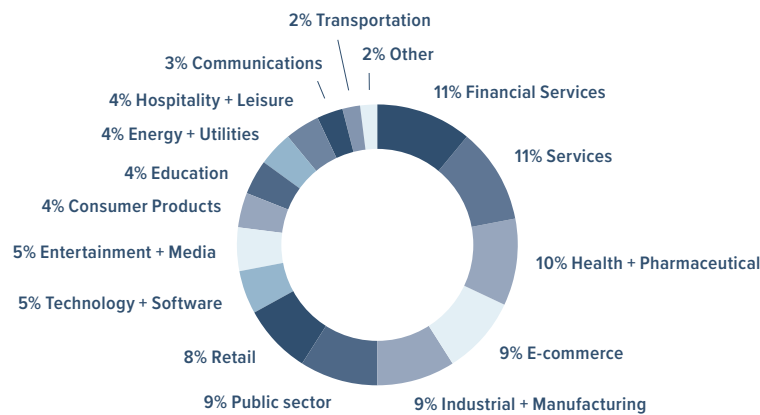
Sixty-seven percent of respondents report directly to a C-level executive, with 49 percent reporting to the CIO.

FIGURE 33 GLOBAL EMPLOYEE HEADCOUNT



Respondents' organizations span many industries. In this study, financial services was the largest segment, followed by services, and health and pharmaceuticals.

FIGURE 34 PRIMARY INDUSTRY FOCUS



As shown in Figure 35, thirty-four percent of respondents have a bachelor’s degree in technology or a science field. Another 34 percent of respondents have a certification, and 24 percent of respondents have a bachelor’s degree in business or management.

**FIGURE 35** EDUCATION AND TRAINING  
MORE THAN ONE RESPONSE PERMITTED

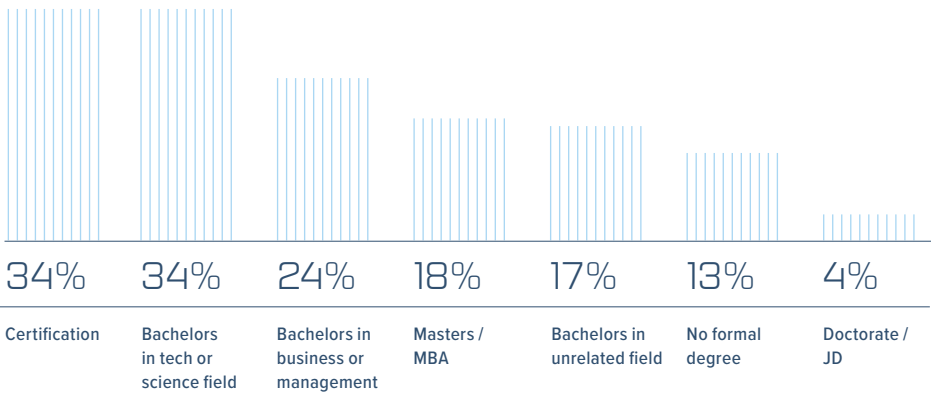
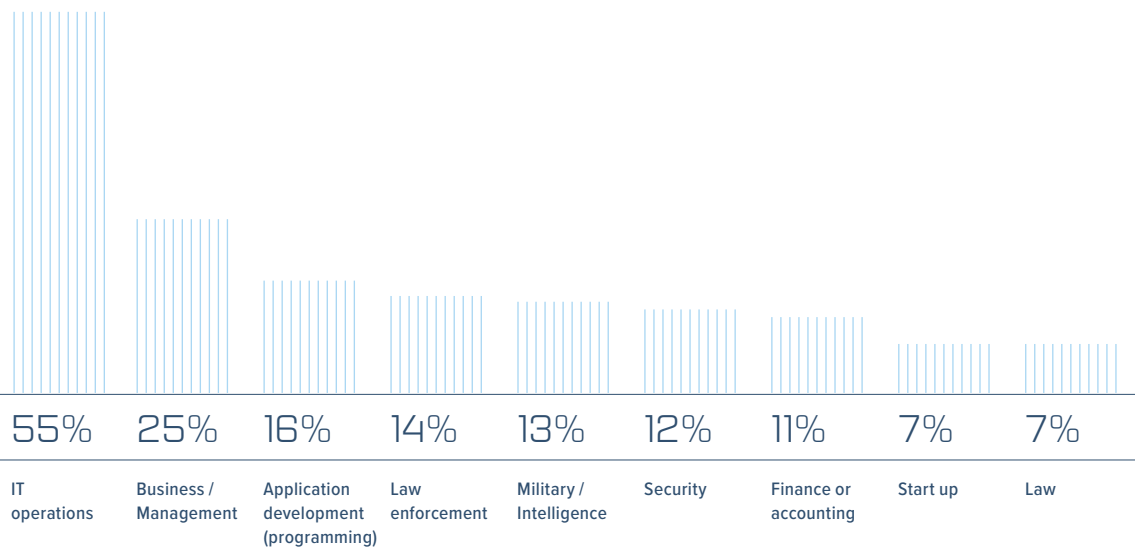


