RESEARCH REPORT APRIL 2020 | $499

Interop NETWORKComputing InformationWeek DARKReading

NEXT

The State of IT Operations and Cybersecurity Operations 2020

This year's survey found that organizations are becoming more aware of their security needs and assigning more responsibilities to the security team. However, those changes are resulting in some increasing tension between the teams.

sponsored by ExtraHop

informatech

PREVIOUS NEXT

Table of Contents

Figures

PREVIOUS NEXT

Author

About the Author

Freelance writer Cynthia Harvey has been covering enterprise IT for more than 20 years. She regularly contributes to InformationWeek and several other technology publications, and she specializes in writing about DevOps, cloud computing, security, data analytics, and artificial intelligence. She makes her home in the Detroit area.

Executive Summary

The good news from this year's State of IT Operations and Cybersecurity Operations survey from InformationWeek in partnership with Dark Reading is that business leaders are becoming much more cognizant of the cybersecurity threats they face. In response, many are assigning more responsibility to their security teams. But these organizational shifts seem to be resulting in some increased tension between security and the rest of IT. CIOs will need to carefully shepherd their teams through these changes to ensure that everyone continues working as a unified group.

Key Findings

- The number of organizations spending a quarter or more of their IT budgets on cybersecurity nearly doubled between 2019 and 2020.
- The percentage of respondents who said that cybersecurity is "absolutely critical" at their organizations climbed from 30% in 2019 to 39% in 2020.
- The percentage of organizations that bring the security team at the beginning of every new project increased from 20% in 2019 to 29% in 2020, and about half of organizations involve security early on for all or most projects.
- Less than half of respondents (48%) said that their general IT and cybersecurity staffs communicate well, a decrease from 57% who said the same thing in 2019.
- About a third of respondents (32%) said that the relationship between IT and security is generally good but needs some work, up from a quarter who said the same thing last year.
- Just under half (45%) of respondents said the CIO makes the final call on disagreements between IT and security, up from 30% last year.

PREVIOUS NEXT

Research Synopsis

Survey Name: 2020 State of IT Operations and Cybersecurity Operations

Survey Date: March 2020

Primary Region: North America

Respondent Base: 115 cybersecurity and technology professionals. The margin of error for the total respondent base (N=115) is +/- 9 percentage points.

Purpose: InformationWeek, in partnership with Dark Reading, surveyed general IT professionals and cybersecurity professionals to discover issues related to security maintenance and operations as well as the relationship between IT professionals and cybersecurity professionals.

Methodology: The survey queried decision-makers with IT or cybersecurity job titles or roles at primarily North American organizations. Respondents were asked about their organizations' information security operations, as well as the roles and communication between general IT department staff and cybersecurity department staff. The survey was conducted online. Respondents were recruited via an email invitation containing an embedded link to the survey. The email invitation was sent to a select group of Informa Tech's qualified database; Informa is the parent company of InformationWeek, Dark Reading, and Interop, among other brands. Informa Tech was responsible for all survey programming, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices.

PREVIOUS NEXT

Introduction

General IT operations groups and IT cybersecurity teams need to work very closely together in order to accomplish their objectives. However, the two groups' goals sometimes conflict with one another. IT operations folks want to provide fast, convenient service to their end users. But the security team needs to make sure that the users and the networks are secure — which sometimes results in slower or less convenient service.

To better understand how businesses are managing those sometimes-conflicting goals and relationships, Dark Reading and InformationWeek surveyed 115 cybersecurity and technology professionals, primarily in North America.

The 2020 State of IT Operations and Cybersecurity Operations survey revealed three distinct but related trends in this relationship. First, business leaders are growing more aware of and concerned about cybersecurity. They are being vocal about their support of security concerns and increasing security budgets.

Second, perhaps as a result of these concerns, security personnel are taking on new and broader responsibilities within the organization. They are becoming involved in projects at an earlier stage, and they are taking on some tasks that IT operations staff formerly performed.

Third, perhaps as a result of these new responsibilities, the relationship between IT operations and security personnel is growing a little bit more tense. The relationship hasn't exactly become hostile, but survey respondents were definitely noticing a need for improvement.

The following sections of the report delve into each of these trends in greater detail.

PREVIOUS NEXT

Increasing Security Concerns

One of the easiest ways to identify what is important to an organization is to look at how it spends its money. This year's survey revealed that organizations are spending significantly more on cybersecurity compared to last year.

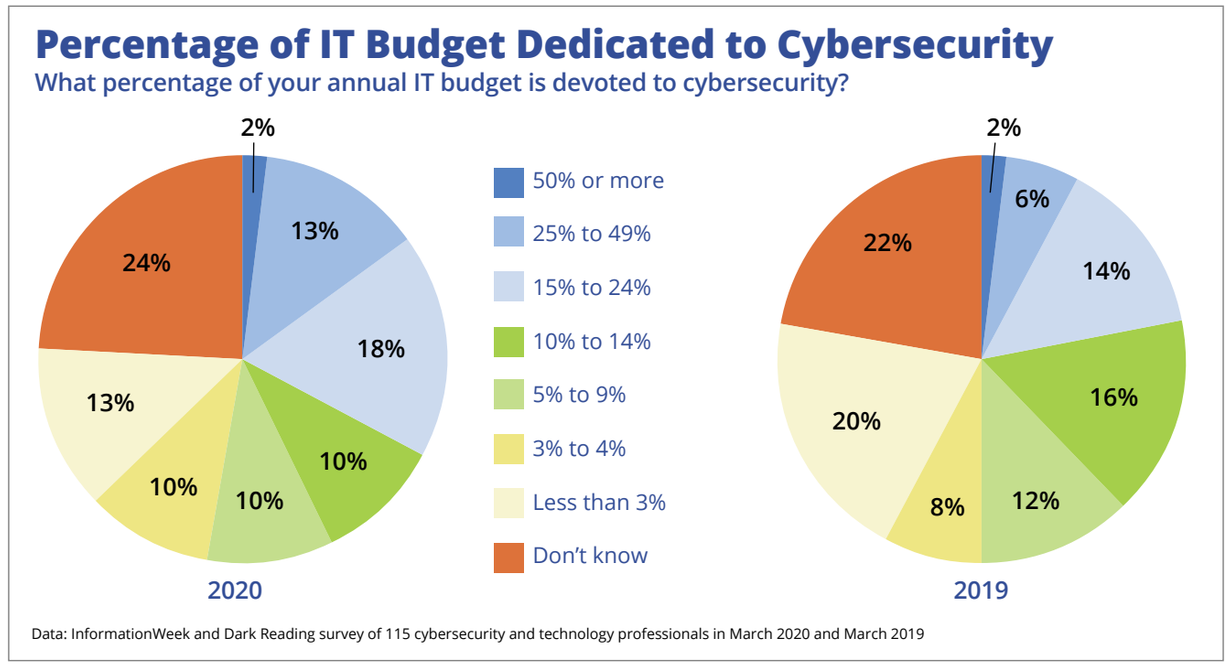
While the percentage of organizations spending more than half of their IT budgets on cybersecurity remained steady at just 2%, those spending a quarter or more on cybersecurity nearly doubled from 8% in 2019 to 15% in 2020. And those spending 15% or more of their IT budgets on cybersecurity climbed from 22% to 33%. Meanwhile, the number spending less than 10% on cybersecurity dropped from 40% to 33% (**Figure 1**).

In an interview, survey participant John Krull, principal consultant at Tech Reformers and former CIO at Seattle Public Schools and former CTO at Oakland Unified School District, echoed these findings. He said that he has noticed "an increasing fear of phishing and ransomware. Leaders are willing to support spending on solutions that solve the problem. They like seeing protections in place and are more open to inconveniences."

Respondents' perceptions of top managers' opinions on cybersecurity also showed an uptick. While 30% of 2019 respondents said that cybersecurity was "absolutely critical, that number climbed to 39% for 2020 (**Figure 2**).

Those who rated cybersecurity as important or critical jumped from 82% to 87%. It's also noteworthy that almost none of the respondents said they didn't know whether cybersecurity was important to their management teams.

Figure 1



PREVIOUS NEXT

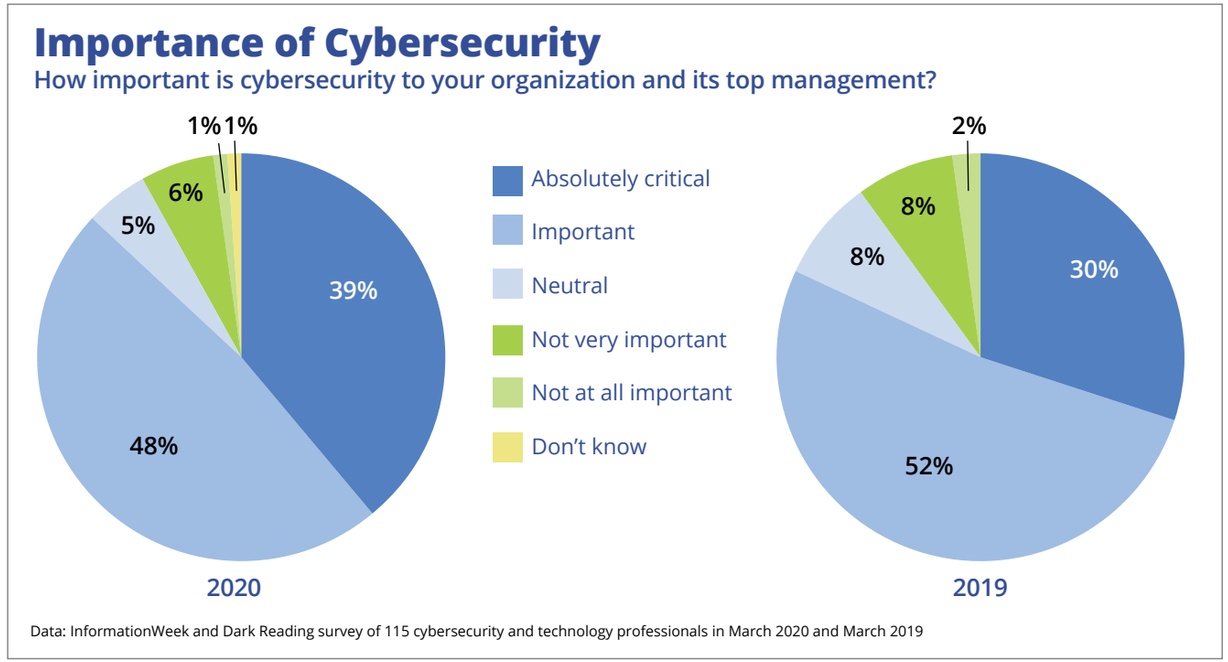
Interestingly, even though organizations are more concerned about cybersecurity, they are not damping down their quest for digital innovation. In fact, the number of respondents saying that digital innovation was absolutely critical climbed from 25% in 2019 to 32% in 2020 (**Figure 3**).

