Your enterprise’s cyber risk may depend upon the relationship between the IT team and the security team. Here’s some insight on what’s working – and what isn’t – in the data center.
The State of IT Operations and Cybersecurity Operations

CONTENTS

Table of contents
3 About the Author
4 Executive Summary
6 Research Synopsis
7 Security Operations and IT Operations: Friends or Foes?
12 Why Can't We Just Get Along?
19 Conclusion
20 Appendix

Figures
Figure 1: Primary Responsibility
Figure 2: Outsourced IT Functions
Figure 3: Ensuring Proper Controls with Cloud Service Providers
Figure 4: Ensuring Proper Controls with Application Service Providers
Figure 5: Ensuring Proper Controls with Network Service Providers
Figure 6: Detecting Security Issues
Figure 7: Fixing Security Issues
Figure 8: Relationship Between IT and Security
Figure 9: Status of Relationship Between IT and Security Teams
Figure 10: Perception of Security Team
Figure 11: Security Staff
Figure 12: Managing Cybersecurity
Figure 13: IT Department Size
Figure 14: Current IT Department Staffing
Figure 15: Current Cybersecurity Department Staffing
Figure 16: Organization's Attitude Toward Cybersecurity
Figure 17: Relationship to IT Security
Figure 18: Annual IT Budget
Figure 19: Percentage of IT Budget Dedicated to Cybersecurity
Figure 20: Importance of Digital Innovation
Figure 21: Importance of Cybersecurity
Figure 22: Organization's Data Centers
Figure 23: Final Decision Maker
Figure 24: Job Title
Figure 25: Company Size
Figure 26: Industry
Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He specializes in writing on information security and data privacy topics. He was most recently a Senior Editor at Computerworld. He is a regular contributor to Dark Reading, CSO Online, Tech Beacon, and several other publications.
When it comes to mitigating the danger of online attacks, many enterprises have two teams that play a critical role: the cybersecurity team and the general IT team. Each team has its own responsibilities – though they often overlap – and each team has its own list of priorities. The key to keeping enterprise data safe, experts say, is to get the two teams communicating and working closely together.

How strong is the relationship between IT operations and security operations? For the second straight year, Dark Reading’s research team polled professionals on both sides of the equation to find out. The Dark Reading 2019 State of IT Operations and Security Operations survey polled 115 IT and cybersecurity professionals on how critical cybersecurity functions are conducted and managed in their organizations. The survey examined the communications and the division of labor between IT and security groups, as well as their respective roles in mitigating enterprise cyber risk. Participants included CIOs, CISOs, CTOs, security management and staff, and IT management and staff from organizations of all sizes.

Compared to last year, the survey results indicate that IT operations and security teams are improving their interaction and their collaboration on risk mitigation and business enablement. Security experts view such collaboration as fundamental to an organization’s ability to defend itself against modern threats. The need for compliance with regulatory requirements for security and privacy may be helping to drive the partnership.

At the same time, security continues to take a back seat to other IT and business priorities in many organizations, and many data centers continue to struggle with communications between IT operations and security operations.
The 2019 Dark Reading State of IT Operations and Security Operations survey uncovered some important developments in the way enterprises are managing security in the data center – and in the boardroom. Here are some key takeaways:

- 57% of respondents said IT and security staff communicate well, up from 47% last year.
- 20% of organizations involve the security team at the start of every major IT project.
- 69% of respondents say that the security team holds primary responsibility for compliance and privacy; this figure rose significantly – more than 12% – from our 2018 survey.
- 90% of organizations expect the security team to take charge of developing and setting security policy.
- 80% said the IT operations team is primarily responsible for patch management.
- 20% of organizations have a distinct security department that operates separately from the IT team.
- 18% of organizations have a fully-staffed security function.
- 37% said the security operations team is most likely to be the first to detect and alert others about security incidents in the organization.
Survey Name 2019 State of IT Operations and Security Operations

Survey Date March 2019

Primary Region North America

Number of Respondents 115 IT and cybersecurity professionals
The margin of error for the total respondent base (N=115) is +/- 9 percentage points.

Purpose 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 staff/functions and cybersecurity staff/functions.