Figure 36 reports the relevant work experience of the respondents. Fifty-five percent of respondents have IT operations experience, 25 percent of respondents have business/management experience and 16 percent of respondents have application development experience.

**FIGURE 36** RELEVANT WORK EXPERIENCE  
MORE THAN ONE RESPONSE PERMITTED



## 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 interviews senior with level IT professionals in 184 companies in the following countries: the United States, the United Kingdom, Germany, Brazil, Mexico, India and China. It is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who were interviewed.

### **Sampling-frame bias**

The accuracy is based on contact information and the degree to which the list is representative of senior level IT professionals. We also acknowledge that the results may be biased by external events such as media coverage.

### **Self-reported results**

The quality of benchmark 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.



## Detailed survey results

The following tables provide the frequency or percentage frequency of responses to all interview questions contained in this study. All interview responses were captured from April 3, 2017 through June 8, 2017.

### Country abbreviation

Sample size by country	184
Average number of interviews per company	3.6
Weight by country	100%

## PART 1

## IT security ecosystem

The following questions pertain to the respondent organization's IT security function and related operations throughout the enterprise.

**Q1a. In the past 12 months, have there been any big developments that marked a change in your organization's attitude about its security program?**

Yes	60%
No	40%
<b>TOTAL</b>	<b>100%</b>

**Q1b. If yes, what were the biggest developments?**

Material data breach	45%
Cyber security exploit	43%
New or emerging compliance requirements	23%
Material change to business process	13%
Other	4%
<b>TOTAL</b>	<b>128%</b>

**Q2a. Does the overall organization consider security a business priority?**

Yes	60%
No	40%
<b>TOTAL</b>	<b>100%</b>

## PART 1, CONT'D

## Q2b. If yes, what teams are most supportive of the IT security function?

Applications development	12%
Brand management	4%
Communications	8%
Compliance	37%
Facilities management	15%
Finance and accounting	21%
Human resources	45%
Internal audit	43%
IT operations	36%
Legal	48%
Line of business (LOB)	43%
Manufacturing	28%
Marketing	8%
Sales	11%

## Q3a. Does your organization have difficulty in hiring qualified security personnel?

Yes	58%
No	42%
<b>TOTAL</b>	<b>100%</b>

## Q3b. If yes, what are your organization's hiring challenges?

Retaining qualified personnel	39%
Identifying and recruiting qualified candidates	56%
Lack of upward mobility / career attainment	19%
Inability to offer a market-level salary	48%
Inability to provide flexible hours	35%
Inability to work from home location	21%
Other	1%
<b>TOTAL</b>	<b>256%</b>

## PART 1, CONT'D

## Q4a. Are IT security objectives aligned with business objectives?

Yes, fully aligned	26%
Yes, partially aligned	34%
No, not aligned	40%
<b>TOTAL</b>	<b>100%</b>

## Q4b. Are IT security operations aligned with IT operations?

Yes, fully aligned	45%
Yes, partially aligned	32%
No, not aligned	23%
<b>TOTAL</b>	<b>100%</b>

## Q5. What best describes how IT security initiatives are rolled out throughout your organization?

Starts at the top and cascaded downward throughout the organization	16%
Starts at the bottom and cascaded upward throughout the organization	59%
Starts in the middle and cascaded both upward and downward throughout the organization	24%
<b>TOTAL</b>	<b>100%</b>