Clearly, business leaders expect IT to be able to support both increasing cybersecurity and increasing digital innovation at the same time. However, respondents' answers to questions about attitudes toward cybersecurity reflect a slight bias in favor of security over innovation.

In 2019, the No. 1 response to being asked about the organization's attitude toward cybersecurity was "security is important, but we are willing to take some risks if we find a new technology that could positively affect our business" (**Figure 4**).

But in 2020, the top answer was "security is paramount, and we take a cautious approach to IT innovation." In addition, the number of people who said that innovation and speed are more important than security dropped from 17% to just 5%.

Figure 2



Changing Roles

As business leaders become more concerned about cybersecurity, they seem to be formalizing security personnel's roles and expecting the security team to handle more responsibilities. For example, in last year's survey, 40% of respondents said that the general IT team usually fixed any security problems that occurred. This year, responses flipped, with 40% saying the security team usually corrects problems while only 36% said it was usually the general IT team (**Figure 5**).

Project managers are also involving security earlier in the project lifecycle. Nearly half (49%) said that security gets involved at the very beginning of "every new project" or "most important projects" (**Figure 6**).

And the number of respondents saying security is not part of project planning and seen as an annoyance dropped from 12% to 3%.

This is good news from the point of view of security experts, who generally recommend bringing in security as early as possible. For example, Krull said, "My advice is bringing in the security team at the very beginning of development or SaaS integration projects."

Still, organizations still have a way to go in formalizing the relationship between developers and security. Only 14% of respondents said that they have "a mature DevSecOps structure that integrates development, operations and security," and 27% use a secure software development lifecycle framework (**Figure 7**).

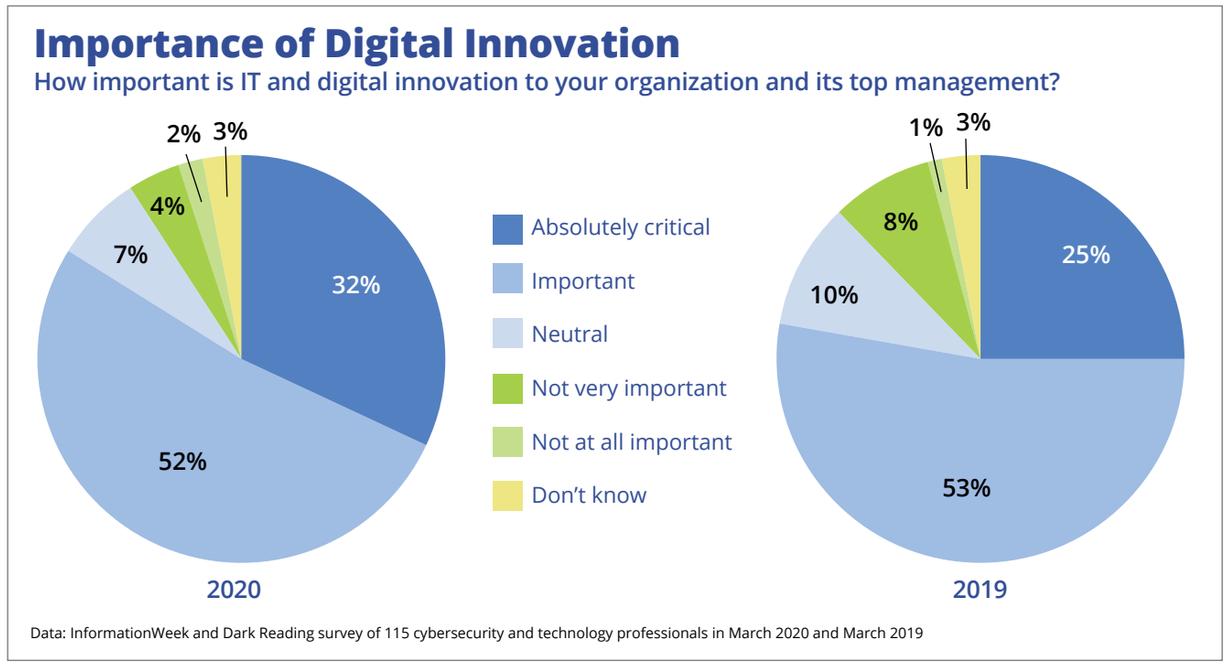
More than a third of respondents indicated that while they consider security in application development, they don't use any formal process to ensure that secure development happens.

The survey results also highlighted some changes in which teams are responsible for which security functions. In particular, it showed significant increases in the number of security teams now handling cloud security, endpoint security, firewall configuration, mobile device security, network security, and supplier/supply chain security. And accordingly, the general IT teams were less likely to be responsible for each of these areas (**Figure 8**).

On the other hand, general IT teams seem to be taking more responsibility for compliance, and while it is still far more common for the security team to handle security policy and privacy, general IT seems to be getting more involved in both of these areas.

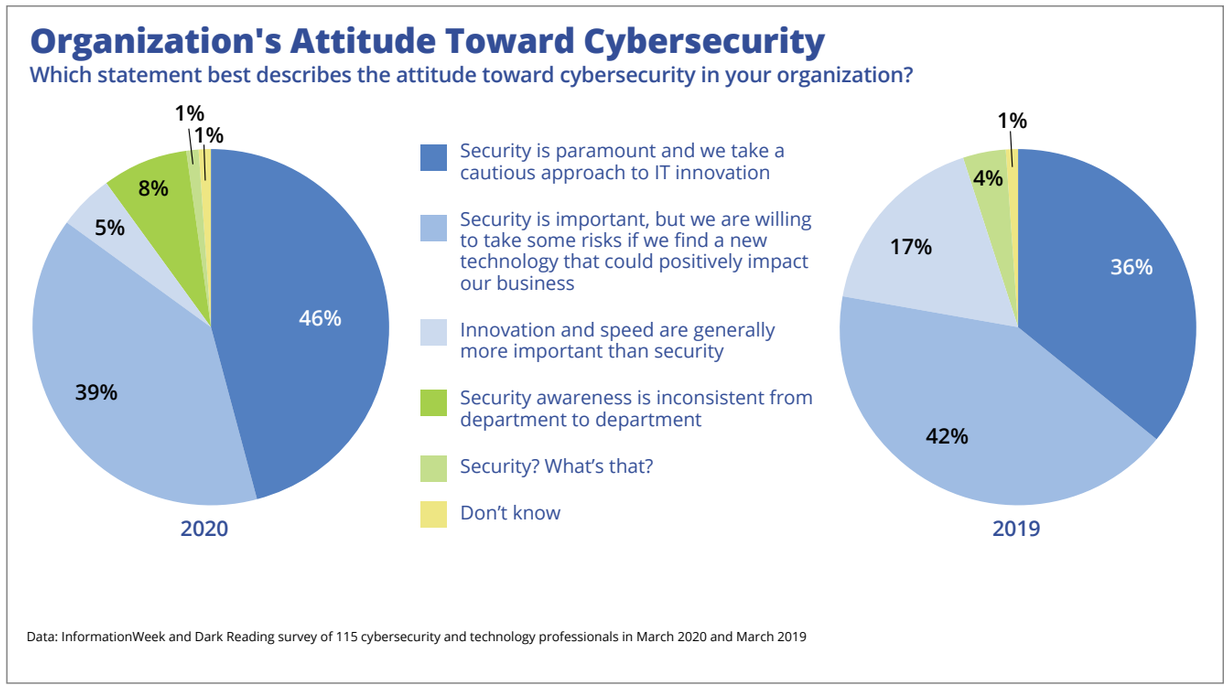
Perhaps the most significant change in this chart between 2019 and 2020 is the decrease in the number of respondents who didn't know who was responsible for a particular function. Organizations seem

Figure 3



PREVIOUS NEXT

Figure 4



to be becoming more deliberate in their assigning of security-related tasks and roles.

Increasing Tension

As security takes on a bigger role, some organizations are experiencing growing pains, particularly in regard to the relationship between security and IT. In 2019, 57% of respondents said that the security and IT staffs were communicating well, but this year, that dropped to just 48% (**Figure 9**). And the number of respondents citing occasional miscommunication problems jumped from 21% to 32% this year.

When asked about problems in the relationship between IT and cybersecurity, several people mentioned difficulties in communication. One said, "Communication that is not formalized or only verbal is a key factor of conflict." Another complained about "not knowing when an incident occurred. It is hush-hush."

But miscommunication isn't the only source of tension. Another respondent pointed to difficulties "overcoming rabid security trying not to yield to allow business to function." On the flip side, a security team member said, "Security concerns are often seen as paranoia."

In general, however, 44% of respondents said, "IT and security are working well together today, and the relationship is improving" (**Figure 10**). That was just a slight drop from the 47% who said the same thing in 2019. There was a somewhat bigger increase in the number of people saying the relationship between the two groups needs work — up to 32% this year from 25% in the previous survey.

When disagreements do occur, it's generally the CIO who decides how to settle it. This year 45% of respondents pointed to the CIO as the final decision maker, up significantly

from the 30% who said the same thing last year (**Figure 11**).

And the number of CISOs and committees making these sorts of decisions dropped. The number of people who said they didn't know who made the final call also dropped significantly, which makes it seem like CIOs are becoming a little stronger and more forceful about asserting their leadership. That could be useful when planning how to overcome some of these challenges in the relationship between IT and security.

