The State of Cybersecurity
Incident Response

Organizations are responding to new threats with new processes for detecting and mitigating them. Here's a look at how the discipline of incident response is evolving.
# Table of Contents

3  About the Author  
4  Executive Summary  
6  Research Synopsis  
7  The Evolution of Incident Response  
11  IR Capabilities Today: A Snapshot  
14  Tools, Training, and Other IR Obstacles  
18  Conclusion

# Figures

7  Figure 1: Number of Security Incidents in a Typical Month  
7  Figure 2: Percentage of Incidents with a Negative Effect  
8  Figure 3: Definition of Incident Response  
9  Figure 4: Common Types of Security Incidents  
10  Figure 5: Greatest Potential Threats to Sensitive Data  
11  Figure 6: Difficult Response Tasks  
12  Figure 7: Incident Response Statements  
13  Figure 8: Dedicated Incident Response Staff  
13  Figure 9: Security Operations Center  
14  Figure 10: Management’s View of Incident Response  
15  Figure 11: Building an Effective Incident Response Program  
17  Figure 12: Balance of Resources  
19  Figure 13: Sharing Information  
20  Figure 14: Respondent Job Title  
21  Figure 15: Respondent Company Size  
22  Figure 16: Respondent 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 Christian Science Monitor Passcode, Dark Reading, CSO Online, TechTarget, and several other publications.

Jai Vijayan
InformationWeek Reports
Organizations today face unprecedented risk of disruption and data exposure from a broad range of cyber threats. For many, the process of detecting and managing security compromises, also known as incident response (IR), has become as important as the process of perimeter system and data protection.

Dark Reading’s 2019 Incident Response Survey, which provides feedback from 150 IT and cybersecurity professionals, reflects a high level of concern about attacks targeting intellectual property, proprietary business information, and customer and employee data. Many of the respondents have implemented measures for responding to and mitigating data compromises, but critical gaps in certain incident response capabilities may be seriously limiting these efforts.

The survey results show that most organizations remain heavily committed to a prevention-first strategy while expanding their IR capabilities. Generally, businesses are still allocating more resources to perimeter defense than to IR, but they differ widely in the proportion of resources devoted to each.

Phishing, malware, and targeted attacks continue to be top security concerns — and the primary causes for security alerts and breaches across organizations. Last year, enterprises reported more data breaches — and spent more on recovering from them — than in almost any previous year. Even so, a high percentage of businesses in the Dark Reading survey appear to be confident about their ability to detect and respond to current cyber threats. The respondents also generally feel that their IR efforts are well supported by upper management.

However, the survey data also indicates that a disturbingly high number of organizations have not implemented IR measures. In some organizations, there is still a lack of management support for IR efforts; in other organizations, security teams are not using tools that many experts deem critical to effective threat detection, response, and mitigation.
The following are some key statistics from the survey:

• 78% of organizations have at least one staffer dedicated specifically to the task of incident response; 11% have more than 25.

• 31% of companies have a security operations center; 16% have outsourced the function.

• 74% say a suspected breach of intellectual property or proprietary business data would trigger their incident response initiatives.

• 5% of companies respond to 3,000 or more security “incidents” per month; 30% to between one and nine.

• 47% of respondents report that fewer than one in 20 of the incidents they investigate has a significant negative impact on the organization.

• 38% consider log analysis for anomalous activity to be the most difficult and time-consuming IR process.

• 56% of respondents say the biggest threat they face is phishing/social engineering attacks that drop malware or result in credential theft.

• 65% of respondents say their upper management recognizes the importance of the IR function to the overall security of enterprise data and business functionality.
Survey Name: Dark Reading 2019 Incident Response Survey

Survey Date: January 2019

Primary Region: North America

Number of Respondents: 150 IT and cybersecurity professionals at companies of all sizes. The margin of error for the total respondent base (N=150) is +/-7.9 percentage points.

Purpose: Dark Reading surveyed business technology and IT security professionals to discover issues and attitudes related to incident response practices and processes, the factors that are driving them, and the capabilities organizations have implemented to address security incidents.

