Next

DARKReading CONNECTING THE INFORMATION SECURITY COMMUNITY
:: reports

May 2017

Surviving the IT Security Skills Shortage

Cybersecurity people are in high demand – and short supply. More than **80%** of organizations plan to keep security staffing levels the same or increase them in 2017, while only **14%** believe there are plenty of skilled security pros available. Here are some strategies for getting through the drought.

Sponsored by
ARCTIC WOLF

TABLE OF CONTENTS

Figures

Ericka Chickowski
Dark Reading Reports

Ericka Chickowski is a business and technology journalist who specializes in coverage of IT security, regulatory compliance, business alignment, project management, and IT employment. She specializes in explaining how technology trends affect real people. Her analysis and perspectives have appeared in dozens of trade and consumer magazines, including CIO Insight, Dark Reading, DevOps.com, Entrepreneur, and InformationWeek.

EXECUTIVE SUMMARY

Finding the right security talent to execute on an effective security strategy is a constant problem for organizations of all sizes. As the threat landscapes continues to evolve and the complexity of IT architecture grows, organizations need people who instinctually understand the threat tracking process, a skill that only comes with experience. They need cybersecurity professionals adept at using cutting-edge tools beyond traditional network perimeter defenses. And they need security leaders capable of communicating risk to their lines of business.

Dark Reading's 2017 Security Skills Survey examined the struggles around recruiting and retaining security professionals with these types of skills. Some of the findings include:

- 82% of organizations plan to keep security staffing levels the same or increase them in 2017
- Just 14% of organizations believe there are plenty of skilled security professionals available on the market
- Only 23% of IT managers say their security team is well trained and up to date on the latest technologies and threats
- 42% of organizations say their greatest security expenditure is on technology, while 33% say it's on the people who use it
- Organizations struggle most to find people with experience in their vertical markets and the soft skills needed to communicate risks to the business

RESEARCH SYNOPSIS

Survey Name Dark Reading Security Staffing Survey

Survey Date April 2017

Region North America

Number of Respondents 400 IT and IT security professionals. The margin of error for the total respondent base (N=400) is +/- 4.8 percentage points.

Purpose Dark Reading surveyed business technology and IT security professionals to discover issues related to IT security staffing.

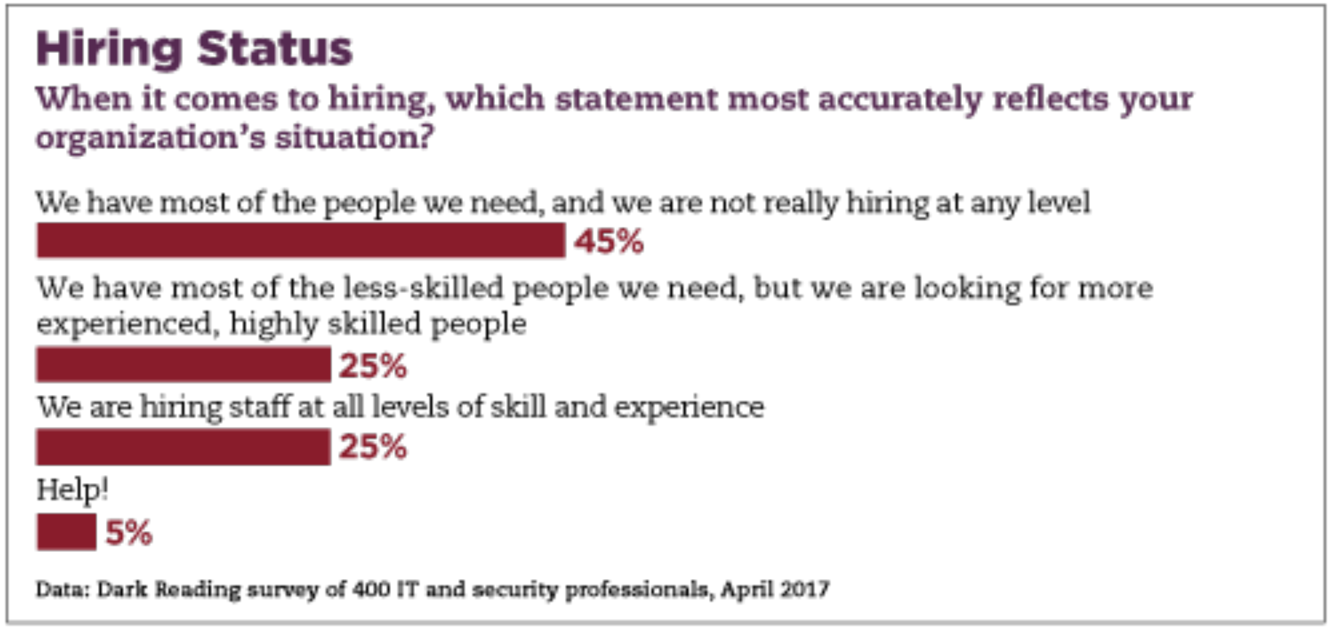
Methodology The survey queried decision-makers with job titles that involved IT or IT security at North American organizations with 100 or more employees. It asked them about their organization's IT security staffing status, plans, and challenges. The survey was conducted online. Respondents were recruited 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.

Previous Next

Table of Contents

Cybersecurity: Facing the Staffing Shortage Challenge

Figure 1



Data: Dark Reading survey of 400 IT and security professionals, April 2017

Security budgets remain on a steady upward trajectory in 2017, and many organizations continue to get the green light to bolster their security programs. But when it comes to putting an effective team in place, organizations of all sizes are struggling to find the right mix of talent they need to execute on their security strategies.

