DARK Reading
REPORTS
February 2020

Next

How Enterprises Respond to the Incident Response Challenge

Data breaches and regulations have forced organizations to pay closer attention to the security incident response function. However, security leaders may be overestimating their ability to detect and respond to security incidents.

Sponsored by paloalto NETWORKS | CORTEX XDR BY PALO ALTO NETWORKS

informa tech

TABLE OF CONTENTS

Table of Contents

3 About the Author
4 Executive Summary
5 Research Synopsis
6 Heightened Awareness of the Need for Incident Response
9 Incident Response Triggers
13 Challenges and Gaps
19 Conclusion
20 Appendix

Figures

Figure 1: Incident Response Statements
Figure 2: Balance of Resources
Figure 3: Relationship Between IR Team and Other Business Partners' IR Teams
Figure 4: Building an Effective Incident Response Program
Figure 5: Methods Used to Detect Incidents
Figure 6: Sharing Information
Figure 7: Definition of Incident Response
Figure 8: Number of Security Incidents in a Typical Month
Figure 9: Common Types of Security Incidents
Figure 10: Percentage of Incidents with a Negative Effect
Figure 11: Greatest Potential Threats to Sensitive Data
Figure 12: Difficult Response Tasks
Figure 13: Dedicated Incident Response Staff
Figure 14: Security Operations Center
Figure 15: Length of Time Between Incidence and Detection of Potential Compromise
Figure 16: Length of Time Between Detection and Remediation of Potential Compromise
Figure 17: Respondent Job Title
Figure 18: Respondent Company Size
Figure 19: Respondent Industry

Jai Vijayan
Dark Reading Reports

About the Author

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, TechTarget, and several other publications.

EXECUTIVE SUMMARY

Data breaches and regulatory compliance pressures have forced organizations to pay closer attention to the security incident response (IR) function in recent years. A growing number of organizations are shifting from a purely intrusion-prevention focus to strategies that are also designed to detect and contain breaches quickly.

Dark Reading's 2020 Incident Response Survey reveals a generally higher level of awareness of IR issues among organizations compared with a year ago. More organizations appear to recognize the need for speed in threat detection and response. Attitudes toward the use of log management, security information and event management, and security analytics tools appear to be maturing, and a high percentage of organizations see value in allocating a substantial proportion of their security resources toward IR.

However, our survey also revealed a troubling gap between perception and reality. Many security leaders appear to be overestimating their ability to detect and respond to security incidents. Many organizations lack dedicated staff for handling IR functions. And for all the heightened awareness around cyber incident response, some organizations' definition of a "security incident" may overlook significant events.

Here are some interesting data points from the survey:

- The No. 1 IR challenge, which 36% of respondents cite, is determining the scope of an incident.
- 31% of organizations experience less than one security incident per month; 10% experience 500 or more.
- 39% of respondents consider endpoint analysis tools to be the most important for IR.
- 30% of organizations lack dedicated staff for incident response, including 6% that have nobody designated to the task at all.
- 36% of organizations do not feel they have adequate technological support to respond to security incidents that may occur in the next 12 months.
- 94% agree that the most critical part of the response takes place within the first 24 hours.
- Most respondents (57%) say that only a small proportion of attacks (less than 5%) cause significant negative impact on their organizations.
- 27% of organizations immediately share security incident data with their business partners.
- 12% do not consider a ransomware infection to be a security incident.

Previous Next

Table of Contents

SYNOPSIS

RESEARCH

Survey Name Dark Reading 2020 Incident Response Survey

Survey Date February 2020

Primary Region North America

Number of Respondents 100 IT and cybersecurity professionals at companies of all sizes. The margin of error for the total respondent base (N=100) is +/-9.7 percentage points.

Purpose Dark Reading surveyed IT and cybersecurity professionals to understand how enterprises are building their incident response teams and processes, how potential compromises are detected, how they respond to new breaches, and what tools and processes they use to remediate problems and improve their cyber defenses for the future.

Methodology The survey queried decision-makers with job titles that involve IT and IT security at predominantly North American organizations. The survey was conducted online. Respondents were recruited via an email invitation containing an embedded link to the survey. The email was sent to a select group of Informa Tech's qualified database; Informa is the parent company of Dark Reading. Informa Tech research was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.

ABOUT US

Dark Reading Reports offer original data and insights on the latest trends and practices in IT security. Compiled and written by experts, Dark Reading Reports illustrate the plans and directions of the cybersecurity community and provide advice on the steps enterprises can take to protect their most critical data.

Dark Reading Reports

Previous Next
Table of Contents

Heightened Awareness of the Need for Incident Response

Data from Dark Reading's 2020 Incident Response Survey suggests a heightened awareness and maturity around key aspects of cyber incident response (IR). For example, 94% of organizations — compared with 79% last year — agree that the first 24 hours after an incident occurs is the most critical from an IR standpoint (**Figure 1**).

That's in line with thinking by many security experts who say the first 24 hours is when organizations should be working on identifying the source, depth, and scope of a breach; locking down systems; protecting evidence; and figuring out a response and recovery plan. The first 24 hours is also when organizations need to work with their lawyers and compliance teams to understand legal and breach disclosure obligations, put into motion their communication and notification plans, and get in touch with law enforcement if needed. With mandates such as the California Consumer Privacy Act (CCPA) and the European Union's General Data Privacy Regulation (GDPR), what companies do in the immediate hours and days after a breach can go a long way toward reducing damages and exposure to compliance-related issues.

Figure 1

Incident Response Statements

Do you agree or disagree with the following statements?

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
When an incident occurs, the most critical part of the response takes place within the first 24 hours	62%	32%	5%	1%
I am confident that my incident response (IR) team is detecting most of the incidents that might affect the security of my organization's data	33%	48%	9%	10%
The availability of external threat intelligence feeds and services has significantly enhanced my organization's IR effort	28%	46%	21%	5%
My organization spends more time and resources on preventing cyberattacks and intrusions than it does on IR	26%	44%	23%	7%
I believe that the discipline of IR is well defined within the security industry, and I have been able to easily find knowledge and guidelines for implementing an IR program in my own organization	25%	44%	25%	6%
My organization has enough skilled people to properly respond to the threats I expect to see in the next 12 months	21%	45%	15%	19%
I feel that the current technology available to aid IR teams is adequate to meet my organization's needs over the next 12 months	19%	45%	24%	12%
My organization has provided sufficient budget to support the IR efforts that will be required in the next 12 months	14%	42%	25%	19%

Data: Dark Reading survey of 100 IT and cybersecurity professionals, February 2020

"One of the most critical elements of IR is the IR plan," says Roselle Safran, president of Rosint Labs, who has managed security operations centers (SOCs) at the White House and US-CERT. The plan has to be well thought-out, well documented, understood, and approved by all of the parties who will be playing a role in IR efforts. All the departments that need to contribute to IR — including security, management, networking, legal, and public relations — must know from whom they will need input and updates, and to whom they will provide input and updates. "When there is a major incident, it's common for communications to go haywire if the pathways weren't clearly defined and the process wasn't practiced beforehand," Safran says.

Dark Reading's survey results yielded other indicators of the maturing attitude and heightened awareness around incident response. For instance, 69% of respondents agree that IR practices are well defined within the security industry and say that guidelines and information for implementing IR programs are now easily available.

After decades of focusing on a prevention-first security strategy, a high percentage of enterprise organizations also have begun seeing value in allocating more resources to IR. Security experts have noted that the trend is driven by the growing realization that organizations can no longer realistically expect to block every single attack that is directed at them. The sheer volume of attacks, and the growing variety of ways that criminals can gain access to enterprise assets — on-premises, in the cloud, and on mobile devices — have made breaches almost a cost of doing business for most organizations.

"Prevention is better than cure," says Maxine Holt, an analyst at Ovum. "However, not every security incident and breach can be prevented, so security time and budget should be allocated to detection and response."

In Dark Reading's 2019 survey, 53% of respondents said it was necessary to allocate 30% or more of their security resources for incident response (**Figure 2**). In our 2020 survey, about the same percentage — 54% — say the same thing. What is noteworthy, though, is the substantial increase in the proportion of respondents who feel that for truly effective IR, they need to split resources evenly between response and intrusion prevention — 19% this year compared with 11% in 2019. Eight percent of respondents even suggest that more than half of their resources should be spent on response.

Significantly, more than a quarter (27%) say their internal IR teams are well connected with the IR teams of their most important business partners (**Figure 3**). These organizations have processes in place for immediately

Figure 2

Balance of Resources

What is the best balance of resources, keeping in mind that, in recent years, the security industry has focused less on perimeter defense and intrusion prevention while investing more in incident response (IR)?