Methodology: The survey queried decision-makers with cybersecurity or IT job titles at predominantly North American organizations. Questions centered on organizations’ strategies and tactics for responding to security incidents of varying levels of criticality, from simple malware infection to major data breaches. 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. UBM was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.
The Evolution of Incident Response

Incident response (IR) has become one of the fastest-growing disciplines in IT. One reason for this growth is the rapid evolution of cyber-attacks that penetrate enterprise defenses, thus triggering the detection of an “incident.” Phishing, malware, targeted attacks, and a range of other threats are all increasingly being categorized as incidents, putting a tremendous strain on enterprise IR processes. And those responsible for responding to security incidents are scrambling to keep up with what appears to be a nearly constant barrage of threat alerts and events.

Dark Reading’s 2019 Incident Response Survey shows that most IR teams are being forced to respond to a high number of security incidents. Five percent in our survey say they are responding to as many as 3,000 or more incidents each month, or about 100 per day. Nine percent are handling between 100 and 1,999 security incidents per month, and 34% are responding to between five and 99 incidents (Figure 1). At the lower end, a fortunate 25% of organizations are handling fewer than one security incident per month.

The numbers are important. Not every security alert that an IR team investigates turns out to be an actual breach. In fact, 47% of the respondents say that less than 5% of the incidents they investigate result in damage, downtime, financial losses, or other negative consequences (Figure 2).
Why are there so many “incidents” that don’t lead to actual compromises? One explanation is “false positives,” in which an automated system triggers a security warning that turns out not to be a breach of defenses. False positives often happen, no matter what tools the enterprise uses. But having too many of them can result in an enormous waste of time and resources and eventually slows down the IR process.

Respondents in a survey that BitDefender conducted last year described 49% of the security alerts triggered by endpoint devices as being false alarms. Too many false positives can result in alert fatigue and cause IR teams to pay less attention to them. Seventy-two percent of the information security professionals in BitDefender’s survey described their IT teams as experiencing such alert fatigue.

Another reason for the wide variance in volume of security incidents is that enterprises define “incidents” differently. Which events are most likely to be categorized as security incidents? In our Dark Reading survey, the compromise of intellectual property is the most universal response.

### Table of Incidents

<table>
<thead>
<tr>
<th>Description</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>A suspected breach of intellectual property or proprietary business information</td>
<td>74%</td>
</tr>
<tr>
<td>The infection of one or more systems by ransomware or other malware</td>
<td>71%</td>
</tr>
<tr>
<td>A suspected breach of a customer information database or internal systems containing employee data</td>
<td>67%</td>
</tr>
<tr>
<td>A reported or suspected successful phishing attempt</td>
<td>55%</td>
</tr>
<tr>
<td>A suspected case of unauthorized use of applications or data by a noncredentialed user</td>
<td>54%</td>
</tr>
<tr>
<td>A suspected case of unauthorized use of applications or data by an employee or other credentialed user</td>
<td>46%</td>
</tr>
<tr>
<td>A report of a successful cyberattack or exploit perpetrated on one of the organization's suppliers, customers, or other business partners</td>
<td>45%</td>
</tr>
<tr>
<td>A report showing anomalous use of the organization's internal systems, applications, or networks</td>
<td>43%</td>
</tr>
<tr>
<td>An outage of internal IT systems, applications, or networks</td>
<td>41%</td>
</tr>
<tr>
<td>A report of security vulnerabilities in a system, application, or network technology that the organization uses</td>
<td>40%</td>
</tr>
<tr>
<td>A report indicating a vulnerability or breach in a carrier network or cloud service provider that the organization uses</td>
<td>38%</td>
</tr>
<tr>
<td>Multiple unsuccessful attempts to log in to a system, application, or network</td>
<td>35%</td>
</tr>
<tr>
<td>A malware attack that is successfully blocked by the organization's existing security tools</td>
<td>35%</td>
</tr>
<tr>
<td>A report indicating successful online attacks on other organizations in the industry</td>
<td>30%</td>
</tr>
<tr>
<td>The firing of a disgruntled employee or other system user</td>
<td>21%</td>
</tr>
</tbody>
</table>

Data: Dark Reading survey of 150 IT and cybersecurity professionals, December 2018
Seventy-four percent of respondents say they would treat any suspected breach of intellectual property or sensitive, proprietary information as an incident that requires an IR response. A ransomware infection is the second-most common incident trigger at 71% of organizations; 67% say they would treat a suspected breach of customer or employee data as an IR trigger.

Other major incident response triggers include phishing attempts and phishing attacks (55%); unauthorized application use by credentialed or noncredentialed users (54%); and reported attacks on customers, business partners, or other affiliated third parties (45%). Interestingly, 21% of the organizations surveyed would consider the firing of a disgruntled employee or other system user as a response-worthy incident. This last data point highlights the fact that many IR teams must respond to insider threats as well as attacks by outsiders (Figure 3).