This problem has gained increasing attention from researchers in recent years as the industry scrambles to figure out why so many organizations continue to be hacked and compromised. The data indicates that skilled security specialists are hard to come by, many open security positions remain unfilled for months on end, and security professionals already on staff don't have sufficient training to get the most out of cutting-edge technology.

Results from Dark Reading's 2017 Security Staffing Survey confirm that recruiting and retaining specialized security skills challenges organizations of all sizes. While 55% of organizations surveyed are hiring security staff (see Figure 1), most hiring managers believe there is a skills shortage: Just 14% of decision-makers say that there are plenty of skilled security professionals available on the market (see Figure 2).

The Dark Reading survey data isn't unique. The 2017 (ISC)^2 Global Information Security Workforce Study conducted by Frost & Sullivan predicts there will be a global shortfall of cybersecurity workers of 1.8 million people by 2022. Meanwhile, a cybersecurity workforce study earlier this year by ISACA's Cybersecurity Nexus reported that more than one in four organizations take six months or longer to fill priority cybersecurity positions – and more than 40% of organizations said they received fewer than five applications for cybersecurity positions.

Yet, while virtually all experts agree that enterprises are having difficulty building and keeping effective security teams intact, the

Previous Next
Table of Contents

FAST FACT

35%

of respondents report a shortage of IT security professionals at every level.

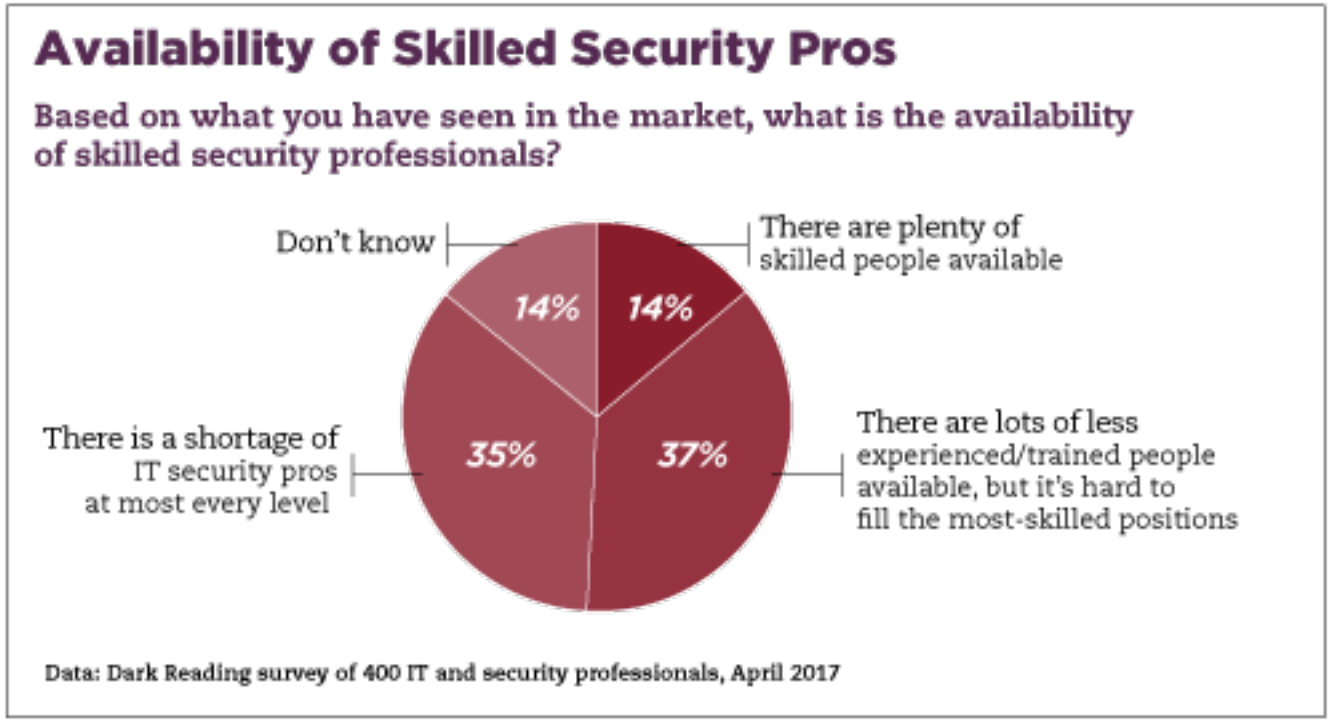
reasons behind the struggle are a matter of debate. Often referred to as the "security skills gap," the struggle to fill all security roles at an organization may be more nuanced than filling one singular gap. Many recruiters and security professionals explain that the challenges around building the right team are more complicated than a binary question of whether there are enough security candidates available for hire. It's not always a simple problem of too few bodies and too many empty seats.

"Is there a shortage? One hundred percent there is. Is it as big as some of these surveys say – a million-and-a-half people? I don't know," says Lee Kushner, president of cybersecurity recruiting firm L.J. Kushner & Associates. "There's definitely a talent shortage of quality information security professionals who are capable of solving emerging problems. It's not a shortage of general skill or average skill, it's a shortage of skills that can help companies solve their problems."

Quantifying the Skills Gap

Ironically, one reason for the hiring crunch in IT security skills is the rapid investment in IT security technology. According to the 2016 Dark Reading Strategic Security Survey, 82% of organizations planned to maintain or increase information security spending last year. The "Security Spending" chart that I see in the 2016 DR Strategic Security Survey is talking about "How spending on Info security will change in 2016" not 2017. And respondents to our staffing survey indicate that nearly four in 10 organizations spend a double-digit percentage of their overall IT budget on security. Yet, despite this high level of spending, most security departments are overwhelmed.