	2020	2019
100% prevention, 0% IR	8%	7%
90% prevention, 10% IR	9%	13%
80% prevention, 20% IR	27%	18%
70% prevention, 30% IR	13%	20%
60% prevention, 40% IR	14%	15%
50% prevention, 50% IR	19%	11%
40% prevention, 60% IR	3%	4%
30% prevention, 70% IR	2%	2%
20% prevention, 80% IR	2%	0%
10% prevention, 90% IR	1%	0%
0% prevention, 100% IR	0%	1%
Don't know/not sure	2%	9%

Data: Dark Reading survey of 100 IT and cybersecurity professionals in February 2020 and 150 in January 2019

FAST FACT

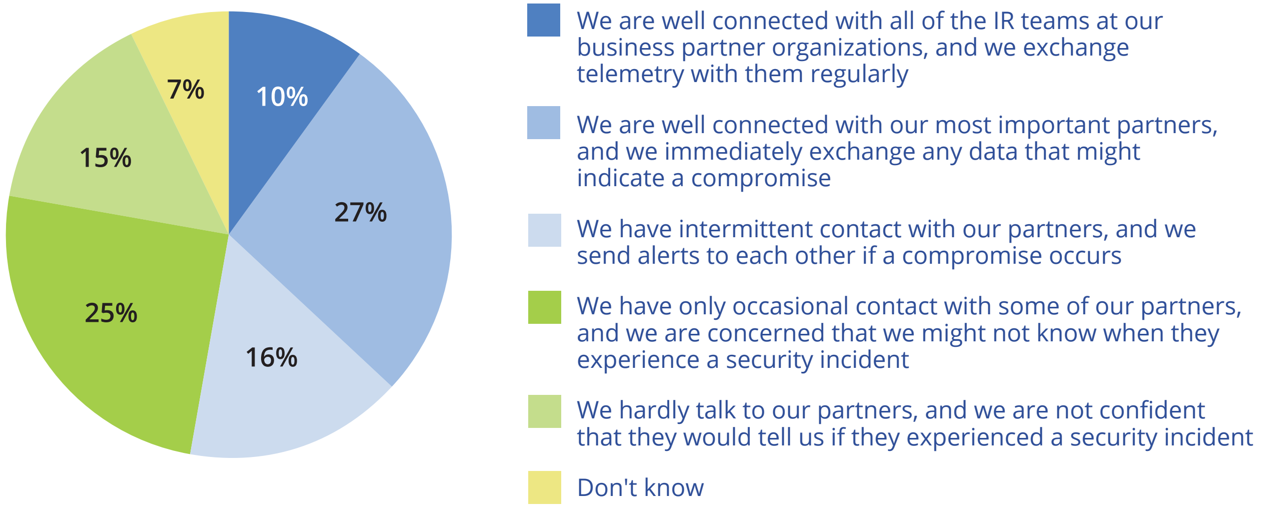
32%

report that SIEM tools are most helpful in building an effective incident response program.

Figure 3

Relationship Between IR Team and Other Business Partners' IR Teams

Which statement best describes the relationship between your incident response (IR) team and the IR teams of customers, suppliers, and other business partners?



Data: Dark Reading survey of 100 IT and cybersecurity professionals, February 2020

exchanging data with key business partners about any incident that might indicate a compromise. Another 10% describe having similar contact with IR teams at all of their business partners and exchanging telemetry with them.

The responses highlight the attention that a substantial number of companies have begun paying to third-party relationships.

Over the last two years, numerous companies have experienced security incidents as the result of an attack on a business partner or supplier. "The traditional boundaries of attack surfaces are shifting as suppliers, partners, and managed service providers integrate with organizations' business processes and infrastructure," Accenture noted in a recent report. Our data suggests that many organizations have seen the threat and have implemented or are implementing plans to work with third parties to contain fallout when a security incident happens.

Our 2020 survey also shows significantly better awareness of the useful role that log aggregation, log management, and malware analysis tools can play in incident response. Such tools enable organizations to quickly sift through and correlate large volumes of historical data from logs and security events to identify anomalous behavior and other indicators of compromise.

Thirty-two percent of survey respondents, compared with just 18% last year, say they find security incident and event management (SIEM) tools to be especially helpful in mounting an effective incident response (**Figure 4**). Interest in endpoint analysis tools nearly doubled from 20% last year to 39% this year, and so, too, did the percentage of organizations describing malware analysis tools as most helpful — up to 31% compared with 17% in 2019.

"Data is an essential component of incident response," says Ovum's Holt. Data from network traffic analysis, endpoint detection

Previous Next

Table of Contents

Figure 4

Building an Effective Incident Response Program

Which tools or processes are most helpful in building an effective incident response program?

	2020	2019
Firewalls/firewall monitoring tools	47%	30%
Antivirus/anti-malware tools	45%	26%
Endpoint analysis	39%	20%
Backup and recovery services	38%	N/A
Network analysis	32%	29%
SIEM/SEM	32%	18%
Malware analysis	31%	17%
System log aggregation/analysis	31%	16%
Behavioral analysis	21%	26%
Security data analytics tools	20%	24%
Threat intelligence feeds/platforms	18%	8%
Digital forensics tools	15%	N/A
Tools that help simulate/rehearse potential breach scenarios	15%	6%
DLP/end-user activity monitoring	12%	N/A
Artificial intelligence	10%	7%
Deep packet inspection	8%	7%
Orchestration tools	8%	3%
Machine learning	7%	10%

Note: Maximum of three responses allowed
Data: Dark Reading survey of 100 IT and cybersecurity professionals in February 2020 and 150 in January 2019

and analysis tools, SIEM, and log management capabilities can help organizations quickly zero in on the source of an incident and mount a response to it, she says.

Many enterprises have begun combining this internal telemetry with data from external threat intelligence sources to get a more holistic understanding of their security exposure. Data from threat intelligence feeds — especially industry-specific data — can alert organizations to new indicators of compromise, new malware, unfolding attacks, and the tactics, techniques, and procedures that threat actors are using in new campaigns. By mapping this data with internal telemetry, many organizations are hoping to stay a step ahead of threats as much as they can.

Dark Reading's 2020 Incident Response Survey shows that a substantial number of organizations view threat intelligence as vital to effective incident response. Nearly three-quarters (74%) of the respondents in our survey say that the availability of external threat intelligence feeds and services has significantly enhanced their organization's IR effort. At four in 10 organizations, threat intelligence sources flag emerging issues or threats and allow them to do a search to see if those issues are occurring within their environment (**Figure 5**). Eighteen percent, compared with 8% in Dark Reading's 2019 survey, consider threat intelligence one of the most helpful tools for building an incident response program.

Many organizations are not just consumers of threat intelligence but also active contributors to it. More than one-third share incident information with business partners, vendors, and service providers; 31% share it with a recognized threat-sharing organization; and 22% share security incident data with law enforcement (**Figure 6**).

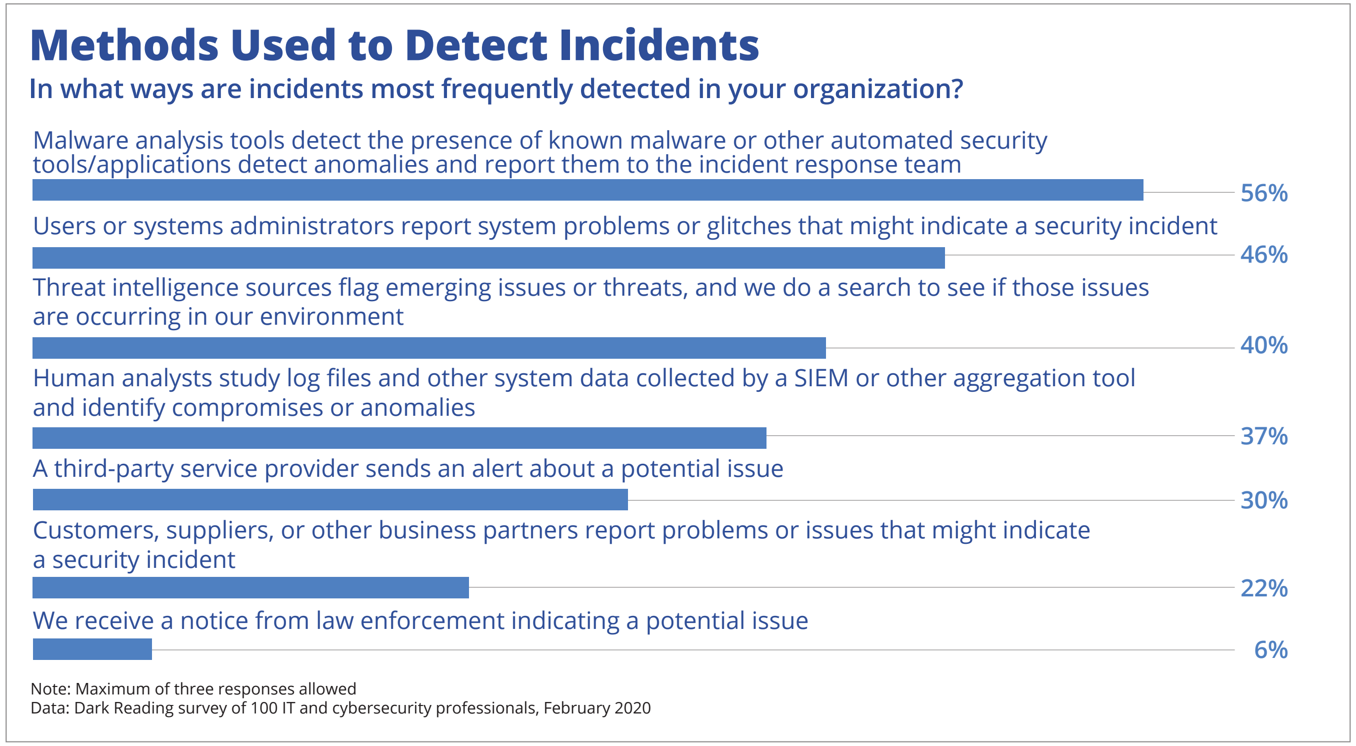
Incident Response Triggers

What security incidents trigger a response process, and what tools or processes are organizations using to respond to them? Given the sheer volume of attack activity and the growing number of ways that bad actors can affect security, it should come as little surprise that most organizations have a pretty broad definition of what defines an incident that merits a formal response.

Previous Next

Table of Contents

Figure 5



Methods Used to Detect Incidents

In what ways are incidents most frequently detected in your organization?

Note: Maximum of three responses allowed
Data: Dark Reading survey of 100 IT and cybersecurity professionals, February 2020

Ransomware tops the list, with 88% of respondents, compared with 71% last year, identifying it as something that would trigger a response process (**Figure 7**). The high level of concern evident in that response is not surprising given the numerous incidents over the past year during which major organizations have experienced significant operational disruptions and financial losses because of ransomware. In response to an open-ended question, numerous survey-takers also highlight ransomware as their top concern. "It causes unbelievable harm, unbudgeted expense, and business reputation damage," one respondent says.