## Q6. Do data breach incidents get reported to the CEO and/or board of directors?

Yes, all data breaches are reported to the CEO and/or board of directors	19%
Yes, only material data breaches are reported to the CEO and/or board of directors	46%
No	35%
<b>TOTAL</b>	<b>100%</b>

## Q7. Do all cyber exploits or attacks get reported to the CEO and/or board of directors?

Yes, all cyber attacks are reported to the CEO and/or board of directors	17%
Yes, only material cyber attacks are reported to the CEO and/or board of directors	46%
No	37%
<b>TOTAL</b>	<b>100%</b>

## PART 1, CONT'D

**Q8a. Are employees in your organization made aware of data security and sensitive information handling requirements?**

Yes	54%
No	46%
<b>TOTAL</b>	<b>100%</b>

**Q8b. If yes, how is employee security awareness achieved?**

Part of the on-boarding process (for new employees)	40%
Formal training program	51%
Informal training or ad hoc program	21%
On-the-job training and mentoring	24%
Other	3%
<b>TOTAL</b>	<b>140%</b>

**Q9a. Are your organization's IT security policies monitored for compliance?**

Yes	63%
No	37%
<b>TOTAL</b>	<b>100%</b>

**Q9b. Are employees and their immediate supervisors held accountable for IT security infractions or non-compliance to the company's policies?**

Yes, strictly enforced	35%
Yes, but exceptions are made	32%
No	33%
<b>TOTAL</b>	<b>100%</b>

**Q10a. Does your organization have an IT security strategy?**

	<b>Total</b>
Yes	51%
No	49%
<b>TOTAL</b>	<b>100%</b>

**Q10b. If yes, does the IT security strategy span the entire enterprise?**

	<b>Total</b>
Yes	46%
No	54%
<b>TOTAL</b>	<b>100%</b>

## PART 1, CONT'D

Q10c. If yes, how important is an “always-on” requirement to your organization’s IT security strategy?

Very important	35%
Important	47%
Not important	17%
Irrelevant	1%
<b>TOTAL</b>	<b>100%</b>

Q10d. If yes, is the IT security strategy reviewed, approved, and supported by C-level executives?

Yes	43%
No	57%
<b>TOTAL</b>	<b>100%</b>

Q11a. Today, what percent of your organization’s IT security efforts focus on prevention, detection, containment and/or remediation (show mix in percentage terms)?

Prevention	33%
Detection	30%
Containment	21%
Remediation	17%
<b>TOTAL</b>	<b>100%</b>

Q11b. Two years ago, what percent of your organization’s IT security efforts focused on prevention, detection, containment and/or remediation (show mix in percentage terms)?

Prevention	40%
Detection	24%
Containment	20%
Remediation	16%
<b>TOTAL</b>	<b>100%</b>

Q11c. Two years from now (think ahead), what percent of your organization’s IT security efforts will focus on prevention, detection, containment and/or remediation (show mix in percentage terms)?

Prevention	21%
Detection	39%
Containment	25%
Remediation	15%
<b>TOTAL</b>	<b>100%</b>

## PART 1, CONT'D

Q12a. Today, what percent of your organization's IT security posture depends on network security, endpoint security, application security, IT security and physical security (show mix in percentage terms)?

Network/perimeter	40%
Endpoint	22%
Application	17%
Data	12%
Physical	8%
<b>TOTAL</b>	<b>100%</b>

Q12b. Two years ago, what percent of your organization's IT security posture depended on network security, endpoint security, application security, IT security and physical security (show mix in percentage terms)?

Network/perimeter	46%
Endpoint	22%
Application	12%
Data	10%
Physical	10%
<b>TOTAL</b>	<b>100%</b>

Q12c. Two years from now (think ahead), what percent of your organization's IT security posture will depend on network security, endpoint security, application security, IT security and physical security (show mix in percentage terms)?

Network/perimeter	23%
Endpoint	28%
Application	29%
Data	13%
Physical	7%
<b>TOTAL</b>	<b>100%</b>

Q13. With respect to IT security, what best describes your organization's most important mission? Please rank the following choices from 1 = most important to 5 = least important.

Ensure availability of IT services (prevent downtime)	1.77
Ensure compliance with policies and regulations	2.94
Protect sensitive or confidential information assets	2.35
Prevent damage to the IT infrastructure	3.65
Preserve customer/user trust	3.97

## PART 1, CONT'D

Q14a. What is the number of data breach incidents experienced by your organization within last 24 months?