Methodology The survey queried decision-makers with IT or IT security job titles at primarily North American organizations. It asked them about their organizations’ information security operations, as well as the roles and communication between general IT professionals and cybersecurity professionals. 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 UBM’s qualified database; UBM is the parent company of Dark Reading and Interop. UBM was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.
Both IT operations and security operations play a key role in enterprise data security. Security operations is responsible for developing and setting policies, as well as for essential functions such as threat monitoring, detection, and response. Yet it is the IT operations team that maintains the systems and networks being protected – they are usually the ones who configure the routers, install patches, and ensure that logs are collecting security-related data. And while the security team is almost entirely focused on data safety and integrity, the IT team has multiple, sometimes conflicting priorities, including system availability and the enablement of business applications.

“Enterprises can’t be successful with threat prevention and fast remediation unless both teams are working well together,” says Joseph Blankenship, an analyst with Forrester Research. Security operations is often dependent on IT operations to take critical actions involving endpoints, networking, and applications, he notes. “If IT and security aren’t getting along, then the process breaks down.”

Dark Reading’s survey shows that at a high percentage of organizations, the IT operations team is often responsible for functions that are fundamental to managing cyber risk. For example, 80% of respondents reported that in their organizations, the general IT team is primarily responsible for security patch management. Yet experts say the patching function is easily one of the most important security functions. Many major breaches — including one at Equifax in 2017 that exposed sensitive personal information on over 120 million people — have resulted from a failure to apply security patches in a timely fashion. Survey respondents also said the IT operations team is usually responsible for many other tasks related to security, including storage and archiving (91%); router configuration (85%); end user identity management and provisioning (77%); and firewall configuration (60%).

At more than 50% of organizations, the general IT staff is also primarily responsible for three other disciplines that are crucial to security: supply chain security, business continuity, and disaster recovery (Figure 1).
A lapse of vigilance by IT operations in any of these areas can have serious security consequences, security experts say. Last year’s destructive VPNFilter attacks, which targeted hundreds of thousands of small and home office users, took advantage of vulnerabilities in routers and network attached storage devices that generally fall into the IT operations realm.

Meanwhile, the role of the security operations organization itself is changing. Once focused entirely on defensive processes and threat response, security operations teams today are becoming more involved in proactive activities such as threat hunting, vulnerability research, and penetration testing. Security operations’ role has evolved toward gathering potential security incident information, analyzing threat intelligence, and plugging this telemetry into an incident response workflow, says Daniel Kennedy, an analyst at 451 Research.

The tools available to security operations teams have become more sophisticated as well, Kennedy observes. “Where IDS [intrusion detection systems] and sometimes SIEM [security information and event

---

**Primary Responsibility**

Which team is primarily responsible for the following functions?