Phishing is by far the most common cause of system compromise investigated by IR teams. In fact, more organizations (63%) identified phishing and social engineering attacks as their biggest problem than those who cited malware and targeted attacks combined (58%) (Figure 4). Phishing and social engineering attacks also pose the greatest threat to sensitive data and critical operations for 56% of organizations. A substantially smaller number of respondents — 37% and 36%, respectively — perceive malware and targeted attacks as posing the greatest threat to their security (Figure 5).

These numbers show the enormous threat that phishing and social engineering have
The State of Cybersecurity Incident Response

become for security organizations — and the strain these threats are putting on IR teams. A massive 93% of the breaches that Verizon investigated in its 2018 Data Breach Investigations Report involved phishing, and email was the delivery vector 96% of the time. Of the 1,450 total phishing incidents that Verizon investigated, 381 resulted in data leaks. Among the most targeted by social engineering attacks are the public, healthcare, and educational sectors.

Verizon’s analysis showed that 78% are wise to phishing scams and don’t click on a single phish all year. But the 4% that do fall for the scams appear to be creating major problems for IR teams. Thirty-six percent of organizations in the Dark Reading Incident Response Survey say that one of their most difficult IR tasks is training end users to follow policy and to recognize potential phishing and social engineering attacks (Figure 6).

Ransomware is also complicating incident response processes in many organizations, according to John Pescatore, director of emerging security threats at the SANS Institute. Most of the IR scenarios and playbooks that enterprises have developed over the years are designed to address malware insertion and data exfiltration attacks. Often, the main goal of such IR playbooks is to detect and mitigate infections quickly and to reduce attacker dwell time on the network, he notes. But ransomware attacks don’t work the way other cyberattacks do and are forcing organizations to develop new playbooks, Pescatore says.

Figure 5

<table>
<thead>
<tr>
<th>Greatest Potential Threats to Sensitive Data</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Which types of incidents pose the greatest potential threat to your organization’s sensitive data and/or critical operations?</td>
<td></td>
</tr>
<tr>
<td>Phishing or social engineering attacks that fool users into clicking on malware or giving up credentials</td>
<td>56%</td>
</tr>
<tr>
<td>Targeted attacks on the organization’s systems, applications, or networks</td>
<td>37%</td>
</tr>
<tr>
<td>Malware that evades traditional defenses</td>
<td>36%</td>
</tr>
<tr>
<td>Theft of sensitive business data or intellectual property by hackers/outsiders</td>
<td>23%</td>
</tr>
<tr>
<td>Stolen/compromised passwords</td>
<td>20%</td>
</tr>
<tr>
<td>Theft of sensitive business data or intellectual property by employees/insiders</td>
<td>17%</td>
</tr>
<tr>
<td>Employees or other trusted users attempting to use applications or systems without authorization</td>
<td>14%</td>
</tr>
<tr>
<td>Anomalous/suspicious activity detected on networks, systems, or applications</td>
<td>13%</td>
</tr>
<tr>
<td>Reported vulnerabilities in off-the-shelf applications that the organization uses</td>
<td>12%</td>
</tr>
<tr>
<td>Reported vulnerabilities in applications developed in-house</td>
<td>9%</td>
</tr>
<tr>
<td>Alerts/compromises coming from suppliers, customers, or other business partners</td>
<td>9%</td>
</tr>
</tbody>
</table>

Note: Maximum of three responses allowed
Data: Dark Reading survey of 150 IT and cybersecurity professionals, December 2018

FAST FACT
56%
say phishing or social engineering attacks pose the greatest potential threat to an organization’s sensitive data.
IR Capabilities Today: A Snapshot
How well equipped are today’s organizations to respond to security incidents? The data suggests a maturing set of capabilities. Most believe they have the staff and budget to support their IR needs; nearly half have a security operations center (SOC) for managing and responding to threats. However, the uptake of some of the tools and processes that experts view as critical to IR remains low in some cases. A lack of analyst training, low user awareness of security threats, and the complexity of some incident response technologies are among other obstacles that hamper IR efforts.