TOTAL	2.34
-------	------

Q14b. Do you believe the frequency of data breach incidents will increase, decrease or stay at the same level over the next 24 months?

Increase	39%
----------	-----

Decrease	17%
----------	-----

Stay the same	44%
---------------	-----

TOTAL	100%
-------	------

Q14c. Do you believe the severity of data breach incidents will increase, decrease or stay at the same level over the next 24 months?

Increase	41%
----------	-----

Decrease	13%
----------	-----

Stay the same	46%
---------------	-----

TOTAL	100%
-------	------

Q15a. What is the number of cyber exploits or attacks experienced by your organization within the last 24 months?

TOTAL	3.00
-------	------

Q15b. Do you believe the frequency of cyber exploits or attacks will increase, decrease or stay at the same level over the next 24 months?

Increase	40%
----------	-----

Decrease	11%
----------	-----

Stay the same	49%
---------------	-----

TOTAL	100%
-------	------

Q15c. Do you believe the severity of cyber exploits or attacks will increase, decrease or stay at the same level over the next 24 months?

Increase	46%
----------	-----

Decrease	9%
----------	----

Stay the same	45%
---------------	-----

TOTAL	100%
-------	------



## PART 1, CONT'D

Q16. On a 10-point scale, how resilient is your organization to future data breaches and cyber attacks?

TOTAL	6.85
-------	------

Q17a. Is the Internet of Things (IoT) driving any changes in your organization's IT security practices or requirements?

Yes, significant change	49%
-------------------------	-----

Yes, some change	31%
------------------	-----

No, none or nominal change	20%
----------------------------	-----

TOTAL	100%
-------	------

Q17b. If yes, what changes have you made?

Purchased and deployed new security technologies	32%
--	-----

Revised controls and governance practices	44%
---	-----

Set new policies and standard operating procedures	64%
--	-----

Conducted tests to ensure IoT devices do not present security risks	64%
---	-----

Hired or engaged IoT security experts	41%
---------------------------------------	-----

Other	2%
-------	----

TOTAL	248%
-------	------

Q18. Does the IT security function evaluate the risk of IoT devices and applications before they are deployed throughout the organization?

Yes	22%
-----	-----

No	78%
----	-----

TOTAL	100%
-------	------

Q19. Is compliance with emerging data protection or privacy regulations a major driver for investments in IT security?

Yes	61%
-----	-----

No	39%
----	-----

TOTAL	100%
-------	------

## PART 1, CONT'D

**Q20. What one statement best describes how IT security within your organization impacts business innovation?**

There is no relationship between IT security and business innovation	51%
Security enhances business innovation	25%
Security diminishes business innovation	23%
<b>TOTAL</b>	<b>100%</b>

**Q21. What one statement best describes how IT security within your organization impacts employee/user productivity?**

There is no relationship between IT security and employee/user productivity	39%
IT security enhances employee/user productivity	39%
IT security diminishes employee/user productivity	23%
<b>TOTAL</b>	<b>100%</b>

**Q22. Do business requirements ever supersede security requirements?**

Yes, frequently	14%
Yes, sometimes	34%
Yes, rarely	32%
No, never	20%
<b>TOTAL</b>	<b>100%</b>

**Q23. Do data privacy requirements ever supersede security requirements?**

Yes, frequently	6%
Yes, sometimes	17%
Yes, rarely	55%
No, never	22%
<b>TOTAL</b>	<b>100%</b>

**Q24. Does your organization's IT security efforts prioritize internal versus external threats?**

Internal threats	32%
External threats	41%
Both threats are equal	27%
<b>TOTAL</b>	<b>100%</b>

## PART 1, CONT'D

Q25. Is IT security considered a standalone function or is it integrated with other business functions within your organization?

Standalone	58%
Integrated	22%
Hybrid (mixture)	20%
<b>TOTAL</b>	<b>100%</b>

Q26. Is the IT security function within your organization integrated with physical security operations?

Fully integrated	21%
Partially integrated	28%
Not integrated	50%
<b>TOTAL</b>	<b>100%</b>

Q27. Does the IT security function have clearly defined lines of responsibility?

Yes	55%
No	45%
<b>TOTAL</b>	<b>100%</b>

Q28a. Who does the IT security leader or CISO report to within your organization?  
Please select only one direct report (i.e., solid line relationship).