<table>
<thead>
<tr>
<th>Function</th>
<th>2019 IT Security Team</th>
<th>2018 IT Security Team</th>
<th>2019 General IT Team</th>
<th>2018 General IT Team</th>
<th>2019 Don’t know</th>
<th>2018 Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing/writing enterprise security policy</td>
<td>90%</td>
<td>87%</td>
<td>6%</td>
<td>11%</td>
<td>4%</td>
<td>2%</td>
</tr>
<tr>
<td>Security threat analysis</td>
<td>89%</td>
<td>91%</td>
<td>4%</td>
<td>6%</td>
<td>7%</td>
<td>3%</td>
</tr>
<tr>
<td>Security incident response</td>
<td>85%</td>
<td>83%</td>
<td>9%</td>
<td>14%</td>
<td>6%</td>
<td>3%</td>
</tr>
<tr>
<td>Security threat detection</td>
<td>80%</td>
<td>84%</td>
<td>13%</td>
<td>11%</td>
<td>7%</td>
<td>5%</td>
</tr>
<tr>
<td>Risk measurement/reporting</td>
<td>75%</td>
<td>71%</td>
<td>21%</td>
<td>27%</td>
<td>4%</td>
<td>2%</td>
</tr>
<tr>
<td>Compliance</td>
<td>69%</td>
<td>57%</td>
<td>21%</td>
<td>41%</td>
<td>10%</td>
<td>2%</td>
</tr>
<tr>
<td>Privacy</td>
<td>69%</td>
<td>52%</td>
<td>19%</td>
<td>42%</td>
<td>12%</td>
<td>6%</td>
</tr>
<tr>
<td>Endpoint security</td>
<td>59%</td>
<td>46%</td>
<td>35%</td>
<td>51%</td>
<td>6%</td>
<td>3%</td>
</tr>
<tr>
<td>Cloud security</td>
<td>48%</td>
<td>45%</td>
<td>41%</td>
<td>42%</td>
<td>11%</td>
<td>13%</td>
</tr>
<tr>
<td>Application security</td>
<td>46%</td>
<td>33%</td>
<td>46%</td>
<td>64%</td>
<td>8%</td>
<td>3%</td>
</tr>
<tr>
<td>Disaster recovery/business continuity</td>
<td>46%</td>
<td>27%</td>
<td>52%</td>
<td>70%</td>
<td>2%</td>
<td>3%</td>
</tr>
<tr>
<td>Network security</td>
<td>44%</td>
<td>43%</td>
<td>48%</td>
<td>56%</td>
<td>7%</td>
<td>1%</td>
</tr>
<tr>
<td>Mobile device security</td>
<td>39%</td>
<td>40%</td>
<td>48%</td>
<td>56%</td>
<td>13%</td>
<td>4%</td>
</tr>
<tr>
<td>Firewall configuration</td>
<td>37%</td>
<td>29%</td>
<td>60%</td>
<td>70%</td>
<td>4%</td>
<td>1%</td>
</tr>
<tr>
<td>Supplier/supply chain security</td>
<td>25%</td>
<td>39%</td>
<td>54%</td>
<td>48%</td>
<td>21%</td>
<td>13%</td>
</tr>
<tr>
<td>End user identity/provisioning</td>
<td>19%</td>
<td>33%</td>
<td>77%</td>
<td>65%</td>
<td>4%</td>
<td>2%</td>
</tr>
<tr>
<td>Router configuration</td>
<td>14%</td>
<td>9%</td>
<td>85%</td>
<td>91%</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Patch management</td>
<td>13%</td>
<td>14%</td>
<td>80%</td>
<td>83%</td>
<td>7%</td>
<td>3%</td>
</tr>
<tr>
<td>Storage/archiving</td>
<td>4%</td>
<td>3%</td>
<td>91%</td>
<td>91%</td>
<td>6%</td>
<td>6%</td>
</tr>
</tbody>
</table>

Base: Those with separate IT and security teams

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals
management platforms] once dominated implementations, security operations folks now have more productized automation tools, playbooks, behavioral analytics, [and] better threat intelligence integration,” he says. Security teams also have a wider range of incident response workflow tools, he adds.

Dark Reading’s survey data illustrates this movement to a more proactive approach. At 90% of surveyed companies, it is the security team that is primarily responsible for developing and setting enterprise-wide security policies. The security team also usually owns responsibility for threat analysis (89%); incident response (85%); and threat detection (80%) (Figure 1).

Compliance and privacy are also becoming increasingly entrusted to the security team. Sixty-nine percent of survey respondents identified compliance as the primary responsibility of the security team and an identical proportion said the same of privacy. The numbers are substantially higher than those of our 2018 survey, in which 57% and 52%, respectively, gave the security team responsibility for compliance and privacy. This rapid rise suggests that the security team increasingly is being given the burden of emerging privacy regulations, such as the European Union’s General Data Protection Regulation (GDPR), which went into effect in 2018 (Figure 1).

In some cases, security functions fall to neither IT operations nor security, but are outsourced to third parties. Nearly one-third of Dark Reading survey respondents (32%) outsource application development to a third party; another 9% plan to do so over the next 12 months. Twenty-eight percent have outsourced Web servers and services; 23% outsource help desk services; and 22% outsource data storage and archiving (Figure 2).

The rapid move toward cloud services also is causing shifts in the roles of IT operations...
and security. At nearly four in 10 firms (39%), the IT or network operations team has primary responsibility for working with cloud service providers to ensure proper security controls and alerts. In another 35% of enterprises, both the IT and security teams regularly work with cloud providers on security matters (Figure 3). When asked which team ensures proper controls over hosted application services and software-as-a-service (SaaS) providers, 37% pointed to the IT team, and an identical proportion said both teams were responsible (Figure 4). When it comes to managing network services and providers, 47% of organizations said the IT and network operations teams are responsible for managing security issues; in another 30% of organizations, both the security and IT teams work on network services security (Figure 5).