Figure 2



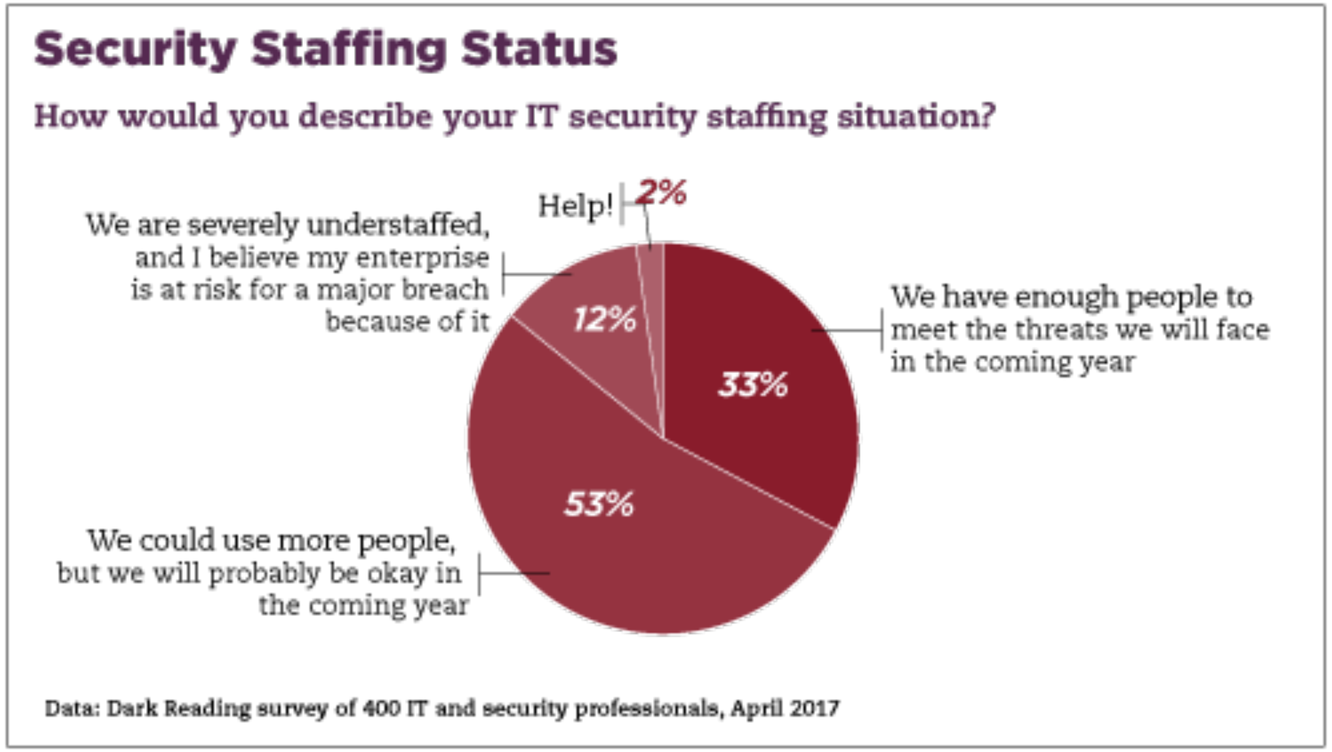
According to the Enterprise Strategy Group, 74% of organizations regularly ignore at least some security alerts because they can't keep up. In fact, ESG figures show that nearly one in three organizations ignore half or more of their security alerts. While organizations may be spending more than ever on detection technologies, their staffs aren't able to recognize or react to the data they receive.

However, lack of automation isn't the entire problem: Recent waves of security technology are peppered with machine learning and artificial intelligence technology designed to help enterprises detect security problems without human intervention. The trouble is that at some point in the process the success or failure of even the most advanced detection and response platforms comes down to the security knowhow of the people behind the dashboards.

Why is this next-generation technology faltering? First, automated systems continue to generate large numbers of false positives that require human analysis. Second, there's just no automating the power of human direction and decision-making.

"For the foreseeable future, cybersecurity is still going to be a human versus human battle, where machines can assist and augment human decisions, not replace them," says Mike Viscuso, CTO for Carbon Black, an endpoint security detection company.