Chief information officer	50%
Chief technology officer	9%
Chief security officer	3%
Chief financial officer	9%
Chief executive officer	4%
Chief operating officer	6%
Corporate compliance leader	6%
General counsel	8%
Risk management leader	6%
<b>TOTAL</b>	<b>100%</b>

## PART 1, CONT'D

**Q28b. Does the IT security leader or CISO report to others within your organization?**  
Please select all that apply (i.e., dotted line relationship).

Chief information officer	16%
Chief technology officer	10%
Chief security officer	7%
Chief financial officer	20%
Chief executive officer	9%
Chief operating officer	9%
Corporate compliance leader	26%
General counsel	23%
Risk management leader	18%
<b>TOTAL</b>	<b>140%</b>

**Q29a. Does your organization outsource some of its IT security operations?**

Yes	58%
No	42%
<b>TOTAL</b>	<b>100%</b>

**Q29b. If yes, approximately what percent of IT security operations are outsourced?**

<b>TOTAL</b>	<b>27%</b>
--------------	------------

**Q29c. If yes, how important are outsourced (managed) functions to overall security objectives?**

Very important	32%
Important	37%
Not important	22%
Irrelevant	8%
<b>TOTAL</b>	<b>100%</b>

**Q29e. If yes, are outsourced services held to the same standards as on-premise security operations within your organization?**

Yes, always	26%
Yes, most of the time	26%
Yes, some of the time	24%
No	24%
<b>TOTAL</b>	<b>100%</b>

## PART 1, CONT'D

Q30. Are your organization's business partners, vendors and other third parties held to high-level security requirements?

Yes, always	22%
Yes, most of the time	21%
Yes, some of the time	28%
No	28%
<b>TOTAL</b>	<b>100%</b>

Q31. Does your organization collaborate with industry partners/competitors on security issues (e.g., the sharing of threat intelligence)?

Yes, always	11%
Yes, most of the time	25%
Yes, some of the time	25%
No	40%
<b>TOTAL</b>	<b>100%</b>

Q32a. Does the CISO directly consume threat intelligence about their organization or industry?

Yes	52%
No	48%
<b>TOTAL</b>	<b>100%</b>

Q32b. If yes, what sources of threat intelligence are consumed?

Vendor threat feeds	69%
Peer-to-peer sharing	68%
Government	19%
Other	2%
<b>TOTAL</b>	<b>158%</b>

Q33. Do cultural differences among people and business operations around the globe influence your organization's local security requirements?

Yes, significant influence	46%
Yes, some influence	26%
Yes, minimal influence	13%
No influence	15%
<b>TOTAL</b>	<b>100%</b>

## PART 1, CONT'D

Q34. Do turf and silo issues among different functions and/or business units diminish your organization's IT security tactics and strategy?

Yes, significant influence	36%
Yes, some influence	39%
Yes, minimal influence	15%
No influence	10%
<b>TOTAL</b>	<b>100%</b>

Q35. Does the IT security function incorporate risk management practices to evaluate the IT security program?

Yes	50%
No	50%
<b>TOTAL</b>	<b>100%</b>

Q36. How much does risk inform your organization's security culture?

Significant influence	28%
Some influence	42%
Nominal influence	20%
No influence	10%
<b>TOTAL</b>	<b>100%</b>

Q37. Does your organization use (or plan to use) cyber insurance to support risk transfer?

Yes	30%
No	69%
<b>TOTAL</b>	<b>100%</b>

Q38a. What is the full-time equivalent headcount of IT security personnel in your organization today.

<b>TOTAL</b>	<b>19</b>
--------------	-----------

Q38b. Two years from now (think ahead), what will be the full-time equivalent headcount of IT security personnel in your organization?

<b>TOTAL</b>	<b>32</b>
--------------	-----------

## PART 1, CONT'D

Q39. Do you consider the current headcount adequate for meeting your organization's security mission and/or strategy?

Yes, more than adequate	7%
Yes, adequate	51%
No, not adequate	42%
<b>TOTAL</b>	<b>100%</b>

Q40a. Today, how important is computer learning and artificial intelligence to the effectiveness of organization's security posture?