The movement toward cloud services further complicates the roles of the IT operations and security teams. “The key issue with cloud adoption is the completeness of visibility,” says Kennedy. IT and security teams have struggled for years to aggregate and integrate all of the security telemetry

![Figure 3](image1.png)

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

- The IT/network operations team 39%
- The security team 17%
- Both teams communicate regularly with our service providers 35%
- Don’t know 9%

![Figure 4](image2.png)

**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 37%
- The security team 15%
- Both teams communicate regularly with our service providers 37%
- Don’t know 11%

Note: Not asked in 2018
Data: Dark Reading and Interop survey of 115 cybersecurity and technology professionals, March 2019
from around the enterprise, he observes. Now, these teams also have to integrate log data collection and analysis from their cloud footprint as well.

Enterprise digital transformation projects are also adding to the complexity of the relationship between IT operations and security. “As managed services become a more prolific offering, there are decisions on what an on-site SOC [security operations center] will do and what the MSSP [managed security services provider] or similar service can be depended on to do to offload some of the stress,” Kennedy states.

Both IT and security teams play a critical role in breach detection. In our survey, 37% of respondents said the security team would be the most likely to be the first to detect a potential data compromise; 29% said the IT operations team would be the most likely to be the first point of detection. Twenty-nine percent of respondents said the IT operations team and security operations are equally likely to be the first to spot and flag a potential breach (Figure 6).

What about fixing security problems
after they are detected? Forty percent of respondents said the IT operations team has primary responsibility for breach/comromise mitigation and remediation; 29% said that responsibility falls to the security team. Significantly, some 27% of enterprises—more than one in four—said the security and IT operations teams share the responsibility for mitigation and remediation evenly. That figure has grown more than 10% in the last year, which suggests that more enterprises are now recognizing the need for better collaboration between IT and security operations (Figure 7).

Why Can’t We Just Get Along?
Security and IT operations teams have often been at odds with each other over the years, usually because their priorities are at odds as well. As stewards of the organization’s computing, storage, and network infrastructure, the IT operations team is all about uptime, uninterrupted operations, and business enablement, experts say. The security team’s focus on vulnerability management, compliance requirements, policy, and risk reduction can at times be contrary to IT’s goals around speed and ease of use.

It is not unusual for IT operations staff and leaders to view security requirements as impeding their ability to fulfill business requirements at speed and scale, security experts say. The conflicts sometimes

---

**Figure 7**

**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>Year</th>
<th>General IT</th>
<th>The security team</th>
<th>It’s about even—half the time it’s the IT team, the other half it’s the security team</th>
<th>Don’t know</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>46%</td>
<td>38%</td>
<td>16%</td>
<td>4%</td>
</tr>
<tr>
<td>2019</td>
<td>40%</td>
<td>29%</td>
<td>27%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals.
jeopardize security.

“A strong security team will be handicapped by IT operations that can’t keep the systems configured in a consistent way, that make changes without notice, and that generally create a lot of noise,” says Chris Crowley, independent consultant at Montance, LLC. At the same time, “a security team that doesn’t understand that IT systems are there to be operated with live data at risk isn’t going to keep pace with the IT team,” he says.

Endpoint security is one area where the need for collaboration is critical — but is also one of the disciplines where the friction between the two sides is most evident. Patch management, for instance, is essential to the security of enterprises of all sizes, notes Avivah Litan, an analyst with Gartner Inc. In fact, research has shown that some 80% of attacks against endpoint systems leverage the same top 10 or 20 patchable vulnerabilities, she says. Organizations can prevent a majority of attacks by patching those vulnerabilities. “It is the SOC that knows what needs to be patched. But it is the IT operations team that does the patching,” she notes. “This is where the conflict happens.”

As previously noted, IT operations is responsible for patch management at 80% of organizations in our survey. But the IT operations team is often reluctant to deploy patches that it suspects might cause operational disruptions or downtime. This difference of opinion with security operations can cause a tug-of-war, Litan states. In a March 2019 survey conducted by security vendor Tanium, 81% of the respondents admitted to delaying critical security updates on at least one occasion because of such concerns—52% admitted to doing it more than once.

Endpoint systems are not the only flashpoint. The question of network segmentation may also cause disagreements between IT operations and security. While security teams often want to implement strict device isolation and micro-segmentation, IT operations teams tend to stick with overly permissive architectures in order to speed network accessibility, the Tanium survey found.