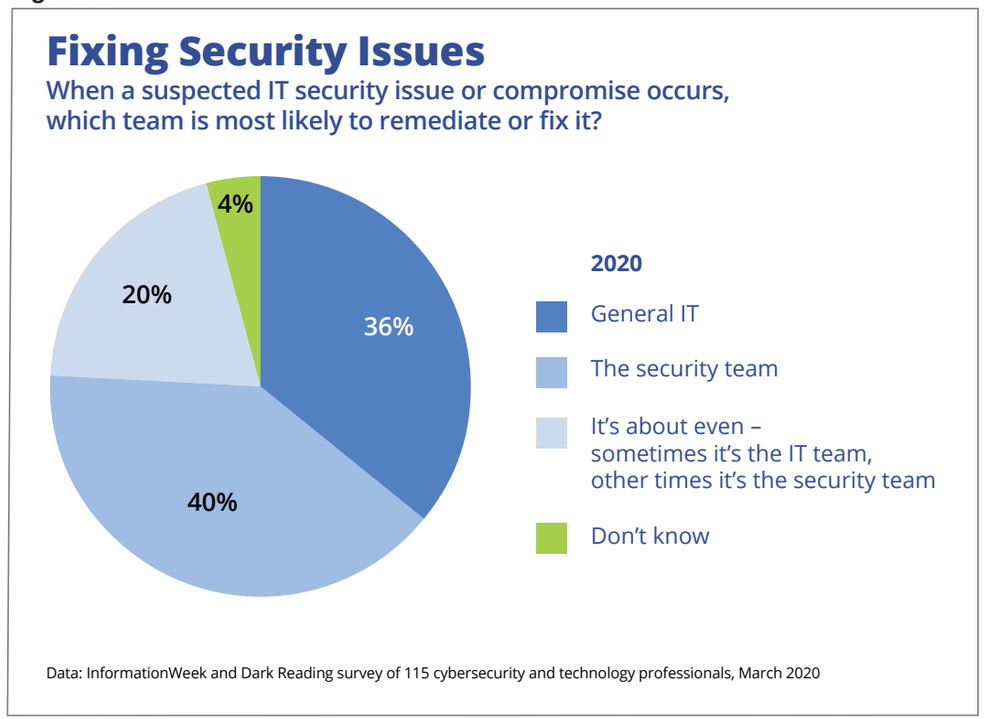
Looking Ahead

The survey asked respondents some open-ended questions about what things they wanted to see their organizations do better, and several respondents also participated in individual interviews where they expressed their opinions on what was working well at their organizations and what could be improved.

Survey respondent Alan Shen of Anthem said that having mature DevSecOps practices in place at his company had been helpful in the relationship between IT and IT security. However, he noted, "The platforms utilized by general IT and security are not yet centralized and shared, thus when responding or addressing issues or incidences, there are lags/gaps/delays which can be removed if there were an integrated/ comprehensive platform utilized by all IT/IS resources."

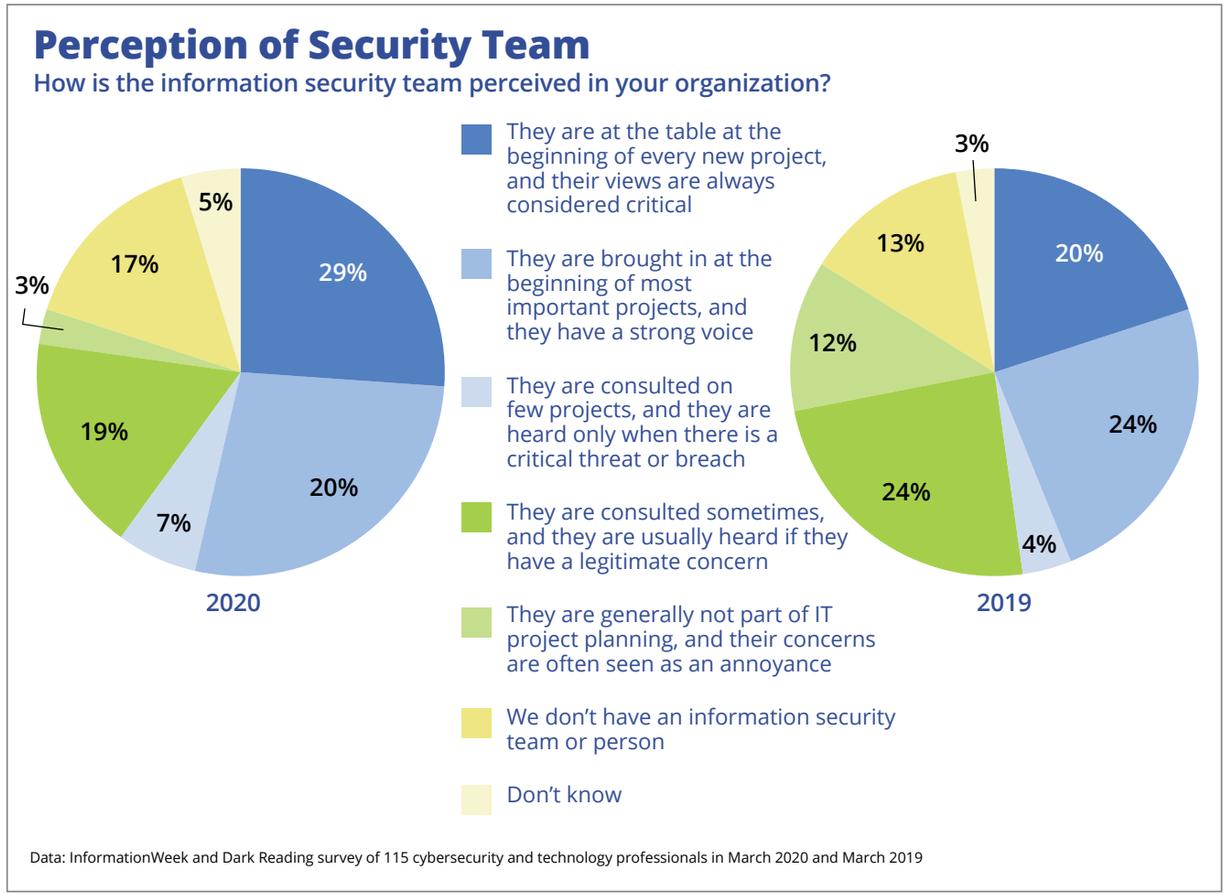
Another participant, Shiva Rajagopalan, a senior director of IT security, agreed on the importance of DevSecOps. "The DevSecOps approach has strengthened the working/ relationship/camaraderie with the security team as there are many educational events/brown bag lunches held internally so that one can appreciate what security wants from IT and vice versa. They work hand-in-glove at the moment."

Figure 5



PREVIOUS NEXT

Figure 6



Rajagopalan added that he would like to see his company do more cross-functional rotations within the teams. "These rotations have improved the overall perspective, made a well-rounded IT pro and also provided educational/stretch assignments."

Another survey respondent said that "using collaboration tools and good old fashion[ed] communication with others" had helped, adding, "Keep it give and take."

Several pointed to the importance of information sharing, including one who said, "Share information and provide training on security and networks so everyone is speaking the same language."

Perhaps one participant summarized the overall advice best, writing, "Understand general IT and security are useless without the other. It is one job, with different means. You need both the hammer and the nail before you can build anything."

PREVIOUS NEXT

Appendix

Figure 7

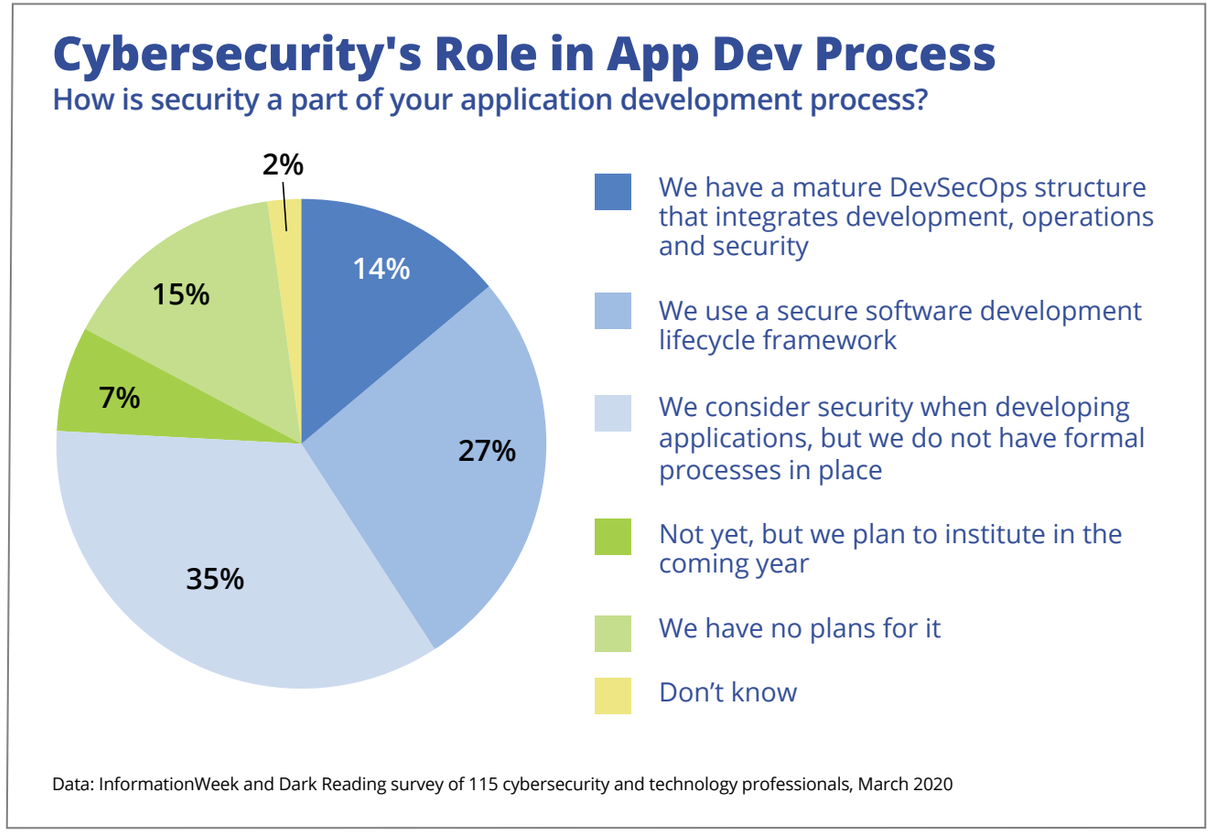


Figure 8

Primary Responsibility

Which team is primarily responsible for the following functions?