Very important	21%
Important	29%
Not important	43%
Irrelevant	8%
<b>TOTAL</b>	<b>101%</b>

Q40b. Two years from now (think ahead), how important will computer learning and artificial intelligence be to the effectiveness of your organization's security posture?

Very important	33%
Important	37%
Not important	24%
Irrelevant	5%
<b>TOTAL</b>	<b>100%</b>

Q40c. What will be the impact of computer learning and artificial intelligence tools on the level of staffing needed to ensure a strong security posture?

Significant decrease in staffing level	14%
Some decrease in staffing level	27%
No change in staffing level	42%
Some increase in staffing level	12%
Significant increase in staffing level	5%
<b>TOTAL</b>	<b>100%</b>



## PART 2

## Controls, governance and technologies

**Q41. Following are general security controls considered important by many organizations. Please check all the controls deployed by your organization.**

Recruitment of qualified security personnel	69%
Clearly defined job descriptions for IT security personnel	52%
Clearly defined IT security policies and SOPs	73%
Backup and disaster recovery program	68%
Business continuity plans	56%
Background checks of all privileged users	47%
Specialized training for IT security personnel	47%
Training and awareness activities for the organization's end-users	62%
Monitoring of security practices by line and supervisory personnel	72%
Monitoring of business partners, vendors and other third-parties	44%
Internal audits of security and other related IT compliance practices	39%
Segregation of duties between IT and businesses	40%
Control self-assessment	38%
Regular IT risk assessment to evaluate the overall IT security posture	64%
Adherence to standardized security requirements	46%
Incident response team	56%
Security test / adversary emulation / red team	43%
Threat hunting / threat intelligence	22%
Software and hardware inventory and valuation	16%

**Q42. Following are governance and oversight practices considered important by many organizations. Please check the governance practices deployed by your organization.**

Appointment of a executive-level security leader with enterprise-wide responsibility	69%
Upstream communication channel from the security leader to the CEO or other C-level personnel	46%
Creation of a cross-functional committee to oversee IT security strategies	56%
Creation of a security or IT security program office	41%
Creation of a program charter approved by executive-level sponsor.	37%
Regularly scheduled report on the state of IT security to the board of directors	55%
Internal or external audits of the IT security function	32%
Benchmarks of IT security operations against peer or reference group	28%
Process for self-reporting compliance violations to appropriate authorities	20%
Execution of risk management practices	34%
Metrics for evaluating the effectiveness of IT security operations	46%

## PART 2, CONT'D

**Q43. Following are enabling security technologies considered important by many organizations. Please check the enabling technologies deployed by your organization.**

Access governance	36%
Anti-virus	83%
Anti-DDoS	35%
Big data analytics	30%
Data loss prevention (DLP)	37%
Dynamic and static scanning	46%
Encryption for data at rest	57%
Encryption for data in motion	57%
Identity management and authentication	54%
Intrusion detection and prevention	48%
Network and traffic intelligence systems	33%
Next generation firewalls	38%
Secure USB flash device or mobile media	52%
Security information and event management (SIEM)	43%
Test data anonymization solution	22%
Tokenization technology	28%
Traditional firewalls	88%
Virtual private networks (VPN)	47%
Web application firewalls (WAF)	39%
Endpoint security solutions	49%

**Q44. What percentage of all deployed security tools communicate meaningfully with each other?**

Less than 5%	21%
5% to 10%	23%
11% to 25%	24%
26% to 50%	17%
51% to 75%	11%
76% to 100	3%
<b>TOTAL</b>	<b>100%</b>

**Q45. How important are third-party analyst reviews to the selection of security solutions?**

	<b>Total</b>
Very important	18%
Important	24%
Not important	29%
Irrelevant	29%
<b>TOTAL</b>	<b>100%</b>

## PART 3

## Budget, funding and investment decisions

Following are budget-related issues that relate to IT security operations with your organization. Please provide your opinion about each question listed below.