Our Dark Reading survey suggests that the relationship between IT operations and security is improving on some fronts. When asked to describe the relationship between security and IT operations teams, more respondents this year (57%) said the teams communicate well and are aware of what the other is doing, compared to 47% last year. Similarly, only 21% of survey respondents this year identified incidents where a miscommunication between the two sides had resulted in security problems, compared to 26% last year (Figure 8).

Members of IT and security operations teams also appear to have better regard for each other than they did a year ago. Nearly half of respondents (47%) in our survey this year said IT operations and security operations are working well together and described the relationship between the two sides as improving. Last year only 30% felt that way. Fewer respondents this year (25%) said the relationship needs work; down from 38% in 2018 (Figure 9).

Security leaders have long argued for a place at the table with other enterprise leaders when launching major business and IT initiatives. Security professionals believe such early involvement helps bake security into enterprise products and services during the development phase, rather than
bolting security on at the end, when changes are much more complex and costly to make. Dark Reading’s survey suggests that enterprises are making some progress on that front. Twenty-percent of organizations—up from 15% last year—now include members of the security team at the beginning of every new project. The security team’s views are considered critical, according to those respondents. At another 24% of companies, the security team is invited to participate at the launch of most new projects. Combined, these numbers indicate that security is called in to most or all major business projects in 44% of enterprises (Figure 10).

While these numbers are encouraging, they also have a flip side—the 56% of enterprises that don’t, or only barely, consult with security when launching a new project. This lack of oversight could create major security risks for organizations that are implementing major new IT-related initiatives, such as adopting cloud services or rolling out new digital transformation initiatives, security experts say.

Staffing is another major issue that may cause issues for IT operations and security groups. Twenty-one percent of organizations in the Dark Reading survey have no full-time security staff; another 22% have only one or two security people. Eleven percent of organizations have more than 100 security

<table>
<thead>
<tr>
<th>Relationship Between IT and Security</th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>The two staffs communicate well and are well aware of what each other are doing</td>
<td>6%</td>
<td>8%</td>
</tr>
<tr>
<td>On a few occasions, the two staffs have miscommunicated, leading to continuity or security problems</td>
<td>8%</td>
<td>7%</td>
</tr>
<tr>
<td>Miscommunication between the two groups routinely causes problems for both</td>
<td>12%</td>
<td>21%</td>
</tr>
<tr>
<td>The two staffs barely communicate at all</td>
<td>26%</td>
<td>47%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>12%</td>
<td>7%</td>
</tr>
</tbody>
</table>

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals.
staffers; 10% have between 10 and 24 (Figure 11). Twenty percent of companies have independent security teams that operate separately from the IT group; at 27% of firms, the security team operates on its own, as part of a broader IT group (Figure 12).

Not surprisingly, general IT teams are typically much larger. Some 20% of Dark Reading survey respondents say they employ more than 100 full time IT staffers; another 12% have between 50 and 99 (Figure 13).

Despite their size differences, IT departments and security teams both feel they are short-staffed. In our survey 40% of general IT respondents said they do not have enough people (Figure 14). Thirty-seven percent of security professionals say their teams are short on staff and could use extra help from an outsourcer or service provider (Figure 15). Twenty-one percent—more than one in five—of the respondents described their IT department as so short-staffed that they are concerned about their ability to properly protect against threats. Fourteen percent expressed the same concern about the short-staffing of their security teams.

The skills shortage is particularly acute in security, says Kennedy of 451 Research. “[Security] people move on once they gain experience,” he says. This “brain drain” means that many organizations are losing
the individuals who know how to operate the security tools that are in place. Many small and medium-sized businesses are also running security technology that requires some level of monitoring, but they do not have SOCs or security operations teams to do the work, he notes.

A lack of security visibility may also make it difficult for IT operations and security operations to work together. When security and IT operation teams work from different data sets, they may arrive at different conclusions about the scope of a threat and how to mitigate it, security experts say. Matt Hastings, director of product management of risk and security at Tanium, states that infected endpoints can escalate to enterprise-wide security incidents in a matter of minutes. Security teams and IT operations teams need complete, up-to-date, and accurate visibility across the environment in order to properly detect, scope, investigate, and quantify cyber risk, he says.

Dark Reading’s survey indicates that professionals in both security and IT operations are frustrated by issues of communication and collaboration between the two sides. When IT

---

**Figure 10**

**Perception of Security Team**

How is the information security team perceived in your organization?

