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.
Table of Contents

3 Author
4 Executive Summary
5 Research Synopsis
6 Introductions
7 Increasing Security Concerns
8 Changing Roles
10 Increasing Tension
11 Looking Ahead
13 Appendix

Figures
Figure 1 Percentage of IT Budget Dedicated to Cybersecurity
Figure 2 Importance of Cybersecurity
Figure 3 Importance of Digital Innovation
Figure 4 Organization's Attitude Toward Cybersecurity
Figure 5 Fixing Security Issues
Figure 6 Perception of Security Team
Figure 7 Cybersecurity's Role in App Dev Process
Figure 8 Primary Responsibility
Figure 9 Relationship Between IT and Cybersecurity
Figure 10 Status of Relationship Between IT and Cybersecurity Teams
Figure 11 Final Decision Maker
Figure 12 Managing Cybersecurity
Figure 13 Relationship to IT Security

Figure 14 IT Department Size
Figure 15 Cybersecurity Staff
Figure 16 Annual IT Budget
Figure 17 Organization's Data Centers
Figure 18 Detecting Security Issues
Figure 19 Current IT Department Staffing
Figure 20 Current Cybersecurity Department Staffing
Figure 21 Outsourced IT Functions
Figure 22 Ensuring Proper Controls with Network Service Providers
Figure 23 Ensuring Proper Controls with Cloud Service Providers
Figure 24 Ensuring Proper Controls with Application Service Providers
Figure 25 Respondent Job Title
Figure 26 Respondent Company Size
Figure 27 Respondent Industry
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.
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.
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.
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.
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%.

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
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**

Fixing Security Issues

When a suspected IT security issue or compromise occurs, which team is most likely to remediate or fix it?

<table>
<thead>
<tr>
<th>Team</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>General IT</td>
<td>20%</td>
</tr>
<tr>
<td>The security team</td>
<td>36%</td>
</tr>
<tr>
<td>It’s about even – sometimes it’s the IT team, other times it’s the security team</td>
<td>40%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>4%</td>
</tr>
</tbody>
</table>

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

![Figure 6: Perception of Security Team](image-url)

How is the information security team perceived in your organization?

- They are at the table at the beginning of every new project, and their views are always considered critical: 20%
- They are brought in at the beginning of most important projects, and they have a strong voice: 24%
- They are consulted on few projects, and they are heard only when there is a critical threat or breach: 24%
- They are consulted sometimes, and they are usually heard if they have a legitimate concern: 17%
- They are generally not part of IT project planning, and their concerns are often seen as an annoyance: 7%
- We don’t have an information security team or person: 29%
- Don’t know: 3%

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

Figure 7

**Cybersecurity's Role in App Dev Process**

How is security a part of your application development process?

- We have a mature DevSecOps structure that integrates development, operations and security: 2%  
- We use a secure software development lifecycle framework: 14%  
- We consider security when developing applications, but we do not have formal processes in place: 27%  
- Not yet, but we plan to institute in the coming year: 35%  
- We have no plans for it: 7%  
- Don't know: 15%  

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals, March 2020
## Figure 8

### Primary Responsibility

Which team is primarily responsible for the following functions?

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

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
Figure 9

**Relationship Between IT and Cybersecurity**

Which statement best describes the relationship between the general IT staff and the information security staff in your organization?

- The two staffs communicate well and are well aware of what each other are doing
- On a few occasions, the two staffs have miscommunicated, leading to continuity or security problems
- Miscommunication between the two groups routinely causes problems for both
- The two staffs barely communicate at all
- Don’t know

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019
**Figure 10**

**Status of Relationship Between IT and Cybersecurity Teams**

Do you think the relationship between the general IT team and the cybersecurity team in your organization is improving or getting worse?

- IT and security are working well together today, and the relationship is improving
- The relationship between IT and security is generally good, but it needs some work
- It’s about half and half — some aspects are improving, others are getting worse
- IT and security don’t work well together today, but things are improving
- IT and security don’t work well together today, and I see no evidence that things will improve in the future
- Don’t know

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019
Figure 11

Final Decision Maker
When the general IT team and the cybersecurity team disagree on decisions or priorities, who generally makes the final call?