Seventy-nine percent of the CIOs, CTOs, CISOs, and other IT security professionals in our survey agree that the most critical part of the IR process takes place within the first 24 hours of discovery of a compromise. Sixty-two percent are confident that their response team is detecting most incidents that might affect the organization’s security posture; 49% say they have enough budget to support the IR program for the next 12 months (Figure 7).

In most cases, organizations have an IR team in place, too. Eleven percent of organizations have at least 25 IT staffers dedicated specifically to the task of security incident response. Another 11% have between 10 and 24 members in their IR team. But for a plurality (31%), the size of the team responding to incidents ranges from two to four; 14% have teams of between five and nine. Some organizations (16%) do not have a separate IR team but have one or two security or IT staffers on standby to help out in the event of an incident (Figure 8).

SOCs have played a key role in supporting incident response at many organizations in recent years. Gartner describes a SOC both as a team that operates in shifts around the clock and as a dedicated facility for preventing, detecting, assessing, and responding to
threats. A SOC capability — either internal or delivered as a managed service — can help organizations establish more control over their security monitoring and IR process. “You can’t do too much in terms of in-depth response if you have an immature SOC,” says Roselle Safran, president of Rosint Labs, who has managed SOCs at both the White House and at US-CERT.

In our survey, 31% of respondents — nearly a third — say their organizations have their own SOC; another 16% contract the function out to a service provider. Twelve percent of the companies that currently do not have a SOC capability plan to implement one internally within the next two years. Together, this means nearly six in 10 organizations have or will soon have a SOC to support their incident response activities (Figure 9).

At the same time, it’s important to recognize that 34% — more than a third of respondent organizations in our survey — do not have either an internal or an outsourced SOC capability and have no plans to build or acquire one. Some experts wonder whether organizations with no SOC capability will be able to adequately respond to a major cybersecurity breach. But some organizations in recent years have begun moving incident response outside the SOC to separate computer security incident response teams.

Upper management support for incident response appears to be strong in most enterprises. Thirty-seven percent say the top executives at their companies understand and...
recognize the importance of the IR process to the security of enterprise data and operations. At 28% of organizations, the board and other top management may not fully understand IR but recognize the need for it. Twenty-one percent of organizations, however, say they lack resources and budget because top management doesn’t understand IR or recognize its importance (Figure 10).

“We are starting to see a lot more incident response tabletop [exercises] and drills being done,” says Christopher Pierson, CEO of security vendor BlackCloak. Corporate boards increasingly ask to understand responses, timelines, how they’ll be notified, and what the process looks like, Pierson says. They also
ask what scenarios the teams have practiced and what lessons have been learned.

“In addition, we are seeing many more internal stakeholders requesting to be a part of the [IR] teams and, in some cases, actually drive the processes,” Pierson says. Marketing and public relations groups, for instance, have become much more involved in IR planning, as have legal teams, he adds.

**Tools, Training, and Other IR Obstacles**

Although there is strong uptake of IR as a discipline, there is some question as to whether organizations are employing the right tools or have the training required to mount an effective IR program.

For example, security experts have for some time advocated the use of security information and event management (SIEM) platforms or other event filtering and log management tools to manage the alert data generated by systems across a large enterprise. Such tools can help SOC operators to quickly sift through the huge volumes of alert and event data generated by myriad threat detection sensors and quickly zero in on the ones that matter. Our survey data suggests that many organizations do not rely on SIEM technology, however: Just 18% of respondent organizations consider SIEM helpful in building an effective IR capability.

Threat intelligence is another tool set that experts recommend as part of the IR process. This intelligence about external threats — including indicators of an emerging attack, reports of new exploits, and insights into threat actors’ tactics, techniques, and procedures — can be combined with internal telemetry to significantly improve IR processes, these experts say. Yet only a bare 8% of respondents in the survey say their organizations are using threat intelligence services or platforms to build
an effective IR process (Figure 11).
Uptake of other IR-related technologies appears to be similarly low. Only 26% of respondent organizations are using behavioral analysis; less than a quarter (24%) have security data analytics capabilities; and just 16% are using log aggregation and analysis tools. The relatively low usage of these technologies suggests that many organizations are pushing forward on IR processes but may not have the tools they need to effectively execute them.

Unsurprisingly, some of the IR tasks that survey respondents identified as being the most cumbersome or time-consuming are those that could be expedited by the use of these missing technologies. For instance, 38% of respondents say that analyzing system, network, and application logs to identify anomalous behavior is one of their most time-consuming IR tasks. Thirty-two percent cite their most time-consuming task as analyzing alert data to determine that an incident had actually occurred. Twenty-five percent complain about the time required to manage false positives.