	2020 IT Security Team	2019 IT Security Team	2020 General IT Team	2019 General IT Team	2020 Don't know	2019 Don't know
Application security	47%	46%	50%	46%	3%	8%
Cloud security	69%	48%	28%	41%	3%	11%
Compliance	47%	69%	53%	21%	0%	10%
Developing/writing enterprise security policy	84%	90%	14%	6%	2%	4%
Disaster recovery/business continuity	41%	46%	59%	52%	0%	2%
End user identity/provisioning	28%	19%	72%	77%	0%	4%
Endpoint security	70%	59%	30%	35%	0%	6%
Firewall configuration	49%	37%	49%	60%	2%	4%
Mobile device security	54%	39%	43%	48%	3%	13%
Network security	61%	44%	39%	48%	0%	7%
Patch management	27%	13%	73%	80%	0%	7%
Privacy	63%	69%	31%	19%	6%	12%
Risk measurement/reporting	70%	75%	27%	21%	3%	4%
Router configuration	31%	14%	64%	85%	5%	2%
Security incident response	87%	85%	13%	9%	0%	6%
Security threat analysis	92%	89%	5%	4%	3%	7%
Security threat detection	81%	80%	16%	13%	3%	7%
Storage/archiving	17%	4%	83%	91%	0%	6%
Supplier/supply chain security	60%	25%	30%	54%	10%	21%

Base: Those with separate IT and cybersecurity teams
Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019

PREVIOUS NEXT

Figure 9

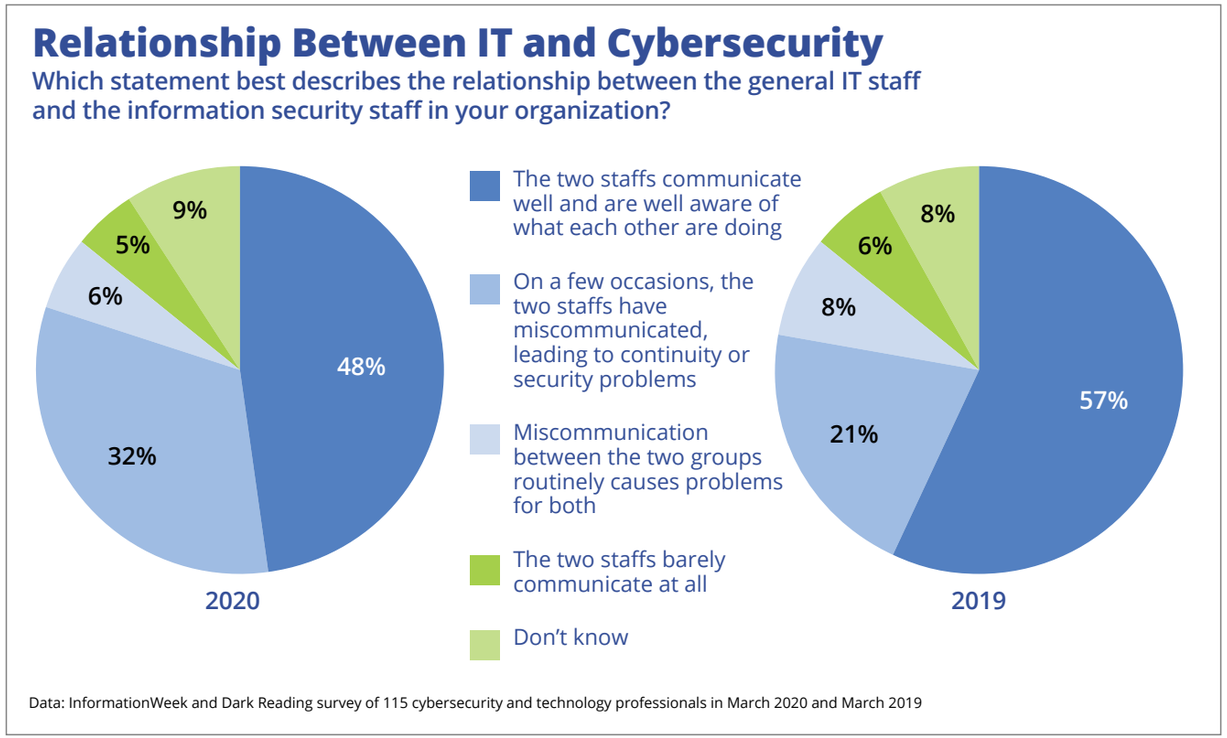
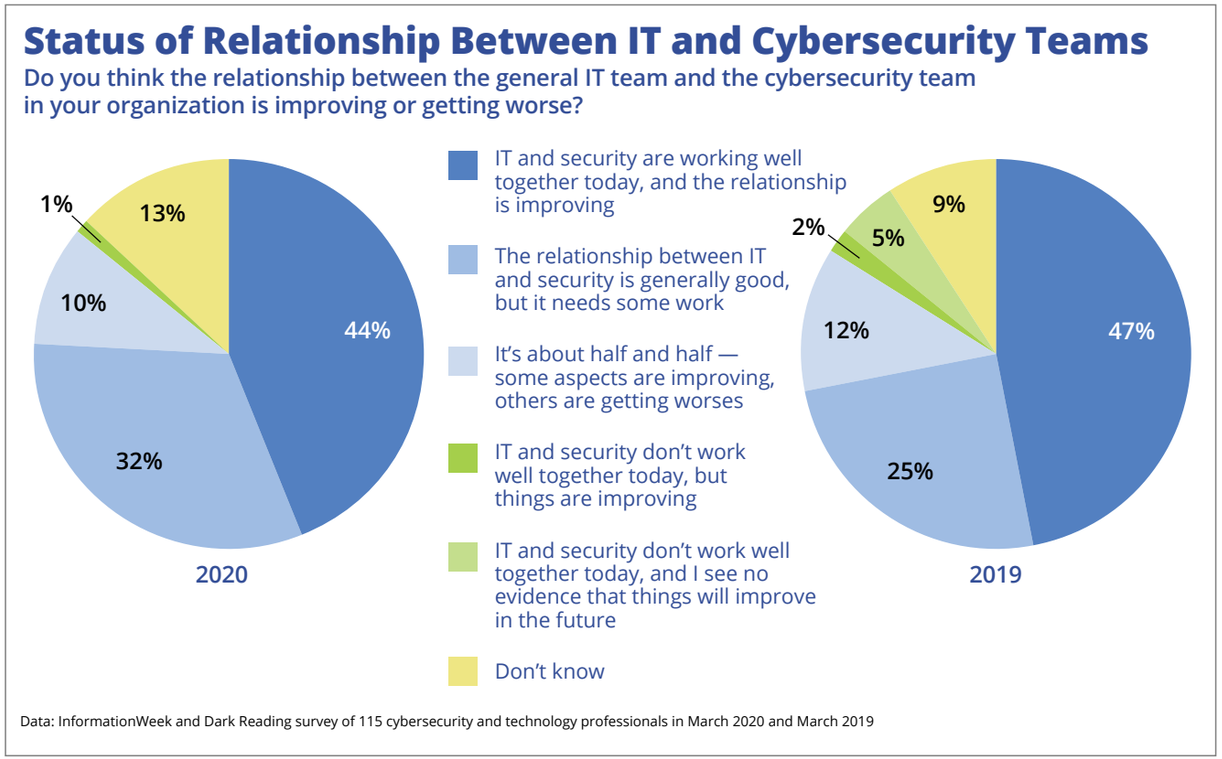
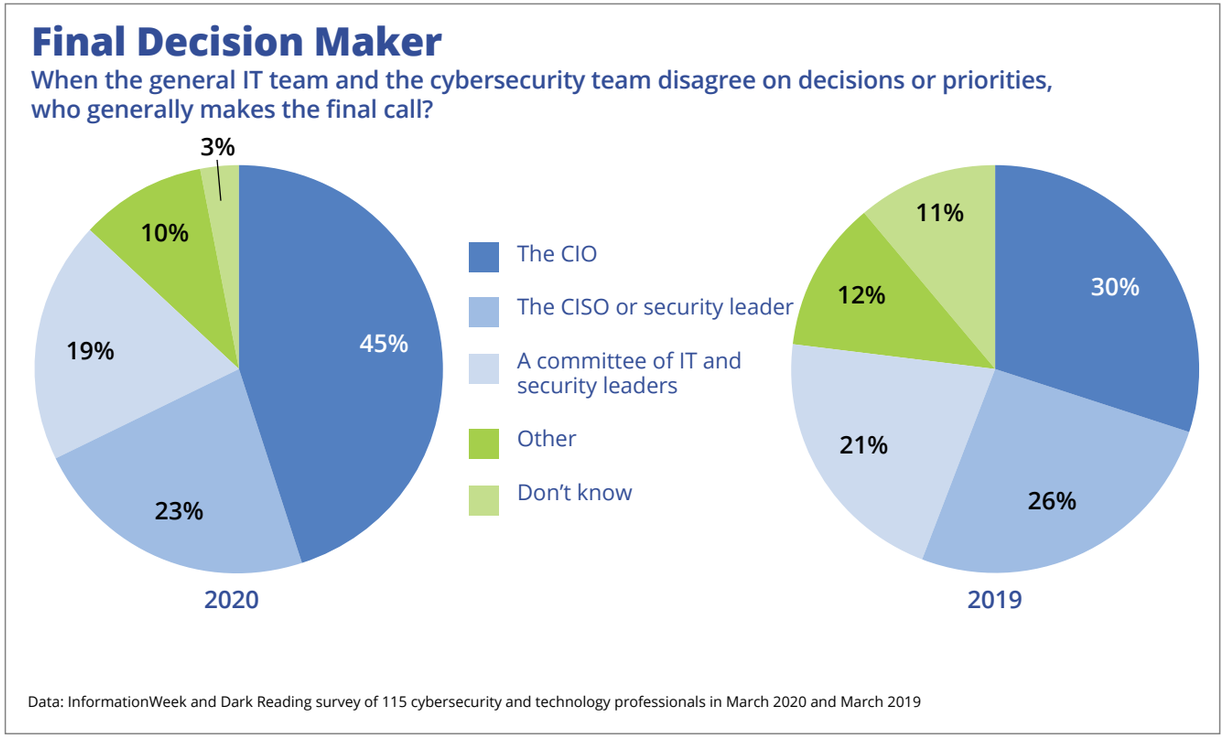