Q46. Approximately, what is your organization's total annual IT budget (US\$ millions)?	\$167
Q47. Approximately, what percent of the total annual IT budget is dedicated to security?	11%
Q48. Over the past two years, has the IT security budget increased, decreased or stayed the same?	
Significant increase	18%
Some increase	29%
No change	40%
Some decrease	11%
Significant decrease	2%
TOTAL	100%
Q49a. In your opinion, are present funding levels adequate?	
Yes, more than adequate	10%
Yes, adequate	53%
No, not adequate	37%
TOTAL	100%
Q49b. If no, how large is the funding deficit or gap (in absolute or percentage terms)?	22%
Q50. How often has your organization experienced a security budget surplus in the past 5 years?	
None	56%
1 time	35%
2 times	7%
3 times	2%
4 times	0%
5 times	0%
More than 5 times	0%
TOTAL	100%

## PART 3, CONT'D

## Q51. How are investments in IT security evaluated?

TCO	66%
ROI	64%
Pay-back	41%
Return on prevention	20%
Increase in availability	34%
Decrease in security incidents	26%
Decrease in business disruption	24%
Other	274%

## Q52. Are there special funds for security operations in the event of an unforeseen event (catastrophe)?

Yes	45%
No	55%
<b>TOTAL</b>	<b>100%</b>

## Q53. Are there adequate funds available for recruiting and staffing personnel with critical security skills?

Yes	45%
No	55%
<b>TOTAL</b>	<b>100%</b>

## Q54. Does the IT security leader (CISO) within your organization have final authority over security-related spending?

Yes	64%
No	36%
<b>TOTAL</b>	<b>100%</b>

## Q55. Does the IT security budget include investments in enabling security technologies?

Yes	77%
No	23%
<b>TOTAL</b>	<b>100%</b>

## Q56. Does the IT security budget include funding for incident response activities?

Yes	71%
No	29%
<b>TOTAL</b>	<b>100%</b>

## PART 3, CONT'D

Q57. Does the IT security budget include funding for business continuity management (e.g., resilience) activities?

Yes	51%
No	49%
TOTAL	100%

Q58. Approximately, what percent of the total annual IT security budget is dedicated to operating costs versus capital expenditures?

Operating costs	55%
Capital investments	41%
Other	4%
TOTAL	100%

Q59. What portion of the IT security budget is dedicated to training of users across the enterprise? 8%

Q60. What portion of the IT security budget is dedicated to the procurement of managed security services? 23%

Q61. What portion of the IT security budget is dedicated to compliance and audit activities? 24%

## PART 4

## The CISO role

**Q62.** Following are job-related aspects or role of the security leader within your organization. Does the CISO or CSO within your organization have the following responsibilities or role? Please check all that apply.

Reports to senior executives (no more than three steps below the CEO on the organization chart)	65%
Direct influence and authority over all security expenditures in our organization	64%
Direct influence over the hiring and firing of security personnel	62%
Direct channel to CEO in the event of a serious security incident	60%
Direct channel to law enforcement or intelligence agencies in the event of a cyber crime	40%
Responsible for setting the security strategy and related initiatives	67%
Responsible for setting the security mission	61%
Responsible for enforcing security policies	56%
Responsible for integrating physical, logical and virtual security across the enterprise	39%
Responsible for securing the organization against all known attacks (and attack signatures)	49%
Sole accountability for information protection and privacy	24%
Final decisions for all IT security spending	68%
Responsible for overcoming the shortage of personnel with critical security skills	66%
Responsible for “thought leadership” communications outside the organization	46%
Responsible for informing the organization about new threats, technologies, practices and compliance requirements	60%

## PART 5

## Third parties and supply chain issues

**Q63.** Following are IT security activities directly related to your organization’s supply chain and third-party issues. Please select all the activities that are deployed.

Establish process in evaluating business partners, vendors, contractors and other third parties IT security protection capability before engaging business activities	57%
Establish objective security requirements or protocols for business partners, vendors, contractors and other third parties	46%
Establish a vetting process to ensure all third parties are evaluated and screened against objective security requirements	52%
Establish procurement procedures to ensure that contract terms contain security and privacy requirements and responsibility / liability in case there is a data breach as result of business activities with the third party	53%
Establish security procedures to ensure that attacks against the organization’s critical infrastructure do not affect supply chain issues or logistics	41%
Establish security procedures to ensure that the supply chain is not corrupted, contaminated or disruptive to business operations (continuity)	33%

Monitor third parties to ensure continued compliance with contractually required security requirements	54%
Periodically review third parties in terms of their compliance with objective security requirements	44%
Establish enforcement actions and termination penalties against third parties that fail to comply with objective security requirements (and fail to remediate)	37%
Establish remediation procedures for third parties that fail to comply with objective security requirements	25%
Establish a direct communication channel between the organizations security program and management responsible for contracts and procurement	27%
Establish security requirements and controls for cloud providers	34%