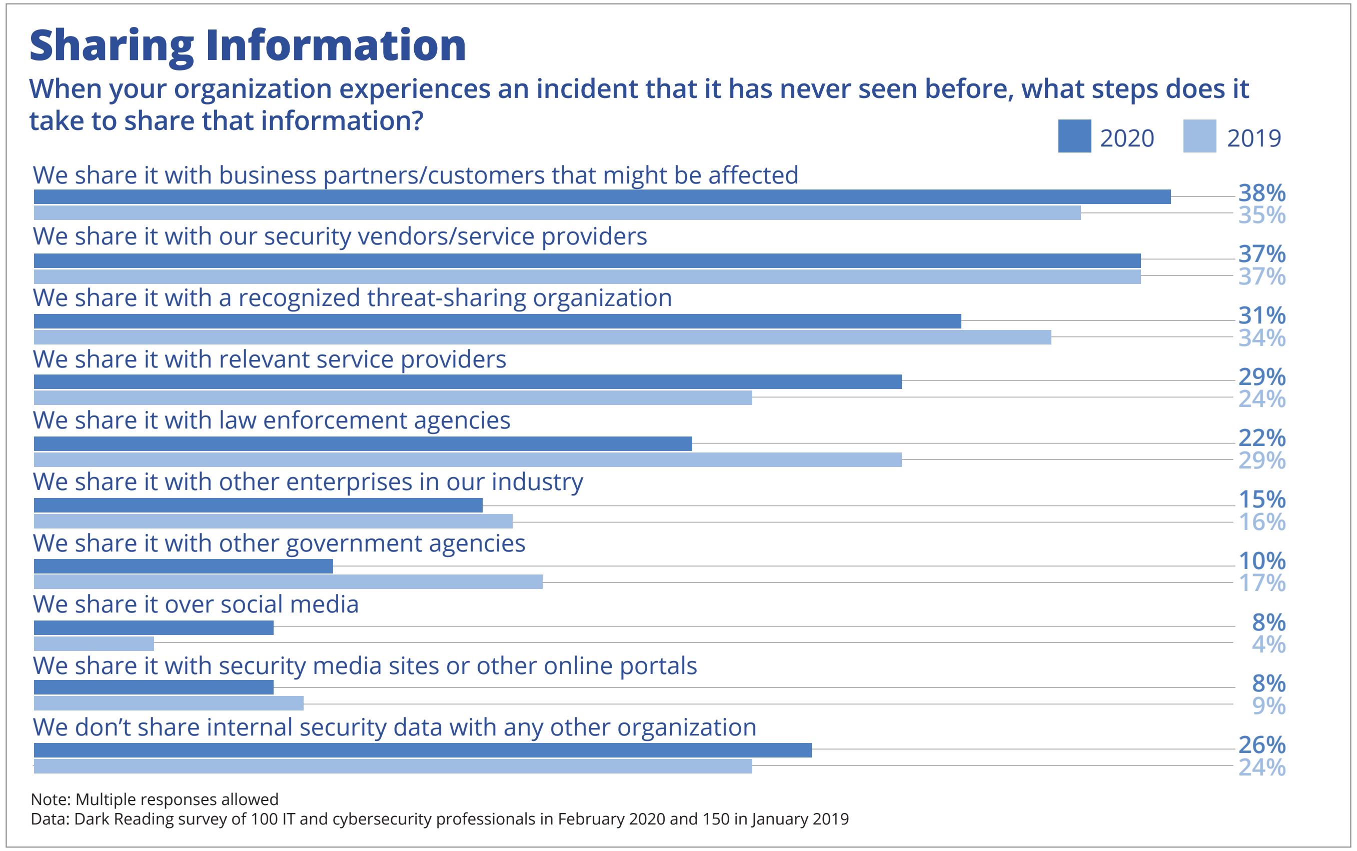
Similarly, 84% of organizations consider any breach involving customer or employee data to be an event that would require a full-fledged incident response. That number is substantially greater than the 67% who responded the same way last year. Data privacy statutes such as CCPA and GDPR — and the stringent consequences for noncompliance associated with them — are likely major factors for the heightened attention to breach response. Another likely issue is reputational damage, based on responses to an open-ended question from survey-takers.

As might be expected, malware and breaches of customer and employee data are by far not the only triggers for incident response. More than 50% of organizations in each instance also define security incidents as any event involving the breach of intellectual property; unauthorized use of applications, data, and systems by credentialed and uncredentialed employees; phishing attempts; attacks on third parties; and unsuccessful login attempts and system outages. Other triggers include reports of security vulnerabilities in applications and systems, reports of vulnerabilities in carrier and cloud provider systems, and the firing of a disgruntled employee.

Previous Next

Table of Contents

Figure 6



Sharing Information

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

Note: Multiple responses allowed
Data: Dark Reading survey of 100 IT and cybersecurity professionals in February 2020 and 150 in January 2019

Once again, our survey responses indicate a heightened awareness of the need for effective response processes for issues that many organizations may not have paid as much attention to in the past. One case involves the anomalous use of the organization's internal systems, applications, or networks. Sixty-nine percent in our 2020 survey describe this as an issue that would trigger an incident response, compared with just 43% last year. Similarly, 62% say they would respond to reports of a successful cyberattack or exploit involving one of their suppliers, customers, or other business partners, compared with 45% who felt that way last year. As one of our survey respondents notes: "The most-feared incident within my organization would be one whereby my client's customer information is hacked in some way. This would be the most sensitive data and would have the greatest impact on my client's company."

Thirty-one percent of respondents say their organizations average fewer than one security incident per month (under 12 per year), but 21% experience between one and four security incidents each month — an increase from the 15% who said they experienced this volume of attacks last year (**Figure 8**).

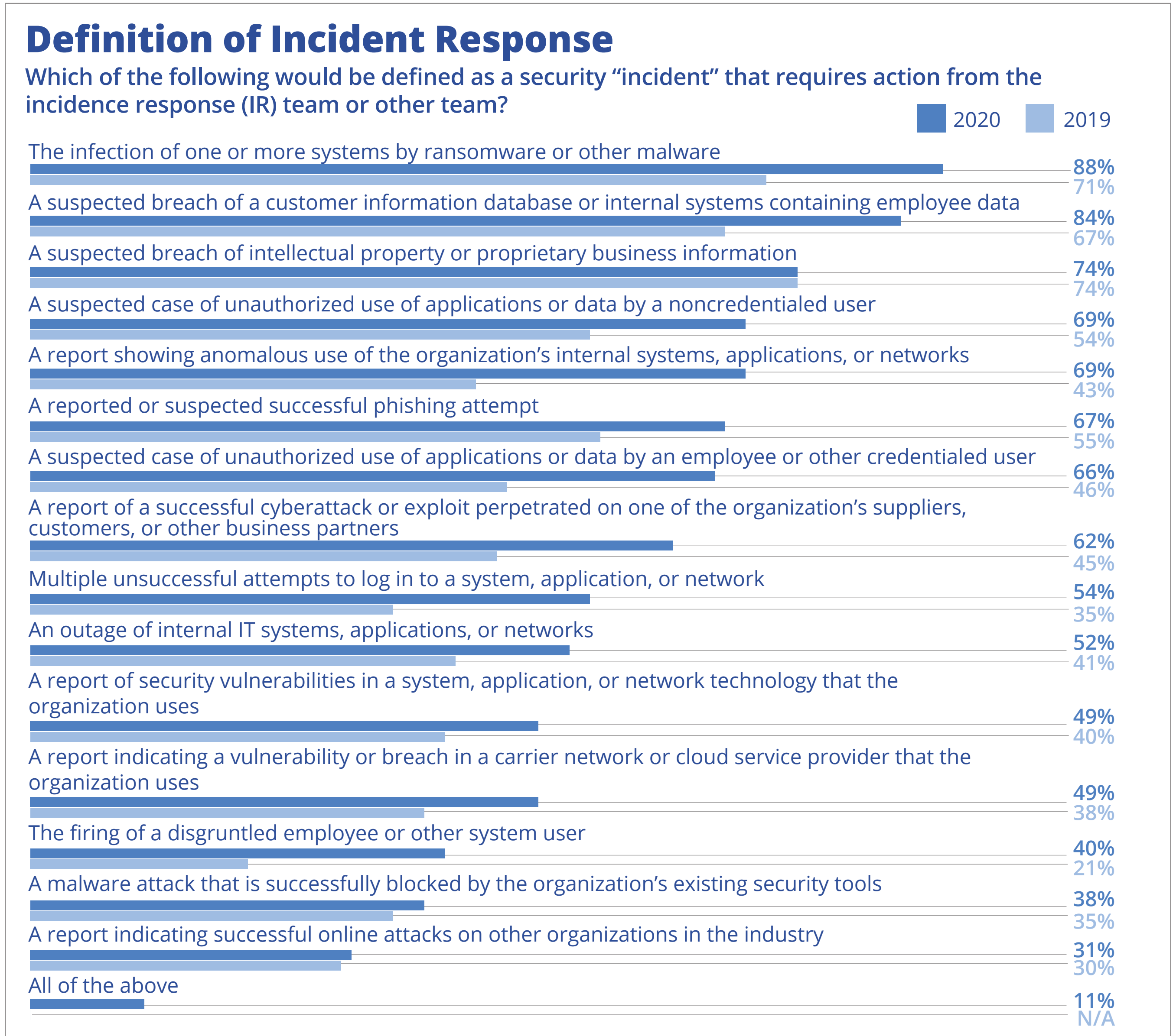
Disturbingly, nearly one in five (19%) experience between five and 24 incidents every single month, and another 5% see between 50 and 99 attacks in the same period. At the extreme end, 6% of our respondents claim their organizations experience 1,000 or more security incidents per month. Although the range in numbers partly reflects organizations' size and differing definitions of "incident," the numbers verify what many security researchers have described and Dark Reading's own surveys have shown: Attack

FAST FACT

32%

report that their organizations respond to 10 or more security incidents in a typical month.