Figure 10



Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019

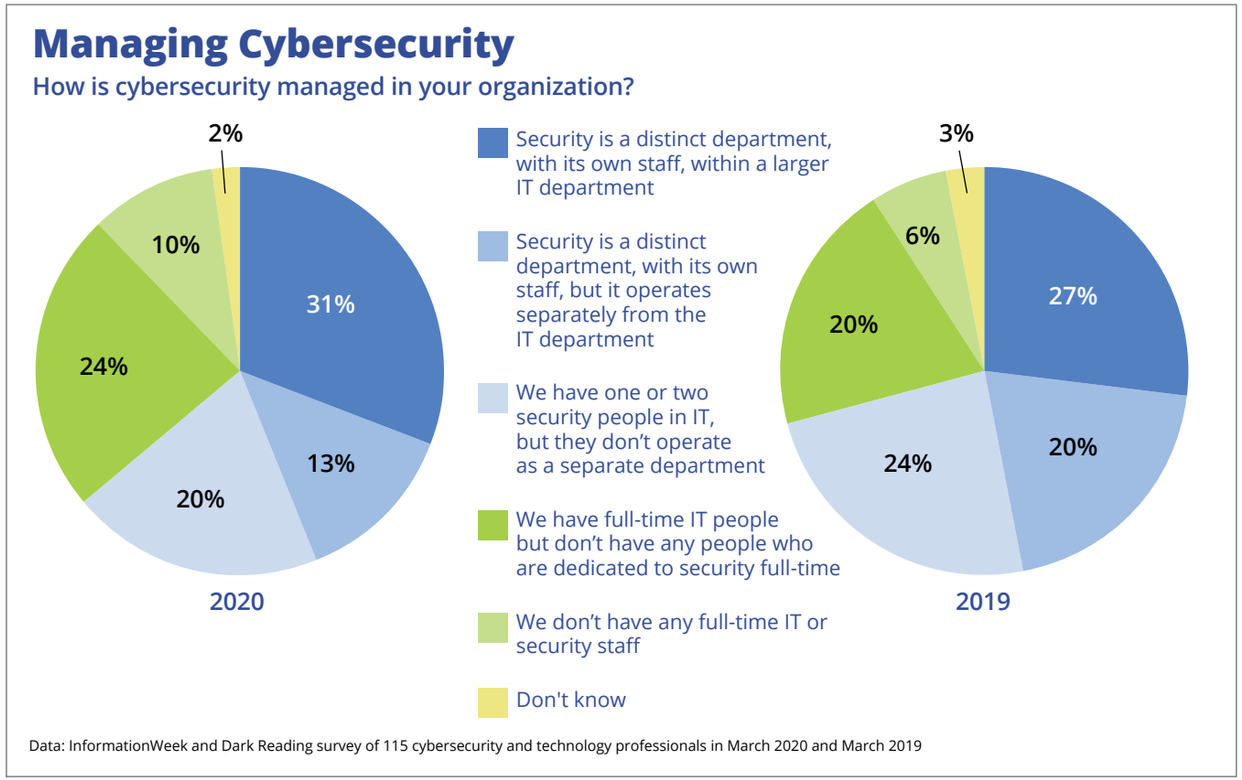
Figure 11



Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019

PREVIOUS NEXT

Figure 12



Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019

Figure 13

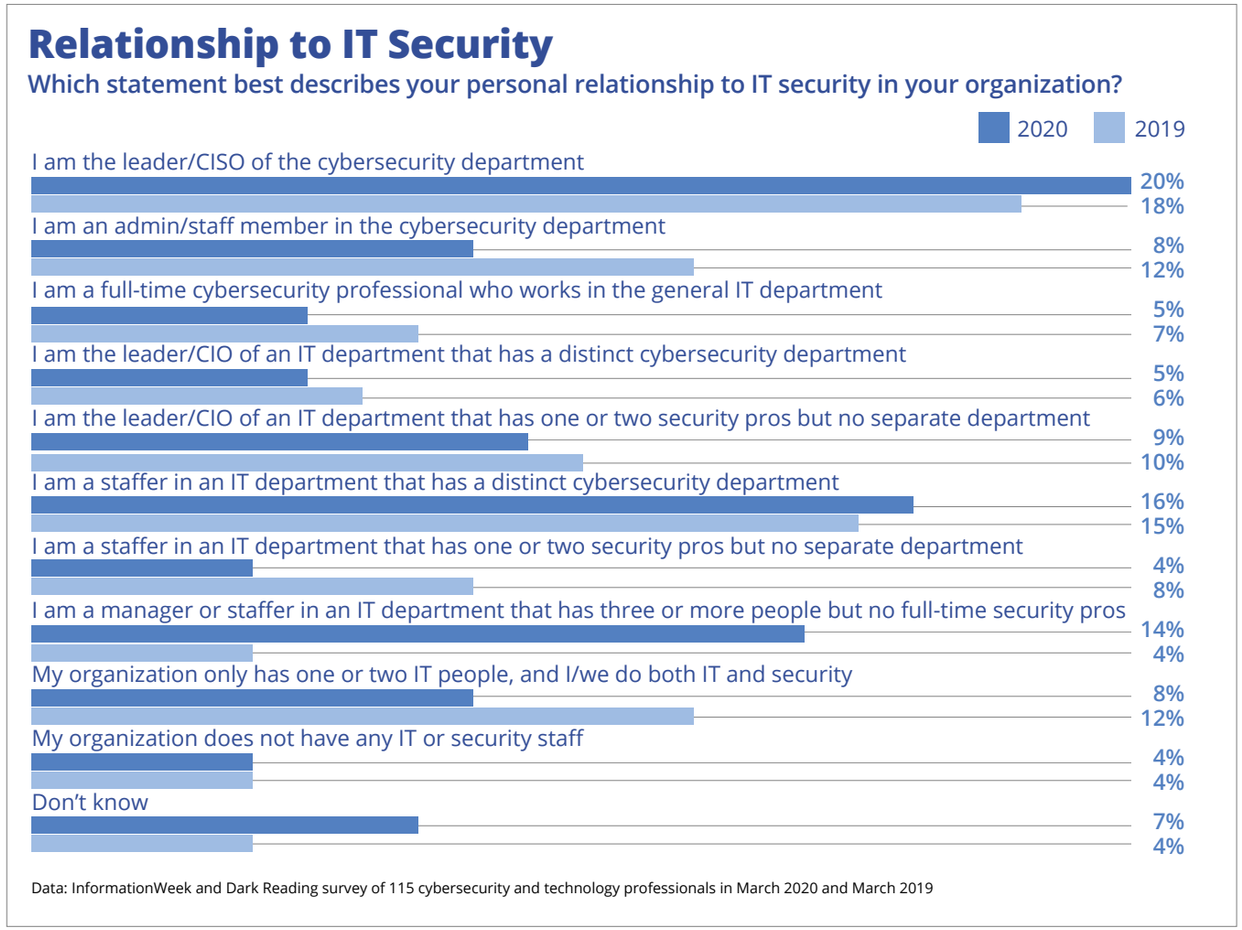
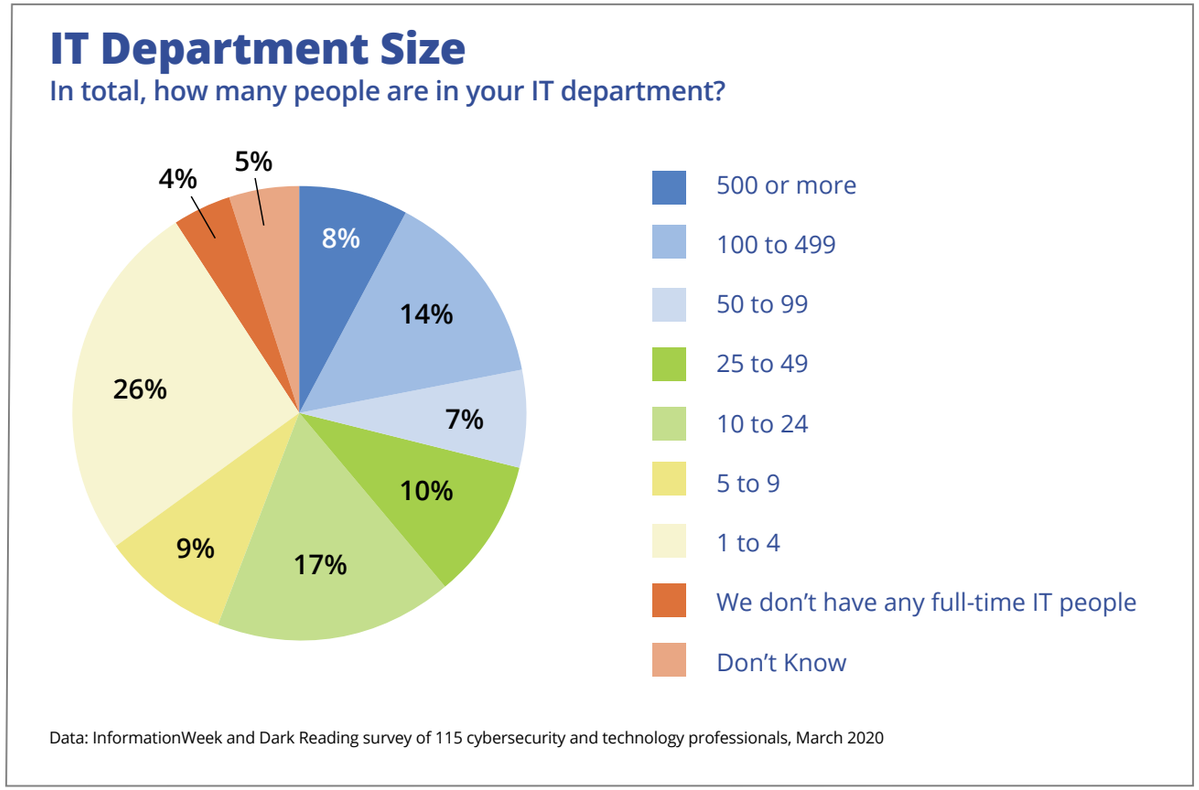

Relationship to IT Security
Which statement best describes your personal relationship to IT security in your organization?
2020
2019
I am the leader/CISO of the cybersecurity department
20%
18%
I am an admin/staff member in the cybersecurity department
8%
12%
I am a full-time cybersecurity professional who works in the general IT department
5%
7%
I am the leader/CIO of an IT department that has a distinct cybersecurity department
5%
6%
I am the leader/CIO of an IT department that has one or two security pros but no separate department
9%
10%
I am a staffer in an IT department that has a distinct cybersecurity department
16%
15%
I am a staffer in an IT department that has one or two security pros but no separate department
4%
8%
I am a manager or staffer in an IT department that has three or more people but no full-time security pros
14%
4%
My organization only has one or two IT people, and I/we do both IT and security
8%
12%
My organization does not have any IT or security staff
4%
4%
Don't know
7%
4%
Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019

Figure 14


IT Department Size
In total, how many people are in your IT department?
8%
14%
7%
10%
17%
9%
26%
4%
5%
500 or more
100 to 499
50 to 99
25 to 49
10 to 24
5 to 9
1 to 4
We don't have any full-time IT people
Don't Know
Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals, March 2020