## PART 6

## Security threats and issues

Botnets	4.4
Web-based attacks	6.5
Credential takeover	8.1
Malicious insiders	7.6
Insecure apps (including SQL injection)	8.2
Phishing	6.8
Social engineering	7.0
Distributed denial of service (DDoS)	8.3
Advanced persistent threats (APTs)	8.8
Nation-state attacks	6.1
Data exfiltration	8.2

Following are issues relating to emerging threats in the IT security ecosystem. Please provide your opinion about each issue listed below.

<b>Q65. Does your organization have a policy on employee's personal use of social networks in the workplace?</b>	
Yes	59%
No	41%
<b>TOTAL</b>	<b>100%</b>

<b>Q66. Does your organization have a policy on employee's use of personally-owned devices (BYOD) in the workplace?</b>	
Yes	60%
No	40%
<b>TOTAL</b>	<b>100%</b>

## PART 6, CONT'D

Q67. Does your organization have a policy on employees working from remote locations including home offices?

Yes	58%
No	42%
<b>TOTAL</b>	<b>100%</b>

Q68. Does your organization have guidelines as to the types of confidential or sensitive information that can be accessed by employees from remote locations?

Yes	61%
No	39%
<b>TOTAL</b>	<b>100%</b>

Q69. Does your organization assess the impact of cloud resources on the ability to protect and secure confidential or sensitive information?

Yes	51%
No	49%
<b>TOTAL</b>	<b>100%</b>

## PART 7

## Demographics and organizational characteristics

D1. What organizational level best describes your current position?

Senior Executive	44
Vice President	32
Director	44
Manager	42
Supervisor	15
Staff	3
Contractor	3
<b>TOTAL</b>	<b>184</b>

D2. Is this a full time position?

Yes	166
No	18
<b>TOTAL</b>	<b>184</b>



## PART 7, CONT'D

## D3. Check the Primary Person you or your IT security leader reports to within the organization.

Chief information officer	91
Chief technology officer	16
Chief security officer	6
Chief financial officer	17
Chief executive officer	7
Chief operating officer	11
Corporate compliance leader	11
General counsel	14
Risk management leader	10
<b>TOTAL</b>	<b>184</b>

## D4. Total years of relevant experience (years)

Total years of IT or security experience	12.8
Total years in current position	8.9

## D5. Gender:

Female	29
Male	155
<b>TOTAL</b>	<b>184</b>

## D6. What is the worldwide headcount of your organization?

Less than 500 people	21
500 to 1,000 people	37
1,001 to 5,000 people	47
5,001 to 25,000 people	50
25,001 to 75,000 people	21
More than 75,000 people	8
<b>TOTAL</b>	<b>184</b>

**D7. What best describes your organization's primary industry classification?**

Aerospace & defense	2
Agriculture & food services	1
Communications	5
Consumer products	8
E-commerce	16
Education	8
Energy & utilities	7
Entertainment & media	9
Financial services	21
Health & pharmaceutical	19
Hospitality & leisure	7
Industrial & manufacturing	16
Public sector	16
Retail	15
Services	20
Technology & software	10
Transportation	4
<b>TOTAL</b>	<b>184</b>

**D8. What education / training have you undergone?**

No formal degree	23
Bachelors in tech or science field	62
Bachelors in business or management	44
Bachelors in an unrelated field	32
Masters / MBA	33
Doctorate / JD	7
Certification	62

D9. What kind of relevant work experience do you have?	
IT operations	102
Security	22
Application development (programming)	29
Finance or accounting	21
Business / management	46
Law	12
Law enforcement	25
Military / Intelligence	23
Start up	13

#### 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.

#### F5 Networks

F5 delivers integrated security solutions that address the primary risks associated to your applications no matter where they reside, enabling organizations to embrace the application infrastructure they choose without sacrificing speed and control. For more information, go to [f5.com](https://f5.com). You can also follow @f5networks on [Twitter](https://twitter.com/f5networks) or visit us on [LinkedIn](https://www.linkedin.com/company/f5) and [Facebook](https://www.facebook.com/f5networks) for more information about F5, its partners, and technologies.