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019
Managing Cybersecurity
How is cybersecurity managed in your organization?

- Security is a distinct department, with its own staff, within a larger IT department: 2020 - 31%, 2019 - 27%
- Security is a distinct department, with its own staff, but it operates separately from the IT department: 2020 - 24%, 2019 - 20%
- We have one or two security people in IT, but they don't operate as a separate department: 2020 - 10%, 2019 - 13%
- We have full-time IT people but don’t have any people who are dedicated to security full-time: 2020 - 2%, 2019 - 6%
- We don't have any full-time IT or security staff: 2020 - 20%, 2019 - 24%
- Don't know: 2020 - 2%, 2019 - 3%

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019
## Relationship to IT Security

Which statement best describes your personal relationship to IT security in your organization?

<table>
<thead>
<tr>
<th>Statement</th>
<th>2020</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>I am the leader/CISO of the cybersecurity department</td>
<td>20%</td>
<td>18%</td>
</tr>
<tr>
<td>I am an admin/staff member in the cybersecurity department</td>
<td>16%</td>
<td>12%</td>
</tr>
<tr>
<td>I am a full-time cybersecurity professional who works in the general IT</td>
<td>5%</td>
<td>7%</td>
</tr>
<tr>
<td>department</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I am the leader/CIO of an IT department that has a distinct cybersecurity</td>
<td>8%</td>
<td>7%</td>
</tr>
<tr>
<td>department</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I am the leader/CIO of an IT department that has one or two security</td>
<td>9%</td>
<td>10%</td>
</tr>
<tr>
<td>pros but no separate department</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I am a staffer in an IT department that has a distinct cybersecurity</td>
<td>16%</td>
<td>15%</td>
</tr>
<tr>
<td>department</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I am a staffer in an IT department that has one or two security pros but</td>
<td>4%</td>
<td>8%</td>
</tr>
<tr>
<td>no separate department</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I am a manager or staffer in an IT department that has three or more</td>
<td>14%</td>
<td>12%</td>
</tr>
<tr>
<td>people but no full-time security pros</td>
<td></td>
<td></td>
</tr>
<tr>
<td>My organization only has one or two IT people, and I/we do both IT and</td>
<td>8%</td>
<td>4%</td>
</tr>
<tr>
<td>security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>My organization does not have any IT or security staff</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>Don't know</td>
<td>7%</td>
<td>4%</td>
</tr>
</tbody>
</table>

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?

- 500 or more: 8%
- 100 to 499: 14%
- 50 to 99: 17%
- 25 to 49: 10%
- 10 to 24: 9%
- 5 to 9: 4%
- 1 to 4: 5%
- We don't have any full-time IT people: 26%
- Don't Know: 4%

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals, March 2020
Figure 15

Cybersecurity Staff
In total, how many information security people does your organization employ?

- 100 or more: 6%
- 50 to 99: 7%
- 25 to 49: 12%
- 10 to 24: 22%
- 5 to 9: 10%
- We don't have any full-time information security people: 5%
- 1 to 2: 5%
- Don't Know: 23%

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals, March 2020
Figure 16

Annual IT Budget
What is your annual IT budget?

- 20%: $25 million or more
- 12%: $5 million to $24.9 million
- 15%: $1 million to $4.9 million
- 11%: $250,000 to $999,999
- 7%: $50,000 to $249,999
- 13%: Under $50,000
- 22%: 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?

<table>
<thead>
<tr>
<th>Data Center Type</th>
<th>2020</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud/premises mix</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT operations center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple data centers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A single, centralized data center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network operations center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security operations center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud only environment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019
Figure 18

Detecting Security Issues
When a suspected IT security issue or compromise occurs, which team is most likely to initially detect and flag it?

- The security team: 36%
- General IT: 12%
- It varies - sometimes it's the IT team, sometimes the security team, and other times an outside source: 8%
- End user/customer/outside source: 12%
- It's about even - sometimes the IT and team and other times the security team: 12%
- Don't know: 2%

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals, March 2020
Figure 19

Current IT Department Staffing
Which statement best describes the current staffing situation in your general IT department?