PREVIOUS NEXT

Figure 15

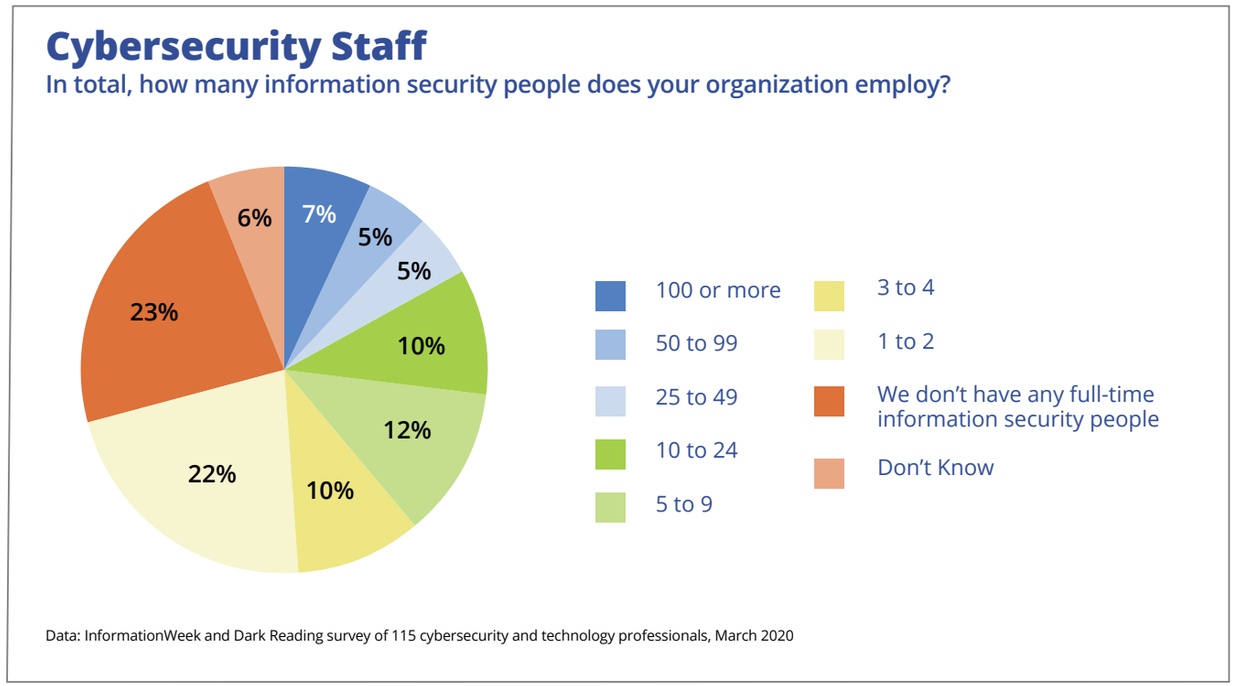


Figure 16

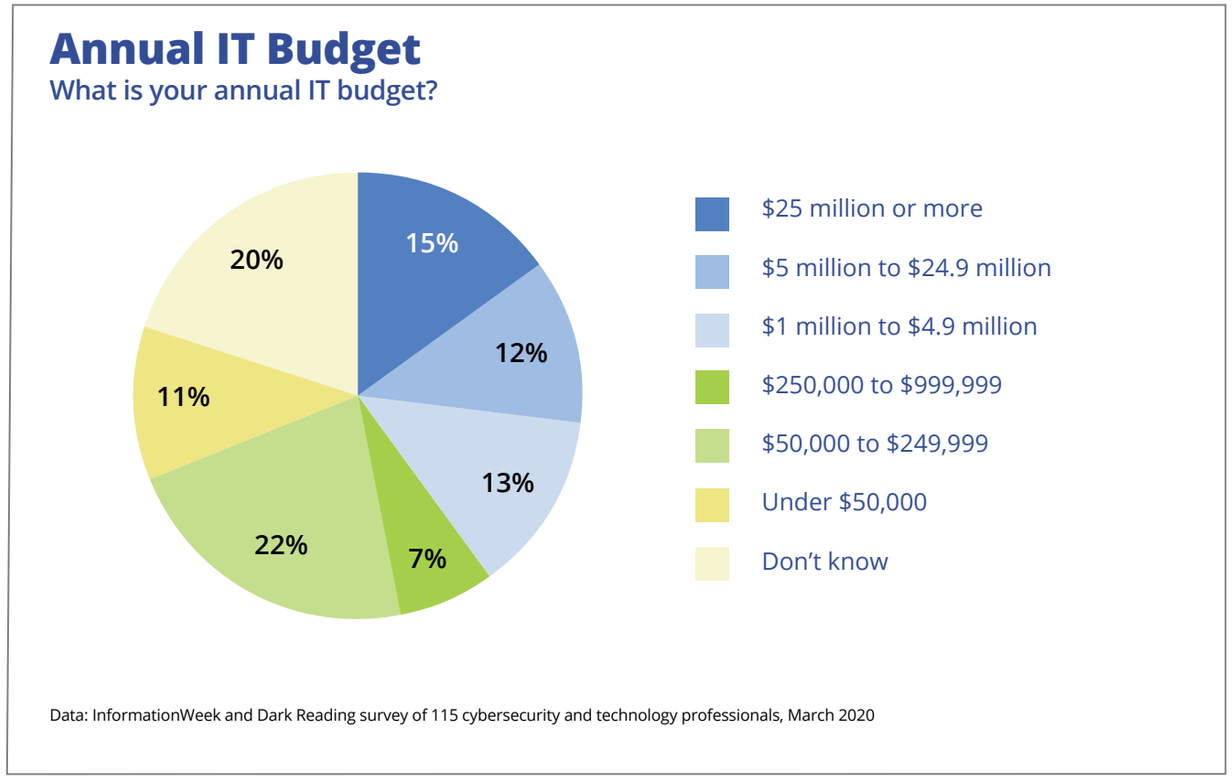
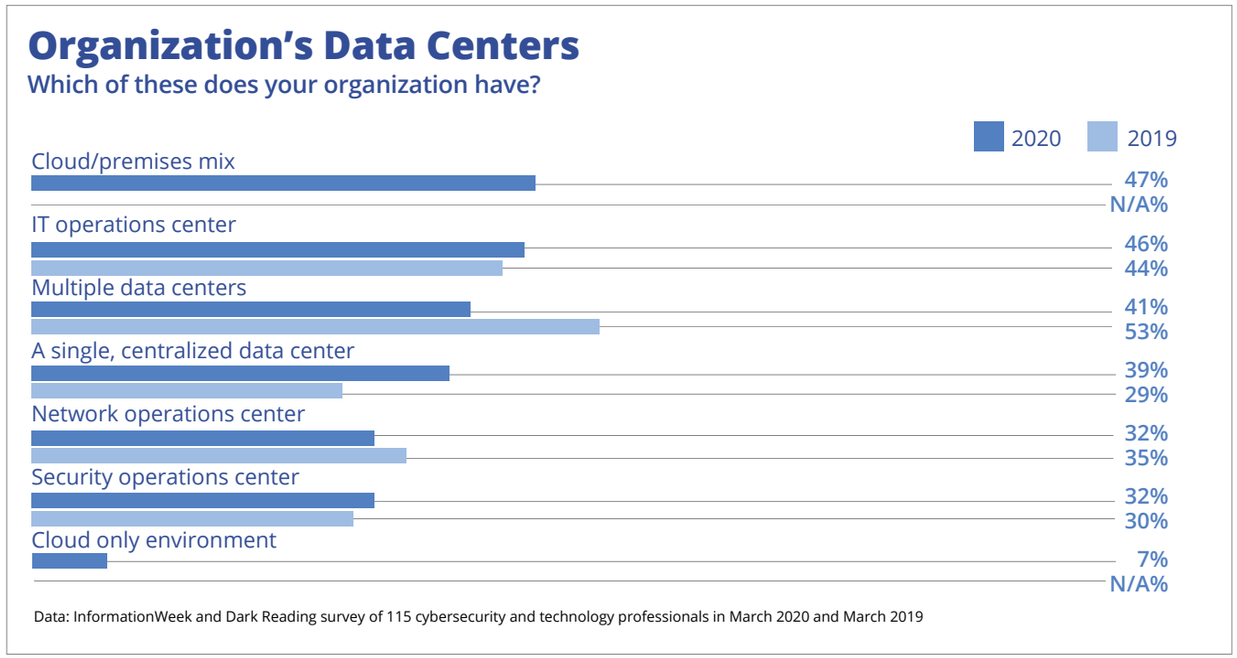

Annual IT Budget
What is your annual IT budget?
15%
12%
13%
7%
22%
11%
20%
$25 million or more
$5 million to $24.9 million
$1 million to $4.9 million
$250,000 to $999,999
$50,000 to $249,999
Under $50,000
Don't know
Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals, March 2020

Figure 17


Organization's Data Centers
Which of these does your organization have?
2020
2019
Cloud/premises mix
47%
N/A%
IT operations center
46%
44%
Multiple data centers
41%
53%
A single, centralized data center
39%
29%
Network operations center
32%
35%
Security operations center
32%
30%
Cloud only environment
7%
N/A%
Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019