Figure 7



Data: Dark Reading survey of 100 IT and cybersecurity professionals in February 2020 and 150 in January 2019

volumes have grown to unmanageable volumes at many organizations.

The most common security events that respondents actually experience and spur an incident response are phishing (35%), ransomware (27%), and unsuccessful login attempts (27%) (**Figure 9**). Other top incident types include malware attacks, vulnerability reports in applications and systems, system outages, and suspected breach of customer or employee data.

A vast majority of the security incidents to which organizations respond have little significant negative impact on their bottom line, cause much damage, or incur high remediation costs (**Figure 10**). In fact, for 57% of organizations, less than 5% of security incidents cause much pain. That number by itself is a bit misleading, though.

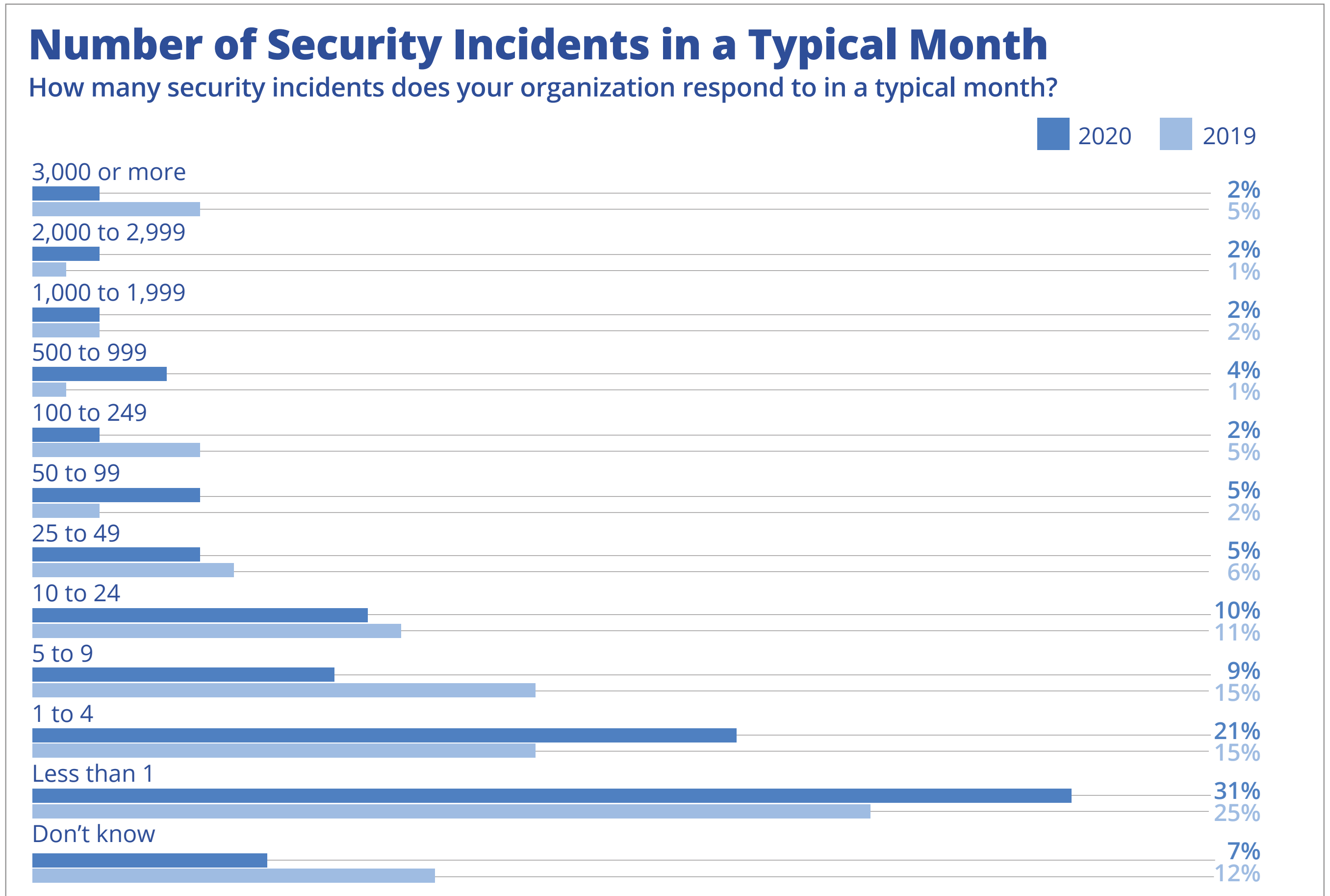
Data from other research has shown that the handful of incidents that do have an impact can cause considerable financial harm. Last year's edition of the annual IBM-sponsored Ponemon Institute study of data breach costs found that US organizations on average spent $8.19 million on breach-related costs in 2019 — more than double

Like This Report?
Share it!
Like Tweet
Share

Previous Next

Table of Contents

Figure 8



Data: Dark Reading survey of 100 IT and cybersecurity professionals in February 2020 and 150 in January 2019

the average costs globally. A disturbingly high 12% of our survey respondents say more than 50% of security incidents have a significant, negative financial and/or operational impact.

Breaches affecting customer and employee data top the list of threats that organizations are most concerned about, with 59% identifying that as their biggest issue (**Figure 11**). Other threats that make businesses and other entities especially nervous include ransomware (58%), threats to intellectual property (39%), and system outages (20%).

Challenges and Gaps

The effectiveness of an organization's IR function depends heavily on the tools and processes in place for detecting threats quickly and mapping them to known vulnerabilities and gaps in internal systems. Our data shows that businesses and other entities are using a wide variety of technologies — including several long-recommended tools such as SIEM and threat intelligence platforms — to enable an IR capability. However, several factors are undermining their ability to derive maximum value from these investments.

"From a technology perspective, the security team will need to access compromised machines and data that may go back weeks or months or longer," Rosint Labs' Safran says. "If the team can't pull information from remote machines because there's no capability in place or can't analyze old logs because they haven't been retained in an accessible manner, the IR team will not be able to effectively investigate the incident," she adds.

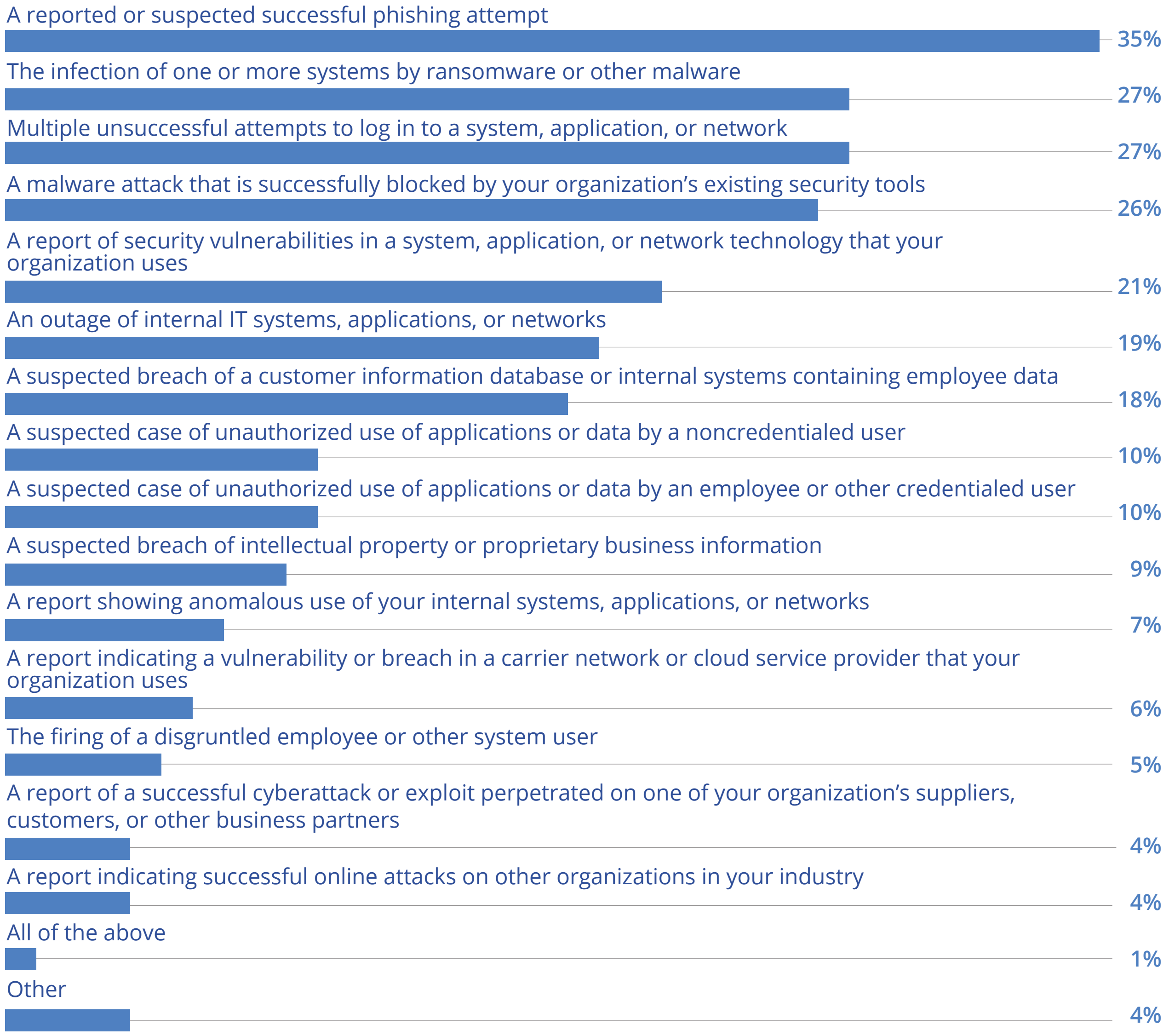
Dark Reading's 2020 Incident Response Survey shows that most companies (56%) rely on malware detection and other automated tools to detect most security threats. Forty percent are warned of incidents via their threat intelligence platform; SIEM systems and other log management tools do the alerting at 37% of organizations. Nearly half (46%) say that users and systems admins or analysts are the ones who most frequently detect security incidents.