Figure 3



Data: Dark Reading survey of 400 IT and security professionals, April 2017

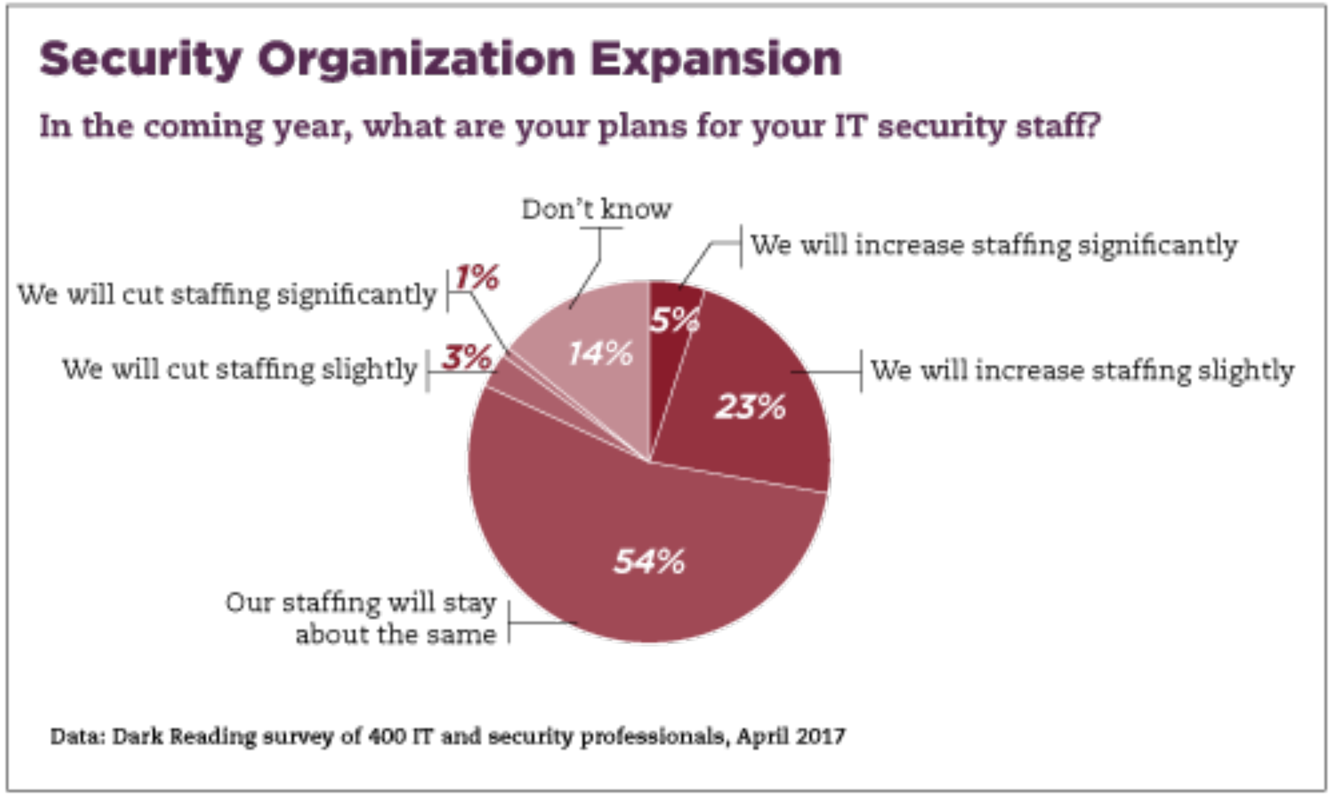
In a recent survey of more than 400 security researchers conducted by Carbon Black, 87% of these industry insiders said they think it will be more than three years before they trust AI to lead cybersecurity decisions. In some organizations, it will likely be much longer than that.

Other research indicates that automation is even less pervasive in small and midsize enterprises. A recent survey conducted by Vanson Bourne on behalf of Arctic Wolf found that just 3% of midmarket companies rely on automated prevention tools and scans to block attacks. Meanwhile, 92% depend on an internal staffer to do analysis and make security decisions.

Part of the problem is that, paradoxically, automated technology often requires a tremendous amount of expertise to deploy and maintain. Some products automate menial tasks, but they require higher-value skills to implement and even more expertise to interpret the resulting data.

This paradox likely explains why the Dark Reading survey found that few organizations – just 12% – would describe their organization as severely understaffed, and about half say they could use more people but will muddle through in the coming year (see Figure 3). The problem isn't a lack of bodies; it's a shortage of high-level technical skills. In fact, even though 82% of organizations will keep their staffing levels the same or add to staff this year, just 5% of organizations say they will increase staffing *significantly* in 2017 (see Figure 4). Similarly, only 5% of respondents reported they're looking to fill more than 20 positions (see Figure 5). Organizations aren't on massive hiring binges – they're just looking for advanced skills and talent that will make their defenses more effective.

Figure 4



Data: Dark Reading survey of 400 IT and security professionals, April 2017

This is where the true skills shortage rears its head. And it's probably why nearly three times as many respondents to the Dark Reading survey value prior experience over formal education when evaluating prospective employees' qualifications (see Figure 6).

One security practitioner at a consulting company who responded to the Dark Reading survey said, "Internally, we are quite well staffed, but numerous customers are seeking more and more security consultants like myself. The really experienced ones are hard to come by these days. Most lack the full set of skills required, and in-house training takes quite a bit of time to bring them up to par. There are very few REAL experts in the security field."