PREVIOUS NEXT

Figure 18

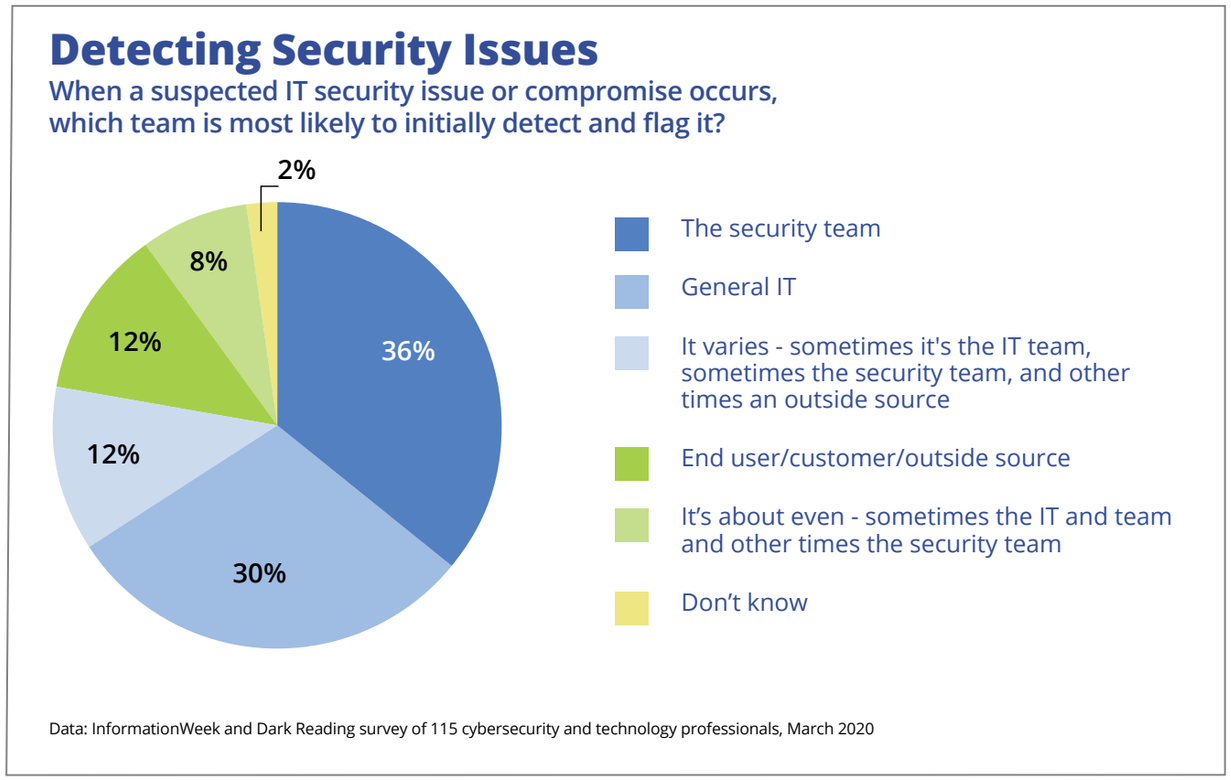
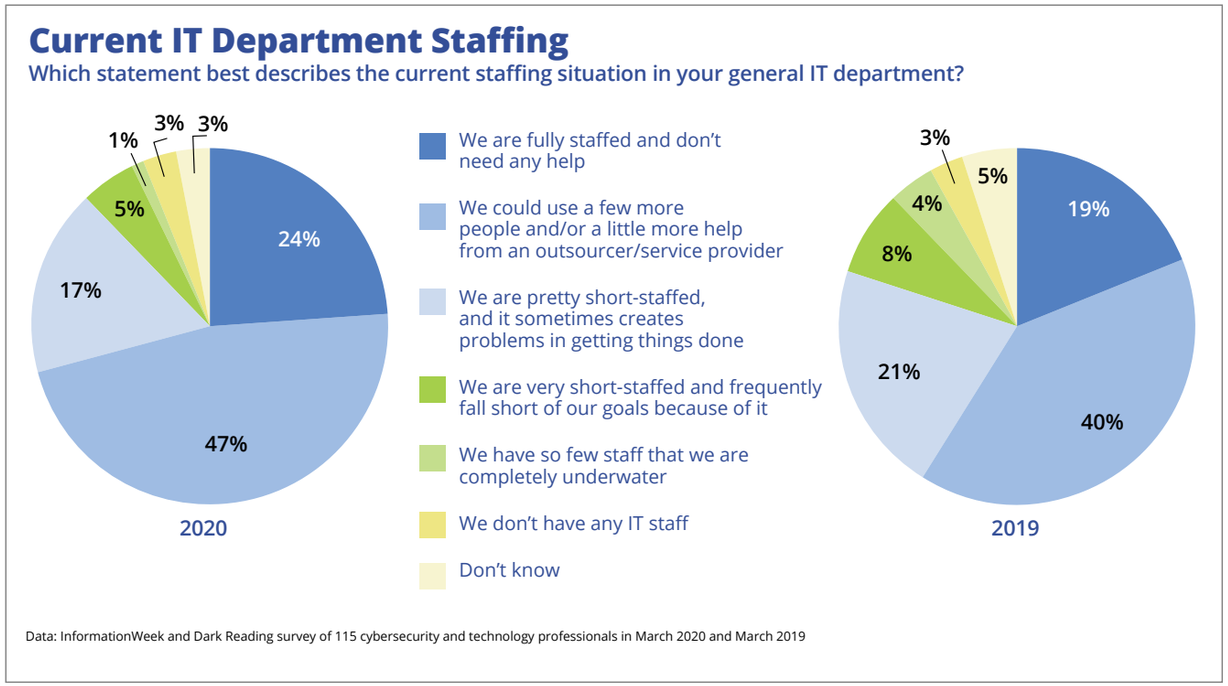
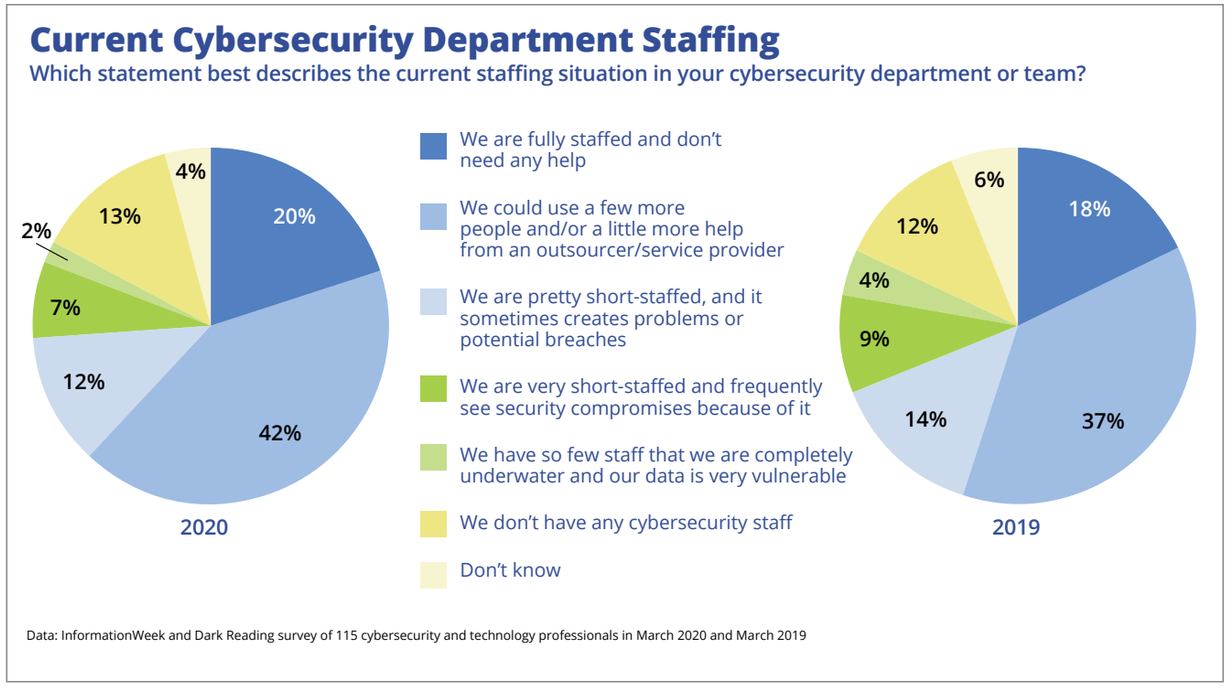


Figure 19


Current IT Department Staffing
Which statement best describes the current staffing situation in your general IT department?
24%
47%
17%
5%
1%
3%
3%
2020
We are fully staffed and don't need any help
We could use a few more people and/or a little more help from an outsourcer/service provider
We are pretty short-staffed, and it sometimes creates problems in getting things done
We are very short-staffed and frequently fall short of our goals because of it
We have so few staff that we are completely underwater
We don't have any IT staff
Don't know
19%
40%
21%
8%
4%
5%
3%
2019
Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019

PREVIOUS NEXT

Figure 20



PREVIOUS NEXT

Figure 21

Outsourced IT Functions

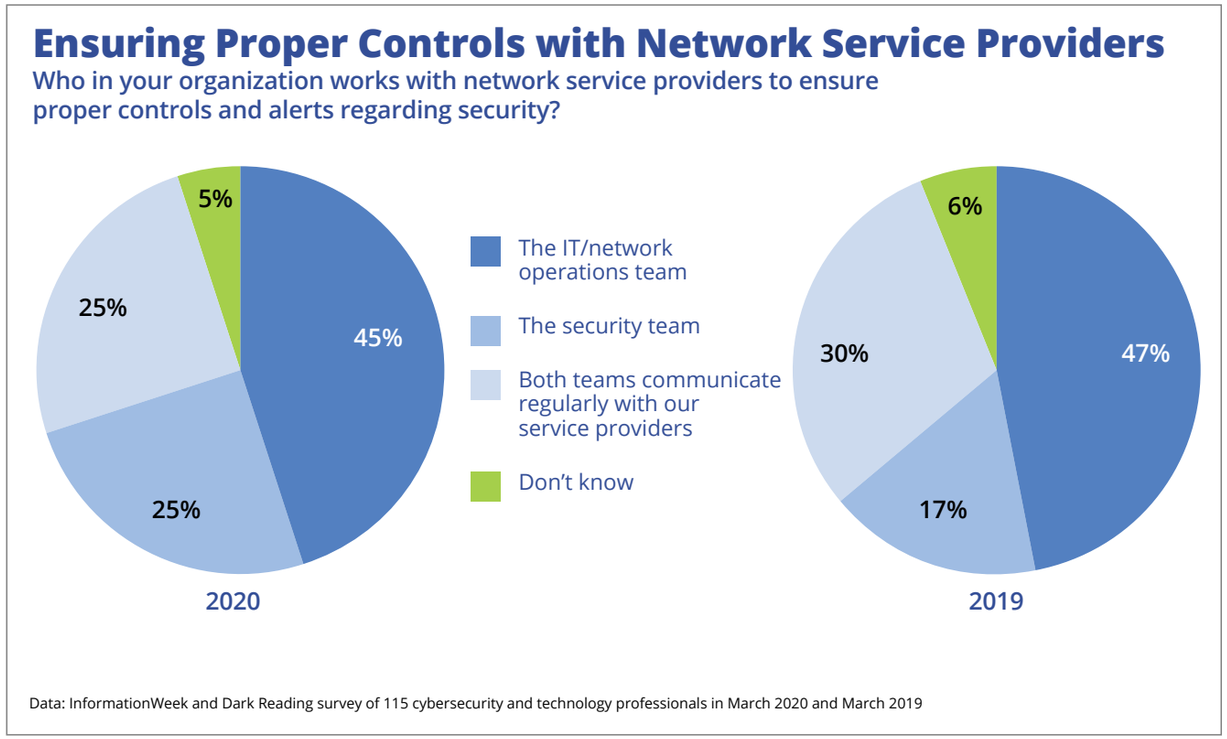
Which IT functions do you outsource?