When asked to identify the tools and processes most helpful in building an effective IR capability, respondents point to a list of old favorites and some less-predictable ones. Unsurprisingly, for instance, 47% and 45%, respectively, identify firewalls and anti-malware tools as core necessities. But a substantial proportion also note the importance of capabilities such as endpoint detection and response (39%), data backup and recovery (38%), SIEM (32%), behavioral analysis (21%), security data analytics tools (20%), and threat intelligence platforms (18%).

Figure 9

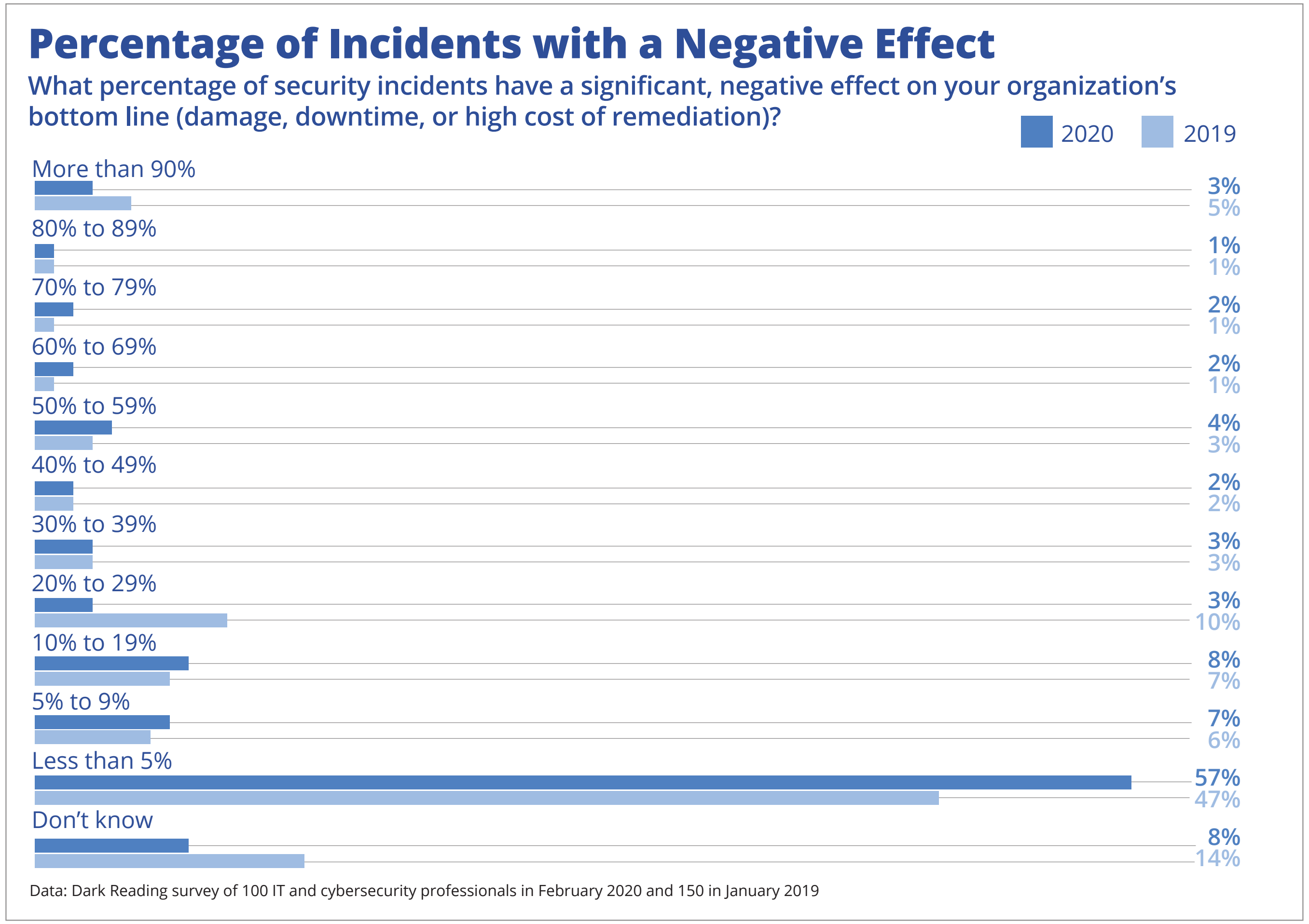
Common Types of Security Incidents

Which types of incidents are most common in your organization?



Note: Maximum of three responses allowed
Data: Dark Reading survey of 100 IT and cybersecurity professionals, February 2020

Figure 10



Percentage of Incidents with a Negative Effect

What percentage of security incidents have a significant, negative effect on your organization's bottom line (damage, downtime, or high cost of remediation)?

Data: Dark Reading survey of 100 IT and cybersecurity professionals in February 2020 and 150 in January 2019

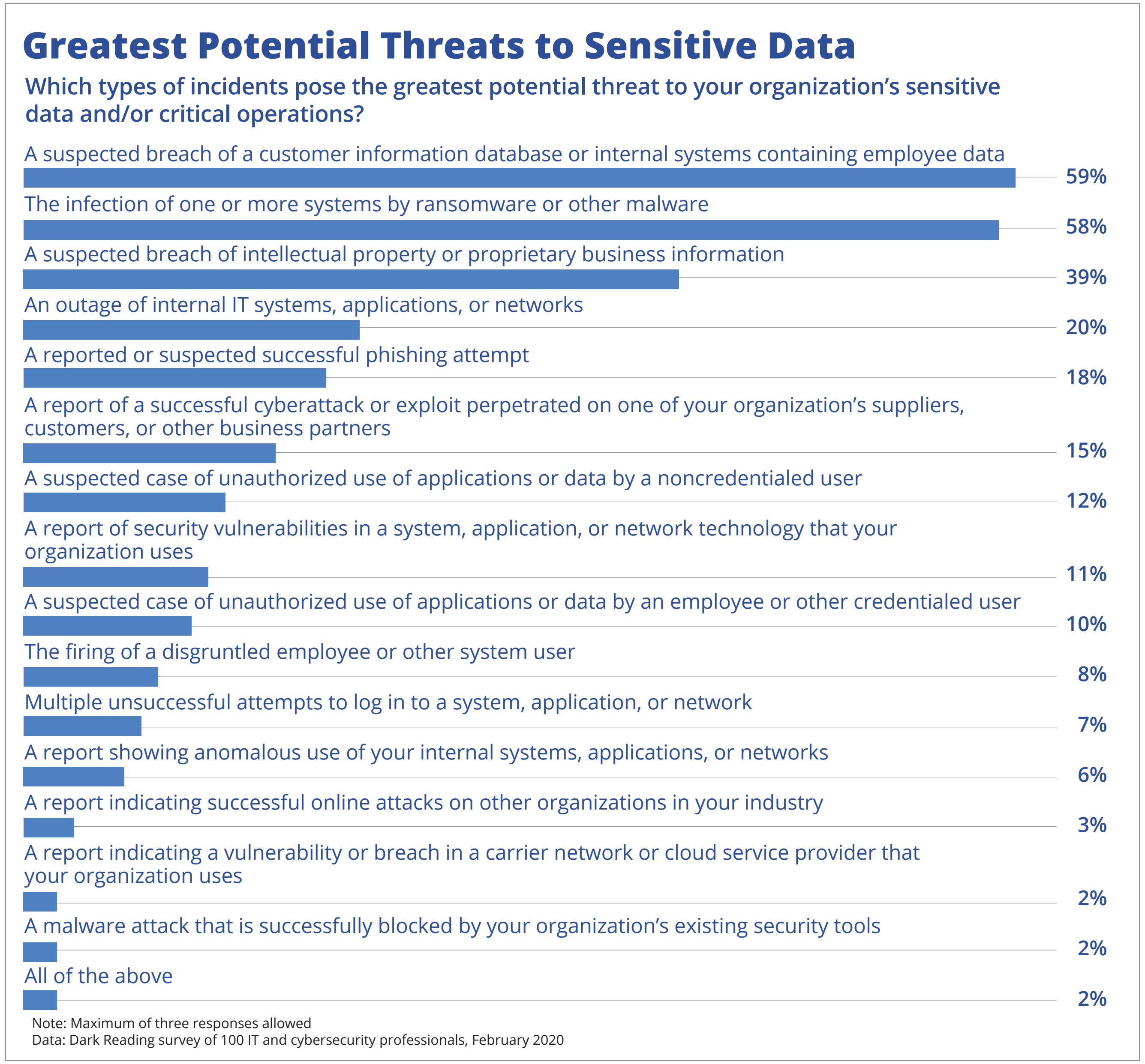
As with most things security-related, however, our survey reveals some issues that might be getting in the way of effective IR at a high percentage of organizations. For instance, third-party risks are mounting, but 41% of organizations only intermittently or occasionally keep in touch with their business partners on IR matters.

Also, while businesses and other enterprise organizations generally appear to be getting better at dealing with IR processes, a high percentage still struggle with many of them. Incident scoping is one example. Thirty-six percent, or more than one-third of organizations in our survey, say that the most difficult or time-consuming part about the IR process was identifying all the systems and data that might have been affected. Similarly, log analysis, which is fundamental to incident response, continues to be a challenge for 34% of organizations.

The list goes on. Thirty percent of organizations still struggle with patch management (compared to 32% in 2019), data analytics (29% in 2020 vs. 32% in 2019), false alerts (22% vs. 25%), and developing/documenting an IR plan (20% vs. 29%) (**Figure 12**).