Among the other time-consuming tasks

| Figure 11 |
| Building an Effective Incident Response Program |
| Which tools or processes are most helpful in building an effective incident response program? |
| Firewalls/firewall monitoring tools | 30% |
| Network analysis | 29% |
| Behavioral analysis | 26% |
| Antivirus/anti-malware tools | 26% |
| Security data analytics tools | 24% |
| Endpoint analysis | 20% |
| Security information and event management/security event management | 18% |
| Malware analysis | 17% |
| System log aggregation/analysis | 16% |
| Machine learning | 10% |
| Threat intelligence feeds/platforms | 8% |
| Deep packet inspection | 7% |
| Artificial intelligence | 7% |
| Data loss prevention/end-user activity monitoring | 7% |
| Tools that help simulate/rehearse potential breach scenarios | 6% |
| Orchestration tools | 3% |

Note: Maximum of three responses allowed
Data: Dark Reading survey of 150 IT and cybersecurity professionals, December 2018

FAST FACT
37%
say upper management understands IR and recognizes its importance to the security of enterprise data and operations.
cited by survey respondents are patch application and management (32%); simulating incident response scenarios with management (23%); and identifying the source of an incident (19%).

Training end users is another key time-consumer for IT organizations. Thirty-six percent of survey respondents say their most time-arduous process is training users to follow policy and learn to recognize potential phishing attacks and social engineering scams.

On the technical side, many incident responders have a hard time understanding the network topology when they first begin to wrestle with a suspected compromise, BlackCloak’s Pierson says. A lot of early hours in IR are wasted as responders try to understand the size of the in-scope network and where they need to focus. “Separately, being able to understand and easily navigate cloud instances — and their specific audit logs and trails — is a learning curve for some forensic responders who are more used to on-premises data centers,” he states.

In response to an open-ended question about IR obstacles, several survey respondents cite a shortage of training. “Training the analyst and keeping them up-to-date is one of my largest challenges,” one respondent wrote. Another wished for “better IR playbook examples and scenario-based training for IT technical staff, to improve handling and forensic investigation.”

Many IR organizations are struggling to find the right people to staff their IR teams, but training internal IT staff on IR processes can be an effective way of addressing the skills shortage.

Many organizations are struggling to find the right people to staff their IR teams, but training internal IT staff on IR processes can be an effective way of addressing the skills shortage.

Joseph Blankenship, principal analyst at Forrester Research, advises organizations that can’t find or train their own incident responders to outsource the function. “Having a retainer with an IR provider is a best practice to speed response and avoid wasted time in the event of an incident,” he says. “Faster response typically means faster containment and recovery.” Many organizations these days rely on third-party services to handle early IR tasks and to augment internal teams.

Security automation and orchestration tools and services also can help internal security teams triage, investigate, and respond to security events, Blankenship observes. “Some of these tools also deliver incident response and case management capabilities to manage workflow across the various teams engaged in an incident response,” he says. Security analytics platforms — including those offered by SIEM vendors and managed service providers — have begun incorporating IR capabilities into their products, he adds.

With so much focus emerging on IR, many security departments today wonder how to find the right resource balance between...
IR and traditional prevention and perimeter defense tasks. Should there be a 50-50 split between the two areas of discipline, or should they spend more time on one of them?

Responses to this question in the Dark Reading 2019 Incident Response Survey show a wide range of opinions on the “right” balance between prevention and IR. A small 20% plurality feels that the right formula is a 70% focus on prevention and a 30% focus on incident response. Eighteen percent say an 80/20 split between prevention and response represents the best balance; 15% say the right mix is 60 percent prevention and 40% IR. Nearly one-third (31%) of respondents say they currently focus 80% to 90% of their resources on perimeter defense (Figure 12). Overall, 45% of organizations say they spend more time and resources on prevention than on IR.

This survey data suggests that many enterprises continue to resist strategies and philosophies that call for the organization to assume that it has already been breached. While such sentiments have certainly fueled the growth of IR activity in recent years, our survey data clearly shows that a majority of organizations still see threat prevention and perimeter defense as the most essential portion of their security strategy.

This emphasis on prevention makes sense, Rosint Labs’ Safran says. “I always advise a focus on the basics of prevention first,” she says. That includes focusing on processes like vulnerability remediation and patch management, which are often considered responsive, rather than preventative, measures. “If you have your defenses shored up well, that
makes detection and response much more feasible and manageable,” Safran advises.