- They are brought in at the beginning of most important projects, and they have a strong voice: 24% (2018), 28% (2019)
- They are consulted sometimes, and they are usually heard if they have a legitimate concern: 13% (2018), 12% (2019)
- They are at the table at the beginning of every new project, and their views are always considered critical: 4% (2018), 4% (2019)
- They are generally not part of IT project planning, and their concerns are often seen as an annoyance: 20% (2018), 24% (2019)
- They are consulted on few projects, and they are heard only when there is a critical threat or breach: 14% (2018), 9% (2019)
- We don’t have an information security team or person: 27% (2018), 20% (2019)
- Don’t know: 3% (2018), 3% (2019)

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals.

---
and security staffs were asked to identify the one problem they most frequently encounter when working together, a high percentage of the open-ended responses cited lack of communication. One respondent described the security team as “operating in a vacuum” and making unexpected changes that cause issues for end users. Another complained about security having “an absolute mandate,” similar to the zero-tolerance policy in schools. “There’s no room to use a little common sense and perhaps back off applying the security policy completely,” the respondent said.

When asked what they would like to see from their security counterparts, IT operations professionals cited better communications, adopting best practices, and more training and education opportunities for IT staff and employees. “Be more industry knowledgeable and less theoretical,” one respondent advised. The security team, meanwhile, wants IT staffers to engage more actively in maintaining enterprise security. “Understand that the security teams are not the bad guys but are simply following the guidelines put into place by the higher ups,” one security professional wrote.
Ultimately, though, it seems likely that security teams will struggle against IT and business decision makers who are more concerned about speed and innovation than about security. More than four in ten respondents (42%) said their enterprises would be willing to compromise on security in order to take advantage of a new technology that might positively impact their business. That figure has grown 3% since 2018 (39%). Seventeen percent—compared to last year’s 15%—described innovation and speed as being more important than security. Barely more than one-third of organizations (36%) consider security to be important enough to merit a cautious approach to new technologies and innovation (Figure 16).

What measures can IT operations and security teams take to enable better collaboration? Tanium’s Hastings says establishing mutual respect between the two teams is key to an effective partnership. Breaking down the silos may also help. “Too often, these teams work with disparate tools with outdated information, which can result in incorrect and conflicting information — and cause contention over the current state of the environment,” he says.

Rules of engagement that clearly delineate the responsibilities of the IT and security groups can help foster better collaboration between the teams, experts say. So, too, can technology integration, Forrester’s Blankenship says. “Lots of security action items get handed off via email or Slack, instead of a ticketing system or system of record,” he observes. Better operational technology may improve the handoff between IT and security teams, he says.

IT operations also needs context about why security is asking it to take an action, Blankenship advises. Security operations should include as much information about the “why” of a request as possible. “Integrating the investigative tools used by the SOC with the ticketing system used by IT [operations] can help with the handoff and provide needed context about the urgency of requests,” he says.
Gartner’s Litan agrees that enterprises should take advantage of technologies that might help bridge gaps between IT operations and security. For example, there are now tools available that help organizations identify systems that are vulnerable to a specific threat and prioritize the manner in which they are patched. Using a vendor that facilitates communication between IT and security groups around patch management priorities can reduce conflict, she notes. “I would start with the endpoint,” Litan says.

Entities that do not have the resources to build their separate security operations capabilities may have to explore hybrid roles, where security responsibilities are delegated to network operations or IT operations teams, Kennedy says. “I personally don’t think it’s ideal, but available resources and prioritization differ from organization to organization.”

**Conclusion**

Security and IT operations teams are getting better at collaborating with each other. But communications gaps, staffing shortages, and poorly integrated technologies continue to undermine this progress. To mitigate risk in today’s fast-changing threat and compliance environment, security and IT groups need to find ways to break down silos of operations, divide the workload more clearly, and assume shared responsibility for enterprise security.
Figure 14

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

- 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 fully staffed and don’t need any help
- 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

2019:
- 40% We could use a few more people and/or a little more help from an outsourcer/service provider
- 5% We are pretty short-staffed, and it sometimes creates problems in getting things done
- 19% We are fully staffed and don’t need any help
- 21% We are very short-staffed and frequently fall short of our goals because of it
- 8% We have so few staff that we are completely underwater
- 4% We don’t have any IT staff
- 3% Don’t know