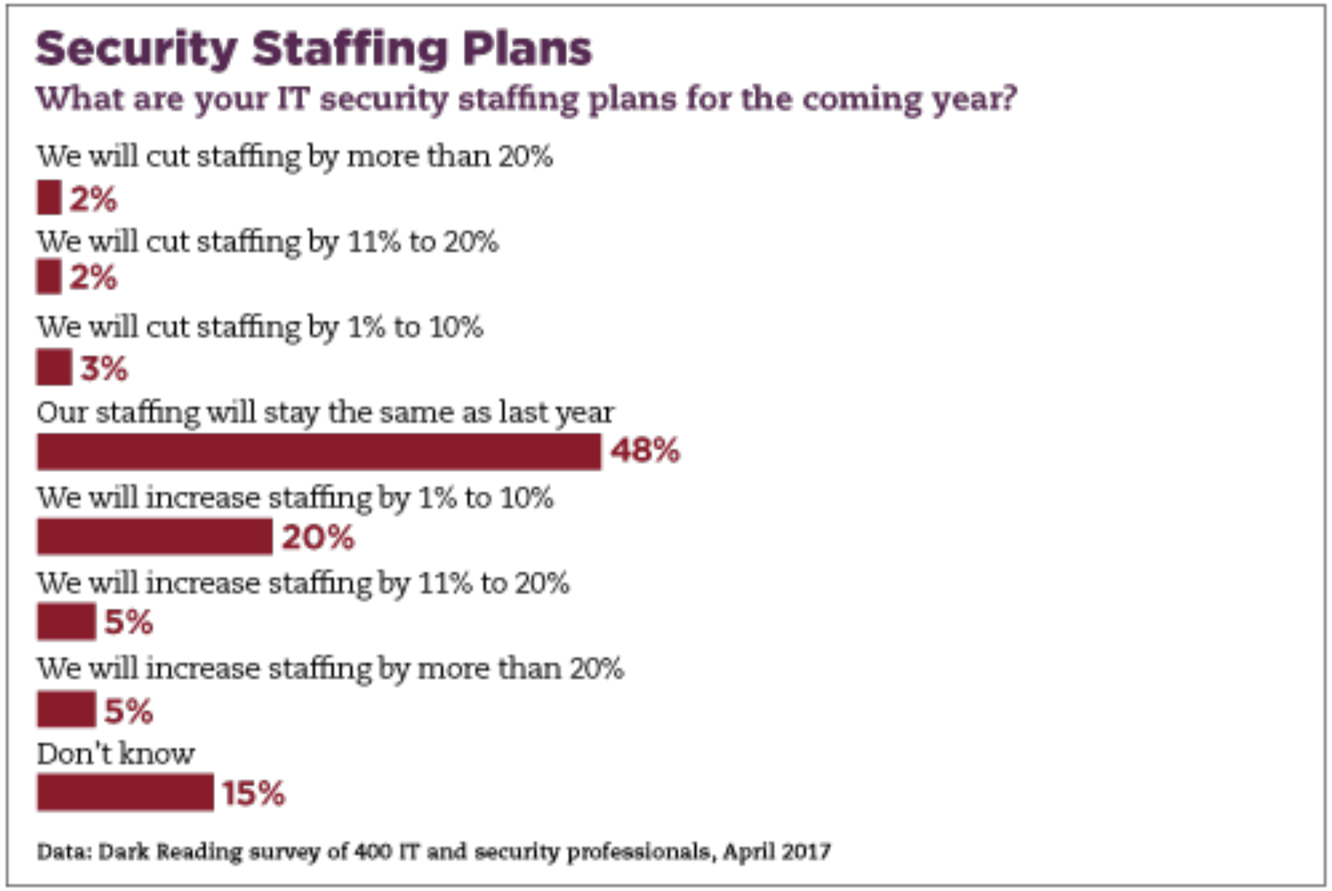
Gaps Vary by Specialization and Industry

Experts say that there isn't just one big "skills gap" in cybersecurity: there are multiple smaller gaps that vary by skill levels and other key variables. One of the biggest gaps is in vertical industries. Dark Reading survey respondents say that one of the most difficult attributes to find in prospective employees is experience in an organization's specific industry (see Figure 7).

It's very market-specific," says Al Lerberg, president of Cyber Security Recruiters. "Financial markets on the East Coast can be hiring a ton of people in information security because of a new regulation or something that they're trying to implement that's exclusive to the financial industry. Or something might have happened, like a breach in a certain industry – I saw that when the Target breach happened. I saw several retail companies start to build up their cybersecurity practices, bring things back in-house that were once overseas, and build up their incident response teams in reaction to what happened to Target."

There is also a strong demand for specific subdomain knowledge and specialization.

Figure 5



Security Staffing Plans

What are your IT security staffing plans for the coming year?

Data: Dark Reading survey of 400 IT and security professionals, April 2017

"So, you have these pockets of domain knowledge in this industry where there's subdomain expertise that's required in order to be effective or efficient in meeting current threats," says talent recruiter Kushner. These subdomains may include knowledge of specific security tool sets, such as SIEM (security information and event management systems) and incident response frameworks, or experience in very specialized roles, like threat intelligence and security architecture."

According to a recent CompTIA Security

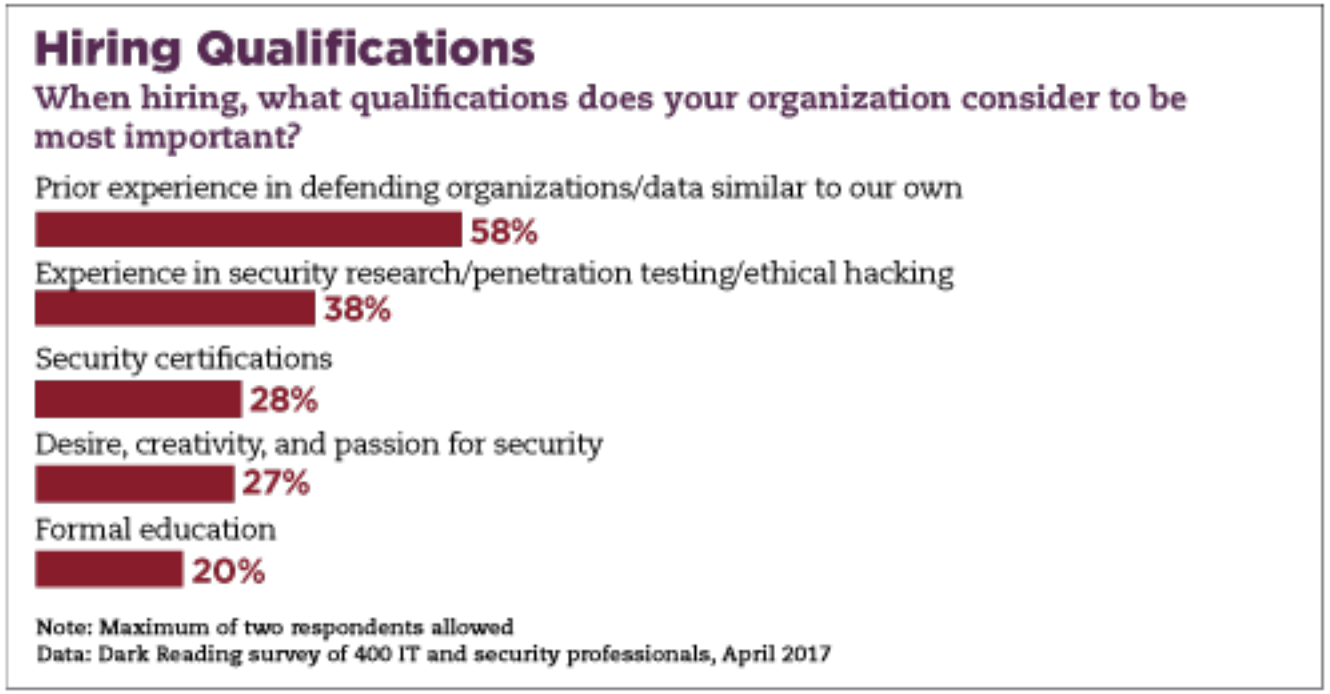
Skills study, the most difficult security roles to fill are cybersecurity analyst, security engineer, security manager, and security architect. In addition, specialized expertise in certain organizational processes – such as risk assessment, DevOps, and security knowledge surrounding new IT technology – are also in short supply.