Budget, management buy-in and manpower resources are other issues. When asked if they have enough resources to adequately respond to incidents that may hit in the next 12 months, many respondents indicate their organizations fall short — citing inadequacies in staff (34%), technology (36%), and budget (44%).

Figure 11


Greatest Potential Threats to Sensitive Data

Which types of incidents pose the greatest potential threat to your organization's sensitive data and/or critical operations?

Note: Maximum of three responses allowed
Data: Dark Reading survey of 100 IT and cybersecurity professionals, February 2020

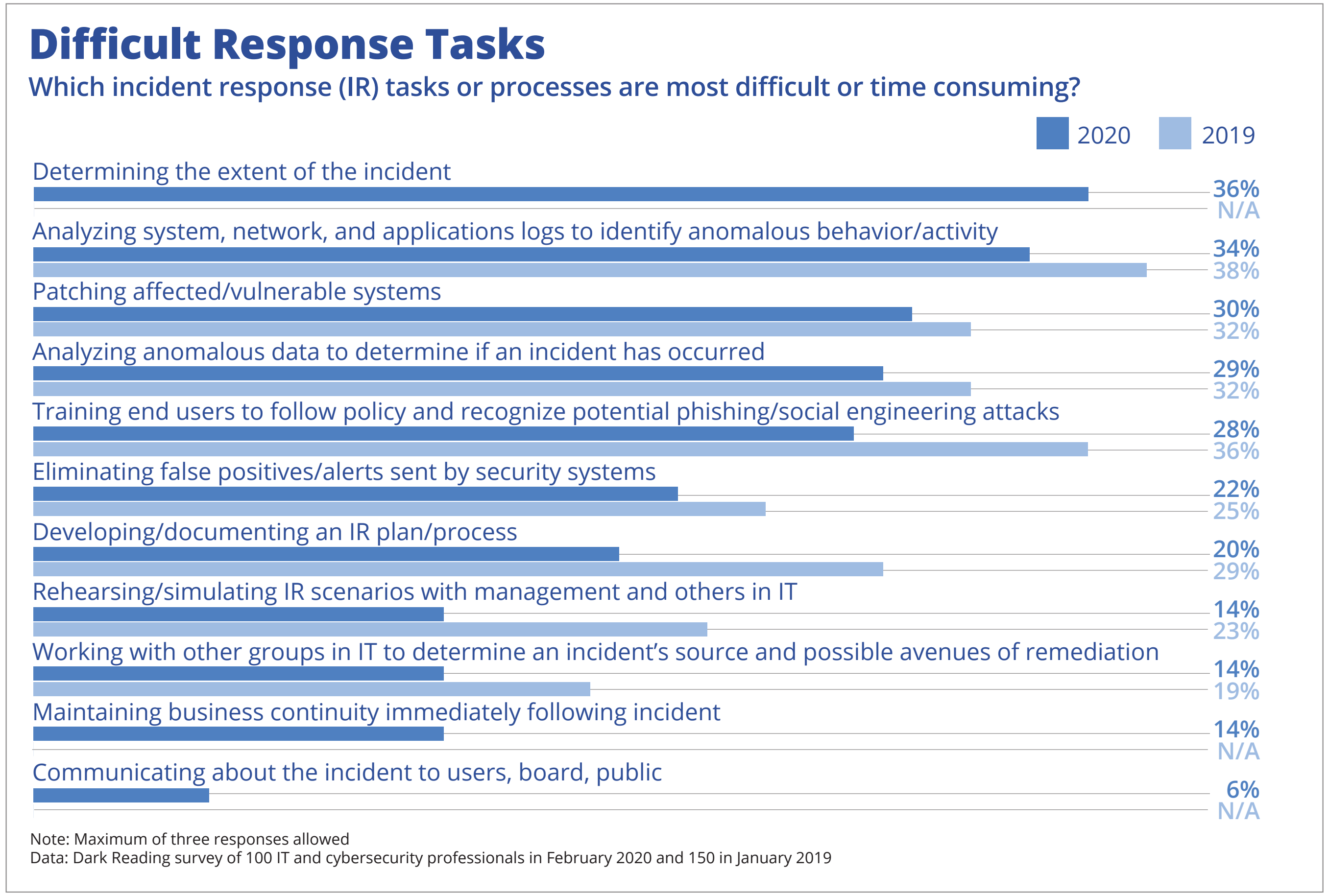
"The biggest obstacles I have faced are getting leadership buy-in and the budget needed," says John Krogulski, a survey respondent and the technology compliance and security manager at the Wisconsin Center for Education Research. Too often, there is tendency for management to view the organization as being too small and of little interest to hackers, he says. "It is hard to get them to understand that all the [personally identifiable information] data we have is extremely valuable and being small actually makes us a bigger target."

Sometimes, budget holders can balk at additional spending on IR because from their viewpoint, a significant amount of money has already gone into security technology that should have been be able to prevent a security incident or breach, Ovum's Holt notes.

Our survey shows that 30% of organizations don't have personnel dedicated to the IR function, despite the heightened awareness of the need for them (**Figure 13**). Another 17% have just one individual dedicated to the task. At the other end of the spectrum, 18% of organizations have 10 or more IR specialists.

Previous Next
Table of Contents

Figure 12



Note: Maximum of three responses allowed
Data: Dark Reading survey of 100 IT and cybersecurity professionals in February 2020 and 150 in January 2019

The biggest challenge is getting buy-in and resources across the organization, says Jon Oltsik, an analyst at Enterprise Strategy Group. For an IR function to be effective, it needs to include stakeholders from across the organization and be thoroughly tested before an incident happens.

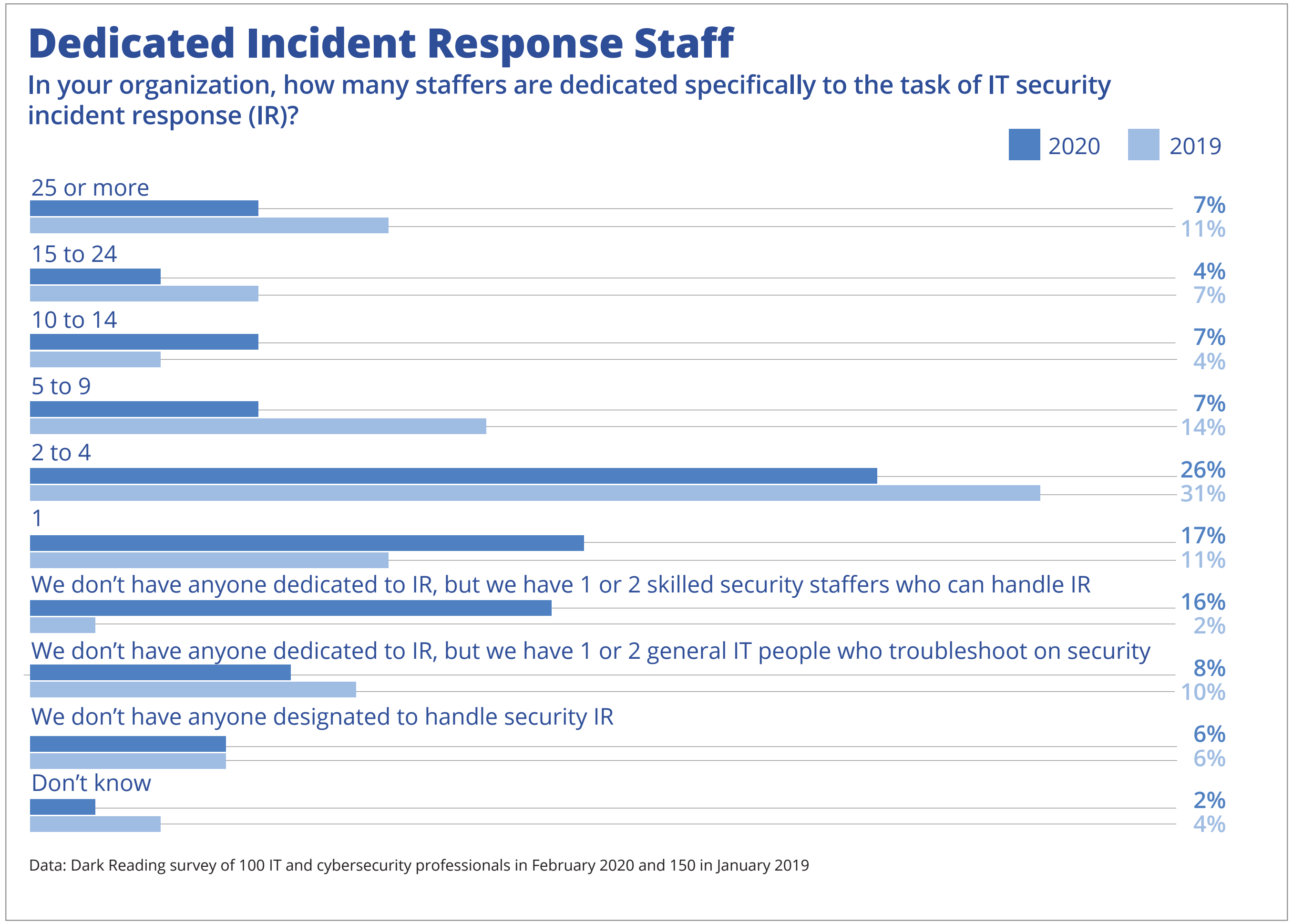
"Business, legal, HR, PR, etc., must all be involved," he says. Additionally, the plan should be formalized, documented, and tested often. "For large and highly targeted organizations, it's worthwhile to retain a contract with a leading IR firm who can parachute in when needed," he says.

Ideally, the IR function should be part of the SOC, Oltsik says. Many large organizations are building fusion centers that aggregate SOC functions, threat intelligence analysis, and IR. "There is no one leader of IR, per se," Oltsik says. "The security team will likely trigger the IR process, but it has to be a team effort after that. The most common mistake companies make is that they treat IR as a technology issue."