	Currently outsource	Plan to outsource in the next 12 months	Do not outsource nor plan to outsource	Don't know
Application development	18%	18%	58%	7%
Data storage/archival	17%	19%	60%	5%
Endpoint device management	17%	11%	62%	10%
Help desk/end user services	18%	13%	64%	4%
IT/systems operations	11%	8%	74%	7%
Network operations	10%	8%	76%	6%
Security operations	17%	10%	68%	6%
Web servers/services	36%	12%	48%	4%

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals, March 2020

PREVIOUS NEXT

Figure 22



PREVIOUS NEXT

Figure 23

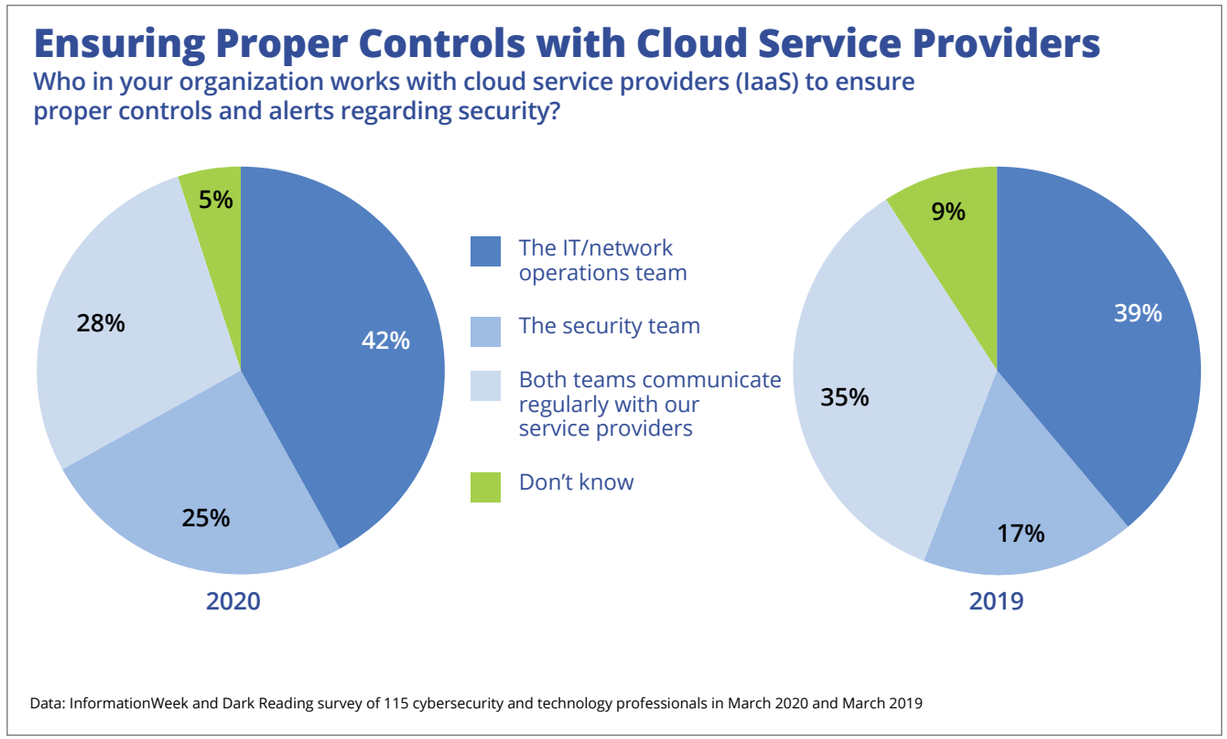
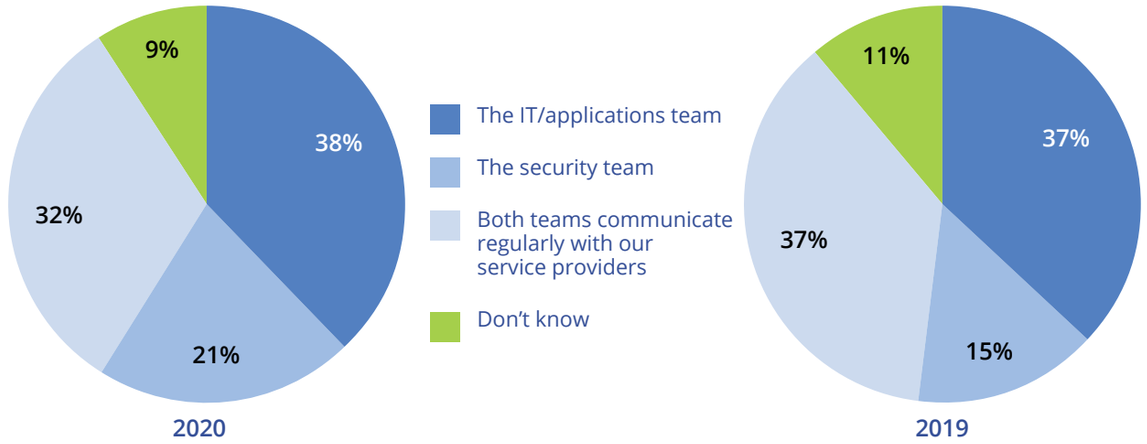


Figure 24

Ensuring Proper Controls with Application Service Providers

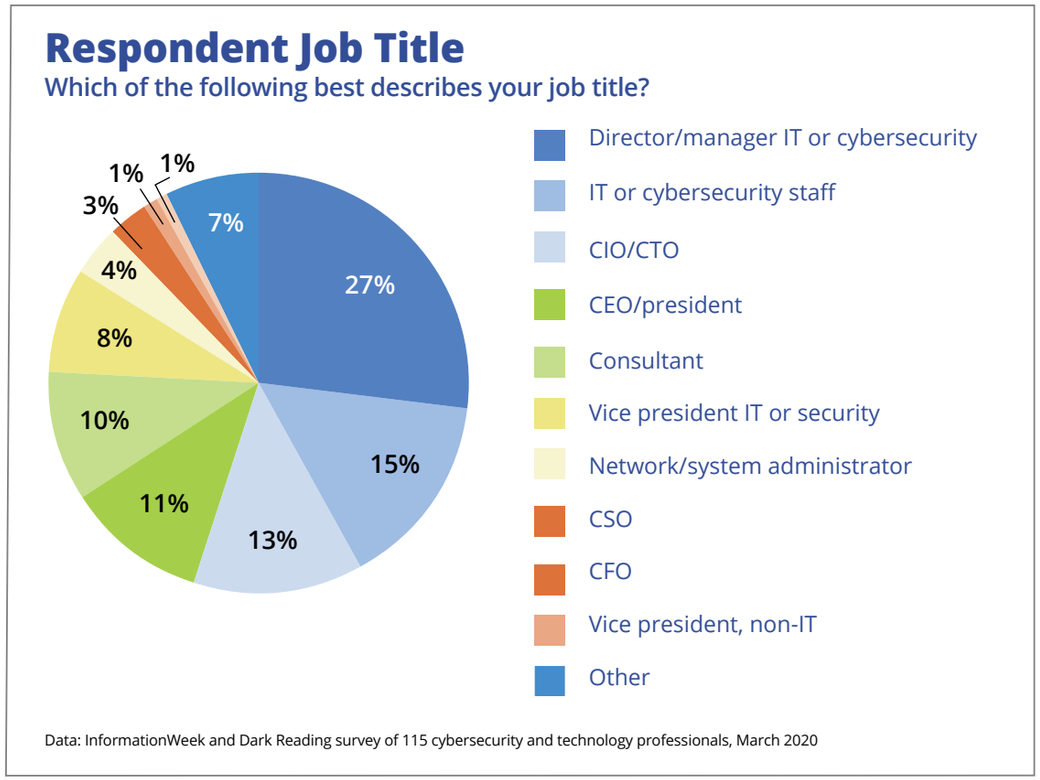
Who in your organization works with application services or software-as-a-service providers to ensure proper controls and alerts regarding security?



Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019

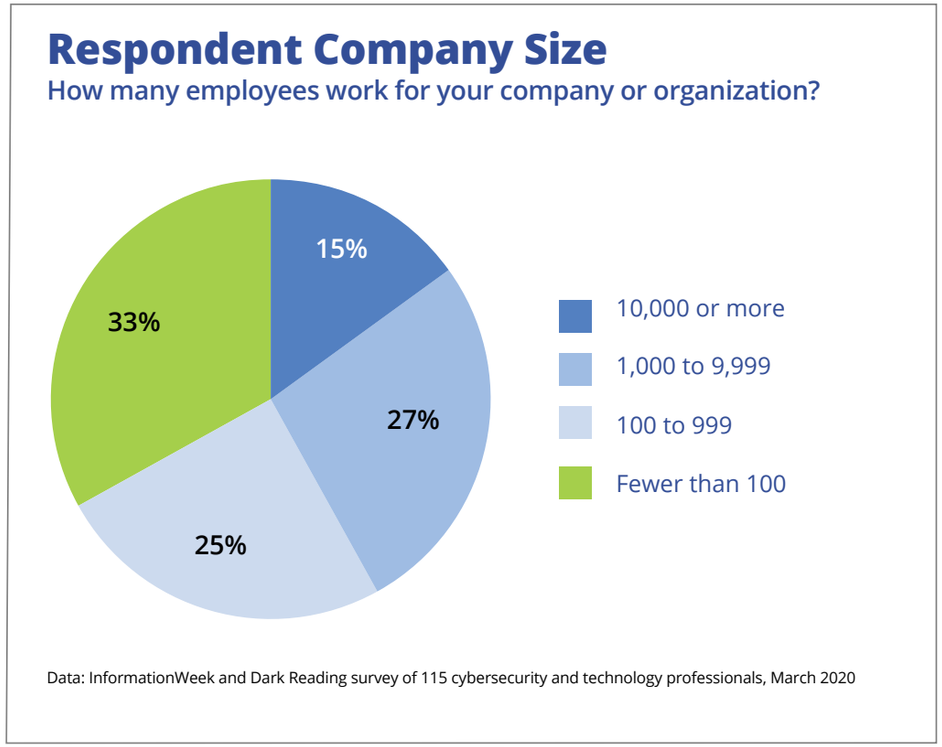
PREVIOUS NEXT

Figure 25



PREVIOUS NEXT

Figure 26



PREVIOUS

Figure 27