2018:
- 5% We could use a few more people and/or a little more help from an outsourcer/service provider
- 1% We are pretty short-staffed, and it sometimes creates problems in getting things done
- 24% We are fully staffed and don’t need any help
- 21% We are very short-staffed and frequently fall short of our goals because of it
- 8% We have so few staff that we are completely underwater
- 4% We don’t have any IT staff
- 3% Don’t know

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals
Figure 15

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

- We could use a few more people and/or a little more help from an outsourcer/service provider
- We are fully staffed and don't need any help
- 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 IT security staff
- Don't know

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals
Figure 16

Organization's Attitude Toward Cybersecurity
Which statement best describes the attitude toward cybersecurity in your organization?

- Security is important, but we are willing to take some risks if we find a new technology that could positively impact our business (42% in 2019, 39% in 2018)
- Security is paramount and we take a cautious approach to IT innovation (36% in 2019, 15% in 2018)
- Innovation and speed are generally more important than security (17% in 2019, 4% in 2018)
- Security? What's that? (3% in 2019, 3% in 2018)
- Don't know (1% in 2019, 4% in 2018)

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals
Figure 17

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

2018

- I am the leader/CISO of the cybersecurity department: 18%
- I am a staffer in an IT department that has a distinct cybersecurity department: 9%
- My organization only has one or two IT people, and I/we do both IT and security: 15%
- I am an admin/staff member in the cybersecurity department: 6%
- I am the leader/CIO of an IT department that has one or two security pros but no separate department: 12%
- I am a staffer in an IT department that has one or two security pros but no separate department: 13%
- I am a full-time cybersecurity professional who works in the general IT department: 15%
- I am the leader/CIO of an IT department that has a distinct cybersecurity department: 10%
- I am a manager or staffer in an IT department that has three or more people but no full-time security pros: 8%
- Don't know: 1%

2019

- I am the leader/CISO of the cybersecurity department: 15%
- I am a staffer in an IT department that has a distinct cybersecurity department: 15%
- My organization only has one or two IT people, and I/we do both IT and security: 15%
- I am an admin/staff member in the cybersecurity department: 13%
- I am the leader/CIO of an IT department that has one or two security pros but no separate department: 8%
- I am a staffer in an IT department that has one or two security pros but no separate department: 8%
- I am a full-time cybersecurity professional who works in the general IT department: 7%
- I am the leader/CIO of an IT department that has a distinct cybersecurity department: 6%
- I am a manager or staffer in an IT department that has three or more people but no full-time security pros: 6%
- Don't know: 4%

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals
Figure 18

Annual IT Budget

What is your annual IT budget?

- $25 million or more: 13%
- $1 million to $24 million: 22%
- $50,000 to $999,999: 25%
- Under $50,000: 29%
- $50,000 to $999,999: 17%
- Don’t know: 12%

2018:
- $25 million or more: 13%
- $1 million to $24 million: 16%
- $50,000 to $999,999: 24%
- Under $50,000: 24%
- $50,000 to $999,999: 25%
- Don’t know: 17%

2019:
- $25 million or more: 12%
- $1 million to $24 million: 29%
- $50,000 to $999,999: 34%
- Under $50,000: 8%
- $50,000 to $999,999: 17%
- Don’t know: 16%

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals.
Figure 19

**Percentage of IT Budget Dedicated to Cybersecurity**

What percentage of your annual IT budget is devoted to cybersecurity?

![Pie charts showing percentage of IT budget dedicated to cybersecurity for 2018 and 2019.](image)

- **2018**
  - More than 50%
  - 25% to 49%
  - 15% to 24%
  - 10% to 14%
  - 5% to 9%
  - 3% to 4%
  - Less than 3%
  - Don't know

- **2019**
  - More than 50%
  - 25% to 49%
  - 15% to 24%
  - 10% to 14%
  - 5% to 9%
  - 3% to 4%
  - Less than 3%
  - Don't know

*Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals*
Figure 20

Importance of Digital Innovation
How important is IT and digital innovation to your organization and its top management?