Dark Reading's 2020 Incident Response Survey shows that this is another potentially troublesome issue for many organizations. Fewer organizations this year (24% compared with last year's 31%) say they have a SOC, and fewer plan to build one internally (8%) compared with a year ago (12%) (**Figure 14**).

Finally, our data suggests that most organizations may be dangerously overestimating their ability to detect security incidents. Asked how long it took them, on average, to spot a potential compromise, a surprising 19% of

Figure 13



Data: Dark Reading survey of 100 IT and cybersecurity professionals in February 2020 and 150 in January 2019

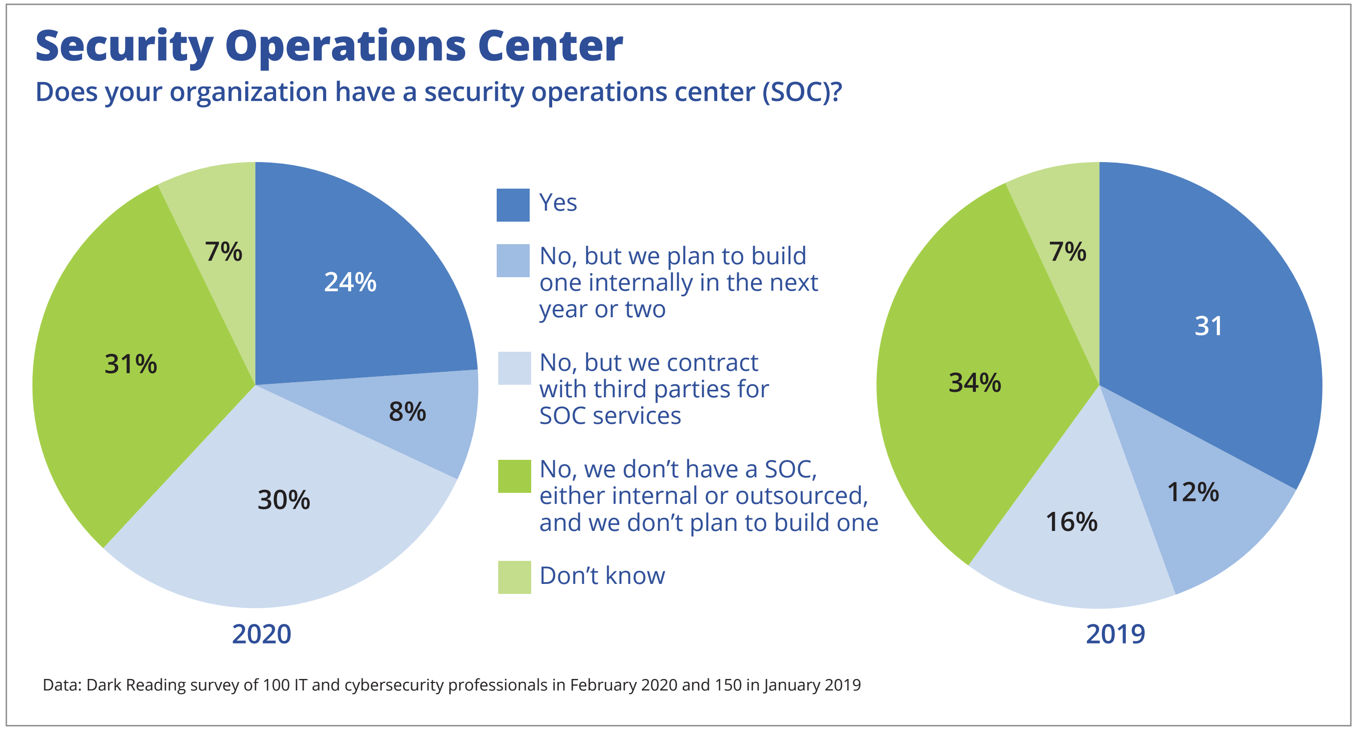
respondents claim they are able to detect it in real time (**Figure 15**). Another 21% say they detect most incidents within minutes of occurrence, and 25% claim to able to do it within hours. In other words, 65% of the respondents in our survey describe themselves as being able to detect and respond to a security compromise in well under a day. Sixteen percent say it takes them between one and two days to discover a new threat in their environment. A mere 4% admit that most security incidents go undetected for more than a week.

A high percentage of respondents describe themselves as being similarly quick at incident remediation. Sixty-two percent say they are able to remediate most incidents within minutes of their occurrence to within hours of occurrence, and 16% say they could do it within one and two days at most (**Figure 16**). Five percent say they need one week or longer to remediate most security incidents.

However, these IR and remediation times reported in our survey are much faster than those reported in studies that have analyzed actual data breaches, and they indicate a potentially serious disconnect between perception and reality.

Last year, FireEye found that 50% of organizations worldwide take 78 days or more to detect an attacker on their network. That number was actually a considerable improvement over the median of 101 days it used to take in 2017, but it is still much bigger than

Figure 14


Security Operations Center

Does your organization have a security operations center (SOC)?

Data: Dark Reading survey of 100 IT and cybersecurity professionals in February 2020 and 150 in January 2019

the detection times reported in our study. The gap is even bigger in the case of small and midsize companies. Infocyte last year found that these entities take an astounding 869 days on average to discover malware on their network.

Security experts consider dwell-time — the length of time it takes for an organization to detect a security incident after it first happens — to be an important IR metric. The idea is that the faster an organization is able to detect and mitigate a security issue, the better its chances of being able to limit damage. In recent years, many companies have considerably improved their ability to detect incidents quickly, but even so, attackers are often able to remain undetected on breached networks for weeks and even months.

Conclusion

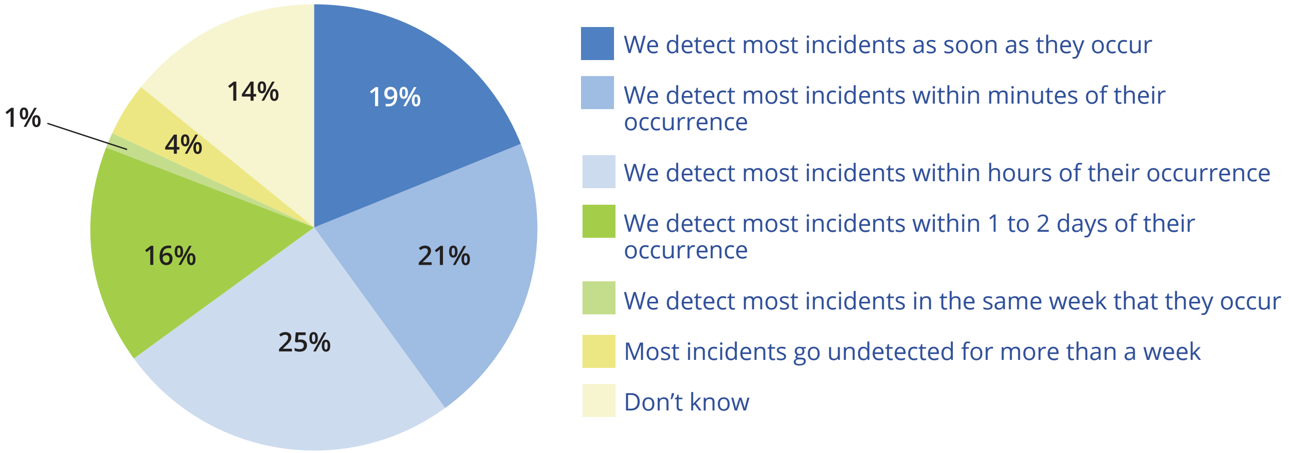
Enterprise awareness and attitudes toward incident response appear to be maturing. Compared with a year ago, more organizations perceive speed as critical to effective incident response and appear willing to devote more security resources to the function. Concerns and apprehensions over key IR functions such as incident scoping, log analysis, patch management, and false alerts have abated somewhat, but remain high nonetheless. A high-percentage of organizations also appear somewhat overly optimistic about the speed at which they can detect and respond to incidents.

APPENDIX

Figure 15

Length of Time Between Incidence and Detection of Potential Compromise

What is the length of time between the incidence of a potential compromise in your environment and the detection of that potential compromise?



Data: Dark Reading survey of 100 IT and cybersecurity professionals, February 2020

Like This Report?
Share it!