For example, there may be lots of experienced security generalists on the market, but if an organization is searching for someone who can inspect internet of things sensors on a factory floor, the pool of available applicants quickly dwindles.

"We run into that all the time in information security as recruiters," Lerberg says. "I hate to call it the purple squirrel search, but that's kind of what it is. The talent pool is extremely small when you're looking for that type of specialized individual."

One respondent to the Dark Reading survey who works for a major multinational apparel brand says his company outsources "commoditized services" but struggles with the "more complex staffing challenges in the application, data, and cloud security spaces," he says.

Figure 6



Note: Maximum of two respondents allowed
Data: Dark Reading survey of 400 IT and security professionals, April 2017

Constantly Shifting Skill Requirements

The specialization is particularly acute because the skills required to keep up with current threats have become a moving target.

"The whole genesis of the security industry is based upon the evolution of talent over time," Kushner explains. "As new technology gets introduced, security concerns come with it. So that creates these continuous learning opportunities for security professionals – if they want to jump on them."

In the 1990s, the security skills gap was in firewall technology. Today, those skills are as meat and potatoes as can be, Kushner says. "Now everybody kind of has that," he says. "Then it moved to PKI and encryption. Then it moved to application security. Then threat intelligence. Then it was AWS and cloud security. Then it was continuous development/continuous integration and SecDevOps."

FAST FACT

52%

of IT and security professionals report it's difficult to find people with industry-specific experience.

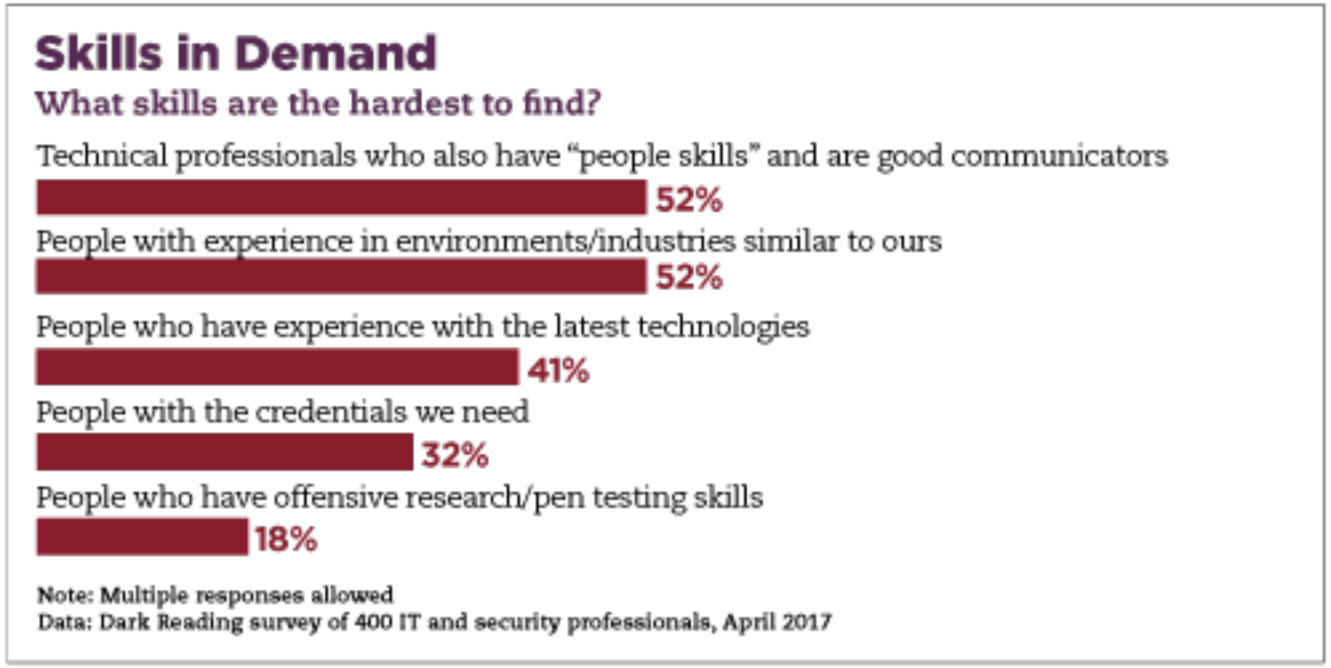
The opportunities are always in flux because technology changes so fast. As a result, the gaps in knowledge are a constantly moving.

Not only that, but the very concepts around what makes a good security practice are also evolving, says Lerberg. In some ways, security skills gaps are a function of the overall market maturing. At first, it was a matter of simply having a security program in place, he says. Organizations were scrambling to secure CISOs and justify the need for one. Then governance, risk, and compliance became critical as organizations struggled to get their arms around new cybersecurity regulations. From there, organizations recognized that compliance didn't guarantee security, so they began to seek out people who could ensure better cyber resilience.