Rather than getting hung up on allocating resources between prevention and response, administrators should focus on making things as difficult as possible for an attacker to enter in the first place, Safran says. That means blocking the attacks you can block, so that you can deal more effectively with the ones you can’t. “If you have that base squared away, the number of detections goes down dramatically, and the need to respond goes down as well,” she says.

Pescatore of SANS Institute agrees there’s more to improving security response than just the manner in which resources are allocated. For instances, research from SANS has shown that the organizations making the greatest IR advancement in recent years are those that have brought their SOC and network operations center processes closer together. IR teams that can integrate information from IT, network, and security operations groups often have better visibility into threat activity across the infrastructure, and are therefore able to act upon it more quickly. “There’s a lot of information that IT is using for network and app performance monitoring that is also useful for incident response,” Pescatore says.

**Conclusion**

Concerns over data breaches and disruptions are driving a greater focus on incident response processes. A majority of enterprises recognize the importance of having a robust IR capability, even as they remain firmly focused on breach prevention and defense. Budgets and support for the IR function are relatively strong across most enterprises. However, many organizations might be limiting their ability to conduct an efficient IR operation by failing to adopt tools and technologies, such as SIEM, threat intelligence, and orchestration, that can help address some of their most complex and time-consuming processes. While most organizations have IR capabilities in place, many will need to upgrade their strategies, tools, and processes if they hope to stay ahead of modern cyber threats.
**Figure 13**

**Sharing Information**
When your organization experiences an incident that it has never seen before, what steps does it take to share that information?

<table>
<thead>
<tr>
<th>Step</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>We share it with our security vendors/service providers</td>
<td>37%</td>
</tr>
<tr>
<td>We share it with business partners/customers that might be affected</td>
<td>35%</td>
</tr>
<tr>
<td>We share it with a recognized threat-sharing organization</td>
<td>34%</td>
</tr>
<tr>
<td>We share it with law enforcement agencies</td>
<td>29%</td>
</tr>
<tr>
<td>We share it with relevant service providers</td>
<td>24%</td>
</tr>
<tr>
<td>We don't share internal security data with any other organization</td>
<td>24%</td>
</tr>
<tr>
<td>We share it with other government agencies</td>
<td>17%</td>
</tr>
<tr>
<td>We share it with other enterprises in our industry</td>
<td>16%</td>
</tr>
<tr>
<td>We share it with security media sites or other online portals</td>
<td>9%</td>
</tr>
<tr>
<td>We share it over social media</td>
<td>4%</td>
</tr>
</tbody>
</table>

Note: Multiple responses allowed
Data: Dark Reading survey of 150 IT and cybersecurity professionals, December 2018
**Figure 14**

**Respondent Job Title**

Which of the following best describes your role in the organization?

- Network/system administrator: 15%
- Information technology executive (CIO, CTO): 6%
- Information technology director/head: 12%
- Information security department staff: 8%
- Information security department manager: 8%
- President/CEO/managing director/other senior level corporate executive: 13%
- Chief security officer/chief privacy officer: 11%
- VP of IT or security: 5%
- Information security director/head: 5%
- Director/VP (non-IT): 5%
- Developer/engineer: 7%
- Other: 3%

Data: Dark Reading survey of 150 IT and cybersecurity professionals, January 2019
Figure 15

**Respondent Company Size**

How many employees are in your company in total?

- 5,000 or more: 22%
- 1,000 to 4,999: 31%
- 100 to 999: 27%
- Fewer than 100: 20%

Data: Dark Reading survey of 150 IT and cybersecurity professionals, January 2019
Figure 16

**Respondent Industry**

**What is your organization's primary industry?**

- Computer or technology manufacturer/tech vendor: 18%
- Banking/financial services/VC/accounting: 13%
- Education: 12%
- Consulting/business services: 11%
- Manufacturing, industrial, process (non-computer): 10%
- Healthcare/pharmaceutical/biotech/biomedical: 9%
- Government: 8%
- Media/marketing/advertising: 7%
- Solutions provider/VAR: 8%
- Travel/hospitality/recreation/entertainment: 3%
- Wholesale/trade/distribution/retail: 3%
- Other: 3%

Data: Dark Reading survey of 150 IT and cybersecurity professionals, January 2019