- 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

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019
Figure 20

Current Cybersecurity Department Staffing
Which statement best describes the current staffing situation in your cybersecurity department or team?

- 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 or potential breaches
- We are very short-staffed and frequently see security compromises because of it
- We have so few staff that we are completely underwater and our data is very vulnerable
- We don’t have any cybersecurity staff
- Don’t know

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019
Figure 21

Outsourced IT Functions
Which IT functions do you outsource?

<table>
<thead>
<tr>
<th>IT Functions</th>
<th>Currently Outsource</th>
<th>Plan to Outsource in the Next 12 Months</th>
<th>Do Not Outsource nor Plan to Outsource</th>
<th>Don’t Know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application development</td>
<td>18%</td>
<td>18%</td>
<td>58%</td>
<td>7%</td>
</tr>
<tr>
<td>Data storage/archival</td>
<td>17%</td>
<td>19%</td>
<td>60%</td>
<td>5%</td>
</tr>
<tr>
<td>Endpoint device management</td>
<td>17%</td>
<td>11%</td>
<td>62%</td>
<td>10%</td>
</tr>
<tr>
<td>Help desk/end user services</td>
<td>18%</td>
<td>13%</td>
<td>64%</td>
<td>4%</td>
</tr>
<tr>
<td>IT/systems operations</td>
<td>11%</td>
<td>8%</td>
<td>74%</td>
<td>7%</td>
</tr>
<tr>
<td>Network operations</td>
<td>10%</td>
<td>8%</td>
<td>76%</td>
<td>6%</td>
</tr>
<tr>
<td>Security operations</td>
<td>17%</td>
<td>10%</td>
<td>68%</td>
<td>6%</td>
</tr>
<tr>
<td>Web servers/services</td>
<td>36%</td>
<td>12%</td>
<td>48%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals, March 2020
Figure 22

Ensuring Proper Controls with Network Service Providers

Who in your organization works with network service providers to ensure proper controls and alerts regarding security?

- The IT/network operations team: 45% in 2020, 47% in 2019
- The security team: 25% in 2020, 30% in 2019
- Both teams communicate regularly with our service providers: 25% in 2020, 6% in 2019
- Don't know: 5% in 2020, 17% in 2019

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019
**Figure 23**

**Ensuring Proper Controls with Cloud Service Providers**
Who in your organization works with cloud service providers (IaaS) to ensure proper controls and alerts regarding security?

- The IT/network operations team: 42% (2020), 39% (2019)
- The security team: 28% (2020), 35% (2019)
- Both teams communicate regularly with our service providers: 25% (2020), 17% (2019)
- Don't know: 5% (2020), 9% (2019)

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

- The IT/applications team: 38% (2020) vs. 37% (2019)
- The security team: 32% (2020) vs. 37% (2019)
- Both teams communicate regularly with our service providers: 21% (2020) vs. 15% (2019)
- Don't know: 9% (2020) vs. 11% (2019)

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals in March 2020 and March 2019
Which of the following best describes your job title?

- Director/manager IT or cybersecurity: 27%
- IT or cybersecurity staff: 15%
- CIO/CTO: 11%
- CEO/president: 11%
- Consultant: 10%
- Vice president IT or security: 8%
- Network/system administrator: 7%
- CSO: 4%
- CFO: 3%
- Vice president, non-IT: 2%
- Other: 1%

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals, March 2020
Figure 26

Respondent Company Size
How many employees work for your company or organization?

- 33% Fewer than 100
- 27% 100 to 999
- 25% 1,000 to 9,999
- 15% 10,000 or more

Data: InformationWeek and Dark Reading survey of 115 cybersecurity and technology professionals, March 2020
**Figure 27**

**Respondent Industry**

What is your organization's primary industry?

- Healthcare/medical: 17%
- Consulting and business services: 16%
- Financial services/banking/securities and investments: 10%
- IT vendor, tech manufacturing: 10%
- Government/military (federal, state or local): 8%
- Education: 7%
- Manufacturing/industrial (non-computer): 5%
- Media/entertainment: 3%
- Nonprofit: 3%
- Construction/engineering: 2%
- Distributor: 2%
- Insurance/HMOs: 2%
- Retail/e-commerce: 2%
- Other: 13%

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