"As organizations mature, the positions have changed. And so again, Level 1, 2, and 3 incident response people might not be in as high demand as architects and threat and vulnerability management experts who might be harder to find," Lerberg says.

For some organizations, years of IT security hiring waves may have contributed to push back from those who hold the purse strings.

Figure 7



Note: Multiple responses allowed
Data: Dark Reading survey of 400 IT and security professionals, April 2017

According to the Dark Reading survey, 33% of organizations say that it is more difficult to get management approval to increase security staffing today compared with a year or two ago (see Figure 8).

Keeping It Real

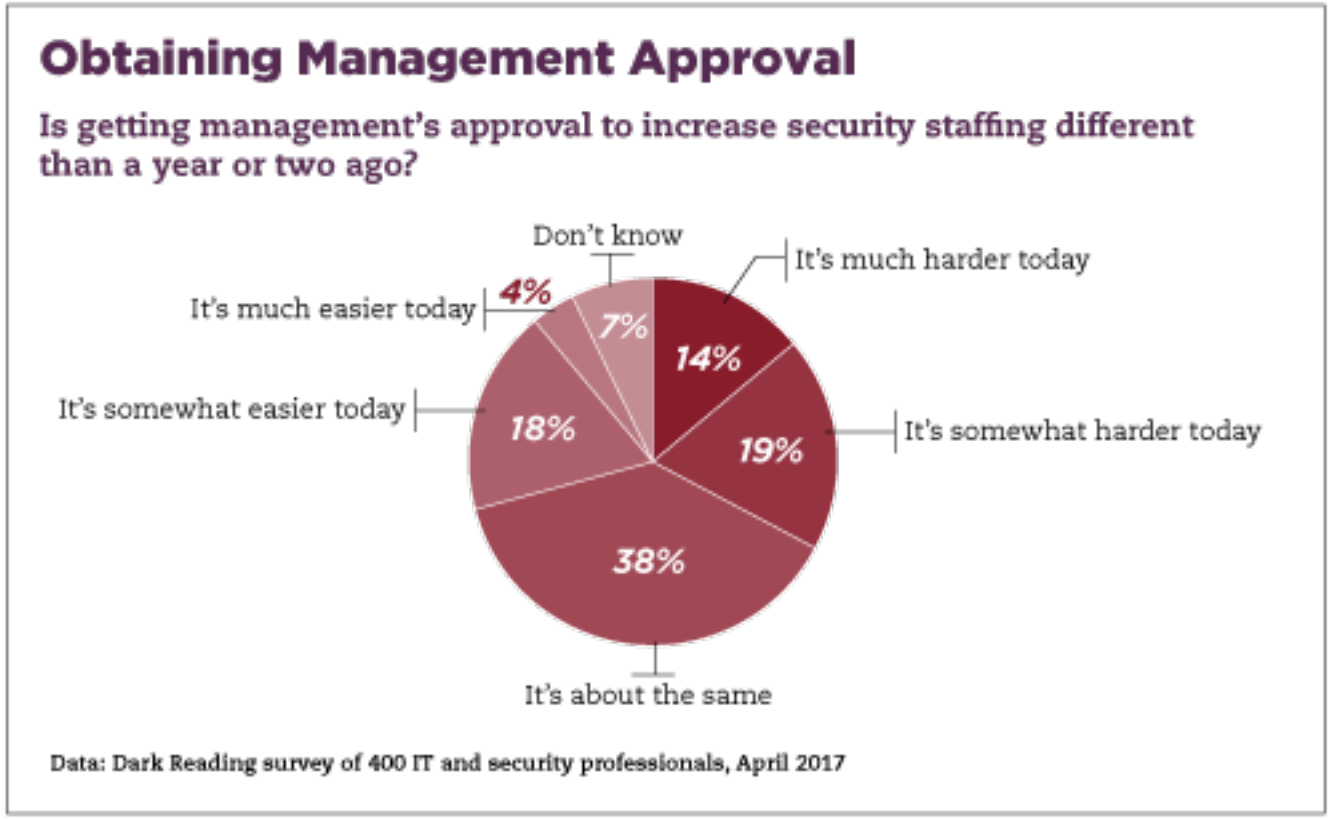
In a tough hiring market, recruiters and other security experts say that many organizations struggle to fill positions because they fail to honestly examine their recruiting and hiring practices and the attractiveness of the job and the organization. In some cases, they may not be allocating enough dollars toward compensation and training compared with their tech investments.

One respondent to the Dark Reading survey said bluntly, "Not enough budget is allocated to staffing and training IT security personnel. Unless we change our attitude towards IT security, we will continue to have a tough time combating cybercrimes." According to the Dark Reading survey, 42% of organizations say they're greatest security expenditure is on technology, while 33% say it's on staff.

"Many times, hiring managers find it difficult to attract people to their positions because their expectations about compensation or skill requirements are not in line with market realities," says Owanate Bestman, a recruiter for Barclay Simpson.

Kushner agrees, stating that the best organizations at recruiting security talent understand the nuances of market restrictions and are "honest with themselves about the appeal of their opportunity." Often he sees organizations stumble when they don't factor in the eccentricities of supply and demand in some security specialties. Less successful organizations tend to assign compensation for a role based on an industry average.

Figure 8



"But when they're looking for talent, they're not looking for industry-average talent," Kushner says, creating a mismatch in compensation that will inevitably leave a position vacant for an extended period. "It's akin to going to a really nice restaurant and expecting to pay for a meal at Friday's. If I go to Friday's, I expect I can get half-price appetizers, two-for-one deals, and I will probably get out of there for two people for 30 bucks. Whereas if I go to a higher-end restaurant, I'm probably not getting out of there for less than $100. I'm still getting the same 'meal,' but it's a much higher-quality meal."