<table>
<thead>
<tr>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolutely critical</td>
<td>53%</td>
</tr>
<tr>
<td>Important</td>
<td>25%</td>
</tr>
<tr>
<td>Neutral</td>
<td>10%</td>
</tr>
<tr>
<td>Not very important</td>
<td>3%</td>
</tr>
<tr>
<td>Not at all important</td>
<td>8%</td>
</tr>
<tr>
<td>Don't know</td>
<td>1%</td>
</tr>
</tbody>
</table>

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals
Figure 21

Importance of Cybersecurity
How important is cybersecurity to your organization and its top management?

- Absolutely critical
- Important
- Neutral
- Not very important
- Not at all important
- Don't know

2019:
- 52% Absolutely critical
- 30% Important
- 8% Neutral
- 8% Not very important
- 2% Not at all important
- 2% Don't know

2018:
- 52% Absolutely critical
- 31% Important
- 5% Neutral
- 10% Not very important
- 5% Not at all important
- 2% Don't know

Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals.
Figure 22

**Organization's Data Centers**
Which of these does your organization have?

<table>
<thead>
<tr>
<th>Data Center</th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple data centers</td>
<td>53%</td>
<td>54%</td>
</tr>
<tr>
<td>IT operations center</td>
<td>44%</td>
<td>37%</td>
</tr>
<tr>
<td>Network operations center</td>
<td>35%</td>
<td>43%</td>
</tr>
<tr>
<td>Security operations center</td>
<td>30%</td>
<td>28%</td>
</tr>
<tr>
<td>A single, centralized data center</td>
<td>29%</td>
<td>32%</td>
</tr>
</tbody>
</table>

Note: Multiple responses allowed
Data: Dark Reading and Interop survey of 120 (May 2018) and 115 (March 2019) cybersecurity and technology professionals
When the general IT team and the security team disagree on decisions or priorities, who generally makes the final call?

- The CIO: 30%
- The CISO or security leader: 26%
- A committee of IT and security leaders: 21%
- Other top executive: 12%
- Don't know: 11%

Note: Not asked in 2018.
Data: Dark Reading and Interop survey of 115 cybersecurity and technology professionals, March 2019.
**Figure 24**

**Respondent Job Title**

Which of the following best describes your job title?

- Director/manager IT: 18%
- Security staff: 17%
- IT staff: 12%
- Director/manager security: 10%
- CIO/CTO or other senior IT exec.: 9%
- CSO (chief security officer or chief privacy officer): 8%
- CEO/president/owner/partner or other senior corp. exec.: 7%
- Network/system administrator: 5%
- Consultant: 5%
- Vice president, IT or security: 4%
- Internal auditor: 3%
- Other: 2%

Data: Dark Reading and Interop survey of 115 cybersecurity and technology professionals, March 2019
Figure 25

**Respondent Company Size**

How many employees work for your company or organization?

- **10,000 or more**: 28%
- **1,000 to 9,999**: 26%
- **100 to 999**: 25%
- **Fewer than 100**: 21%

*Data: Dark Reading and Interop survey of 115 cybersecurity and technology professionals, March 2019*
## Respondent Industry
What is your organization’s primary industry?

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare/medical</td>
<td>11%</td>
</tr>
<tr>
<td>Education</td>
<td>11%</td>
</tr>
<tr>
<td>Financial services/banking/securities and investments</td>
<td>10%</td>
</tr>
<tr>
<td>Government/military (federal, state or local)</td>
<td>9%</td>
</tr>
<tr>
<td>IT vendor, tech manufacturing</td>
<td>8%</td>
</tr>
<tr>
<td>Insurance/HMOs</td>
<td>7%</td>
</tr>
<tr>
<td>Consulting and business services</td>
<td>5%</td>
</tr>
<tr>
<td>Logistics/transportation</td>
<td>4%</td>
</tr>
<tr>
<td>Manufacturing/industrial (non-computer)</td>
<td>4%</td>
</tr>
<tr>
<td>Biotech/biomedical/pharmaceutical</td>
<td>3%</td>
</tr>
<tr>
<td>Retail/e-commerce</td>
<td>3%</td>
</tr>
<tr>
<td>Construction/engineering/energy/utilities</td>
<td>3%</td>
</tr>
<tr>
<td>Consumer goods</td>
<td>2%</td>
</tr>
<tr>
<td>Distributor</td>
<td>2%</td>
</tr>
<tr>
<td>Telecommunications/ISPs</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>16%</td>
</tr>
</tbody>
</table>

Data: Dark Reading and Interop survey of 115 cybersecurity and technology professionals, March 2019