Like Tweet
Share

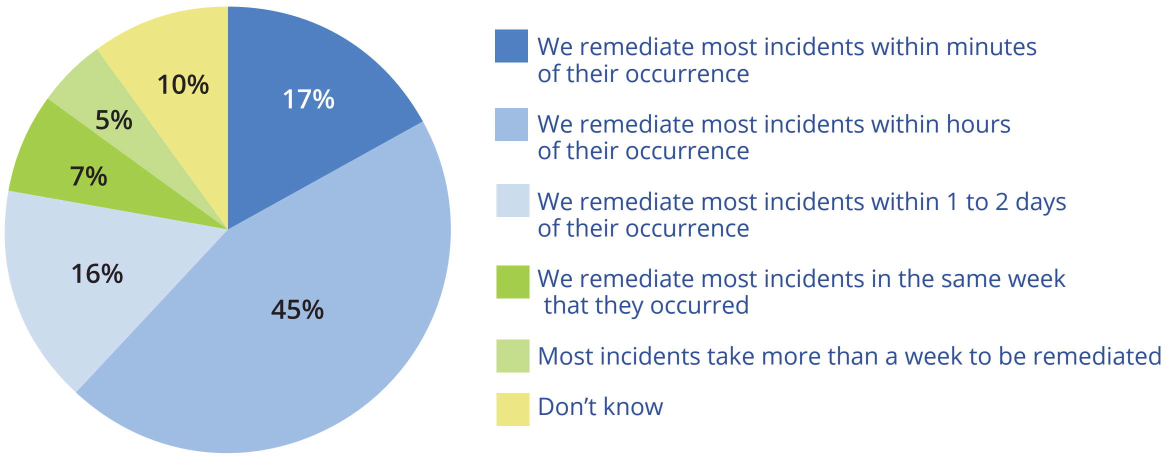
Previous Next

Table of Contents

Figure 16

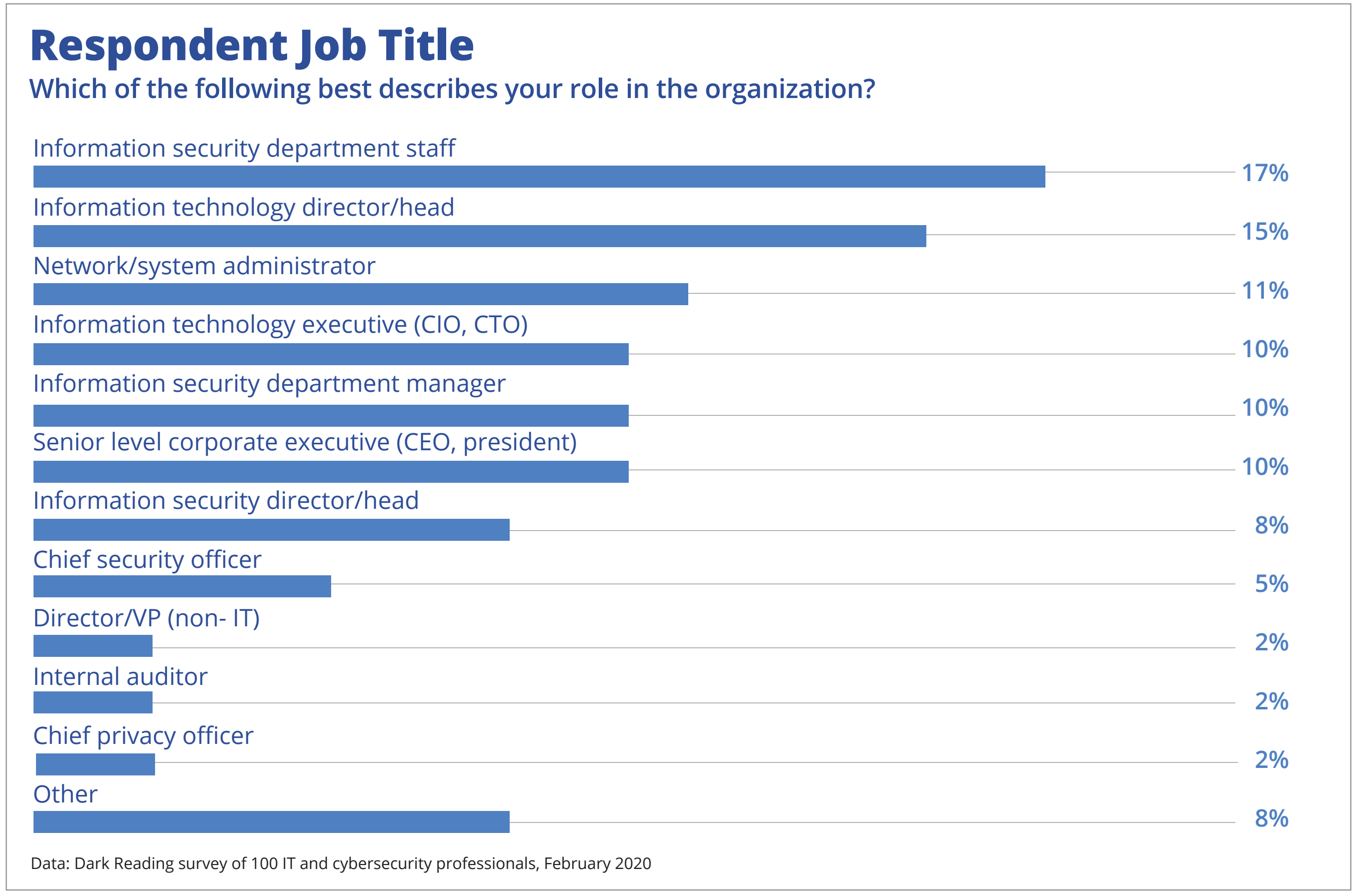
Length of Time Between Detection and Remediation of Potential Compromise

What is the length of time between the detection of a potential compromise in your environment and the remediation of that potential compromise?



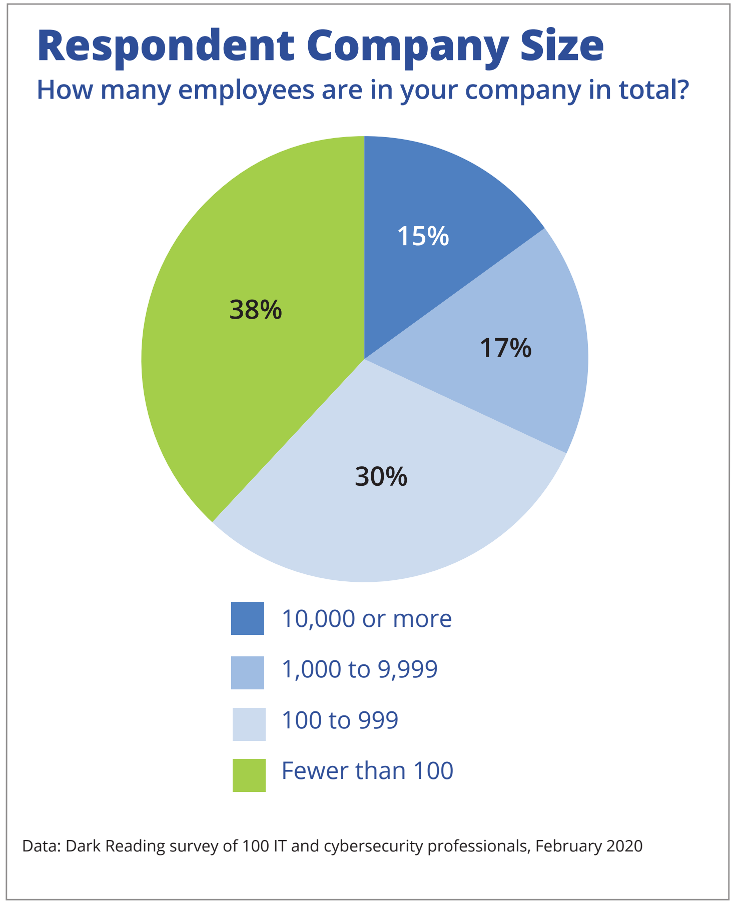
Data: Dark Reading survey of 100 IT and cybersecurity professionals, February 2020

Figure 17



Data: Dark Reading survey of 100 IT and cybersecurity professionals, February 2020

Figure 18



Respondent Company Size

How many employees are in your company in total?

Data: Dark Reading survey of 100 IT and cybersecurity professionals, February 2020

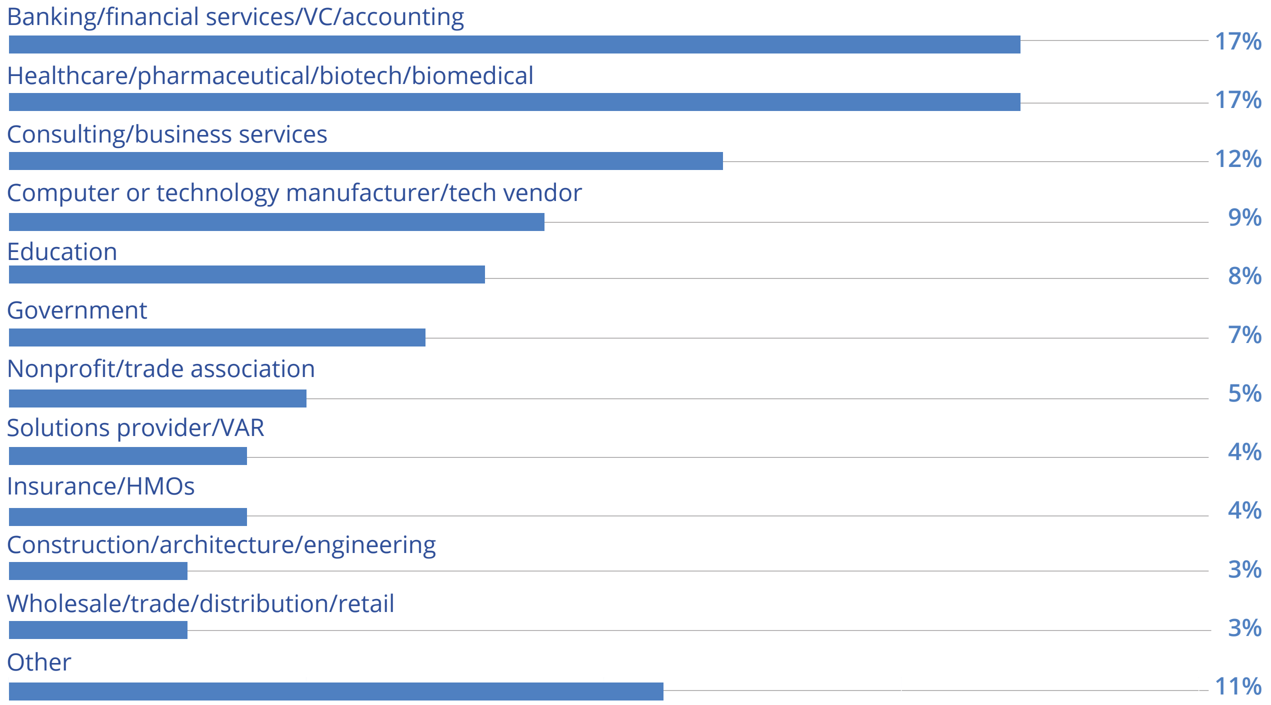
Previous

Table of Contents

Figure 19

Respondent Industry

What is your organization’s primary industry?



Data: Dark Reading survey of 100 IT and cybersecurity professionals, February 2020