There are two other crucial variables that are sometimes even more important to security job seekers than compensation: the novelty of the work and the culture of the organization. As Lerberg puts it, the two biggest questions he hears from job seekers are

Previous Next

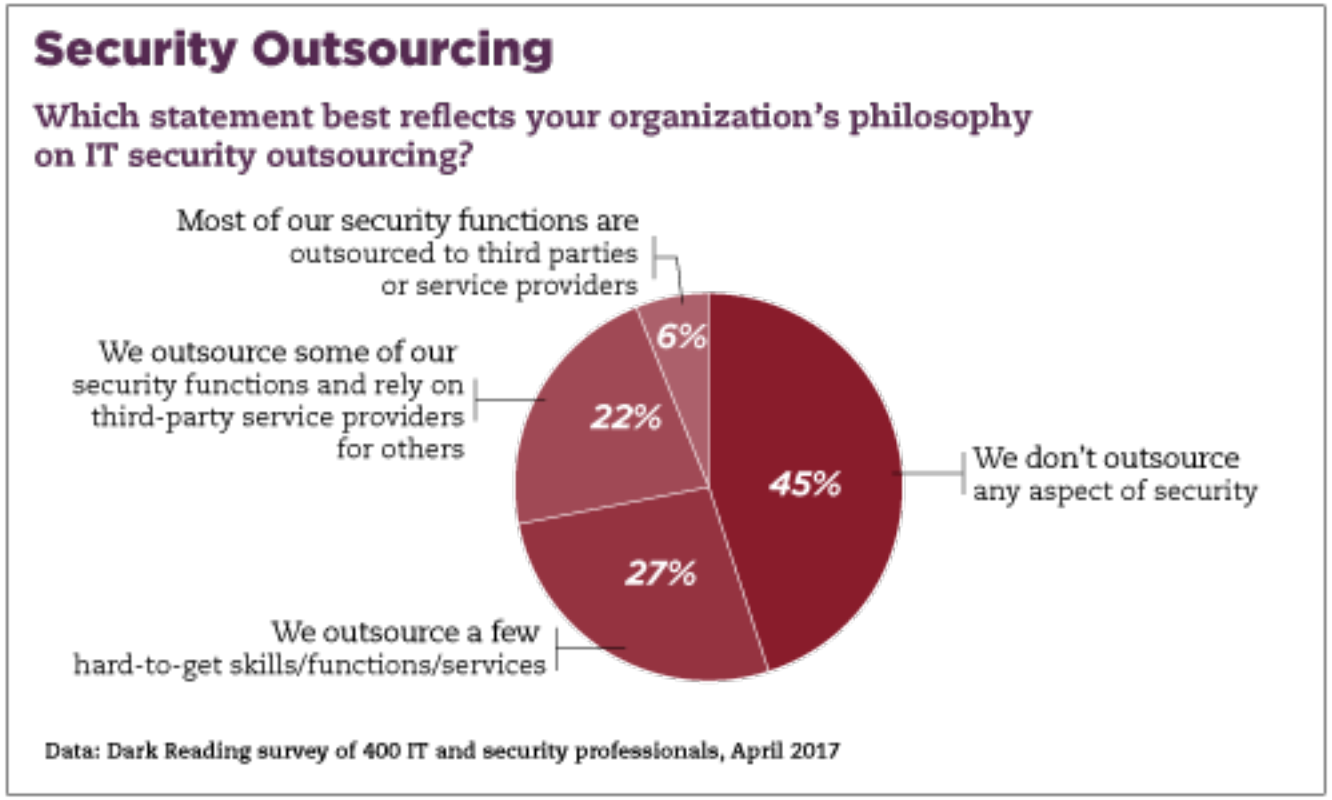
Table of Contents

FAST FACT

45%

of the companies in this survey do not outsource any aspect of seurity.

Figure 9



Data: Dark Reading survey of 400 IT and security professionals, April 2017

"What problems are they trying to solve?" and "What is the environment like?"

"I have found if the work is extremely interesting – new, cutting edge, a different approach to an old problem – then that gets someone more motivated than compensation or benefits," he says. This is one area where organizational self-honesty comes into play.

"I had this large bank come to me and they said, 'We're going to be just like Apple,' " Lerberg recalls. "I'm like, do you think Apple ever says, 'we're going to be just like this bank in Omaha?' I said, 'You might get people to buy into that, but chances are it's going to fall apart at some point.' "

In some cases, an organization can offset a ho-hum job with perks and benefits. But one thing it can't fake is security culture, experts say. Security pros seek out organizations that aren't going to approach security with a quick-fix approach or a checkbox compliance attitude. They know that those types of jobs lead to burnout and scapegoating.

"If they smell it's more of a compliance mentality or slapping-a-Band-Aid-on-something-to-fix-it attitude, then they're not as excited about the opportunity – and those organizations are going to have a very difficult time attracting top talent in the space," Lerberg says.

Addressing culture issues is no small feat and often requires intervention that starts at the top. But there are small changes that organizations can make to move the needle. For example, reconsider the reporting structure used for security staff, recommends Candy Alexander, a cybersecurity consultant and chair of ISSA's Cyber Security Career Lifecycle.

"People who work in information [security] or cybersecurity like to feel that they are making a difference and that the work they perform is valued. My advice for organizations would be to look at the reporting structure for the role. Don't bury the role within the IT group, like many do," Alexander says.

"Often, by placing the security role within IT, the first thing that happens is that resources are pulled from security and put onto IT tasks," Alexander says. "This subliminally sends the message to security staff: 'Your work is not important, we need to focus on keeping the lights on.'"

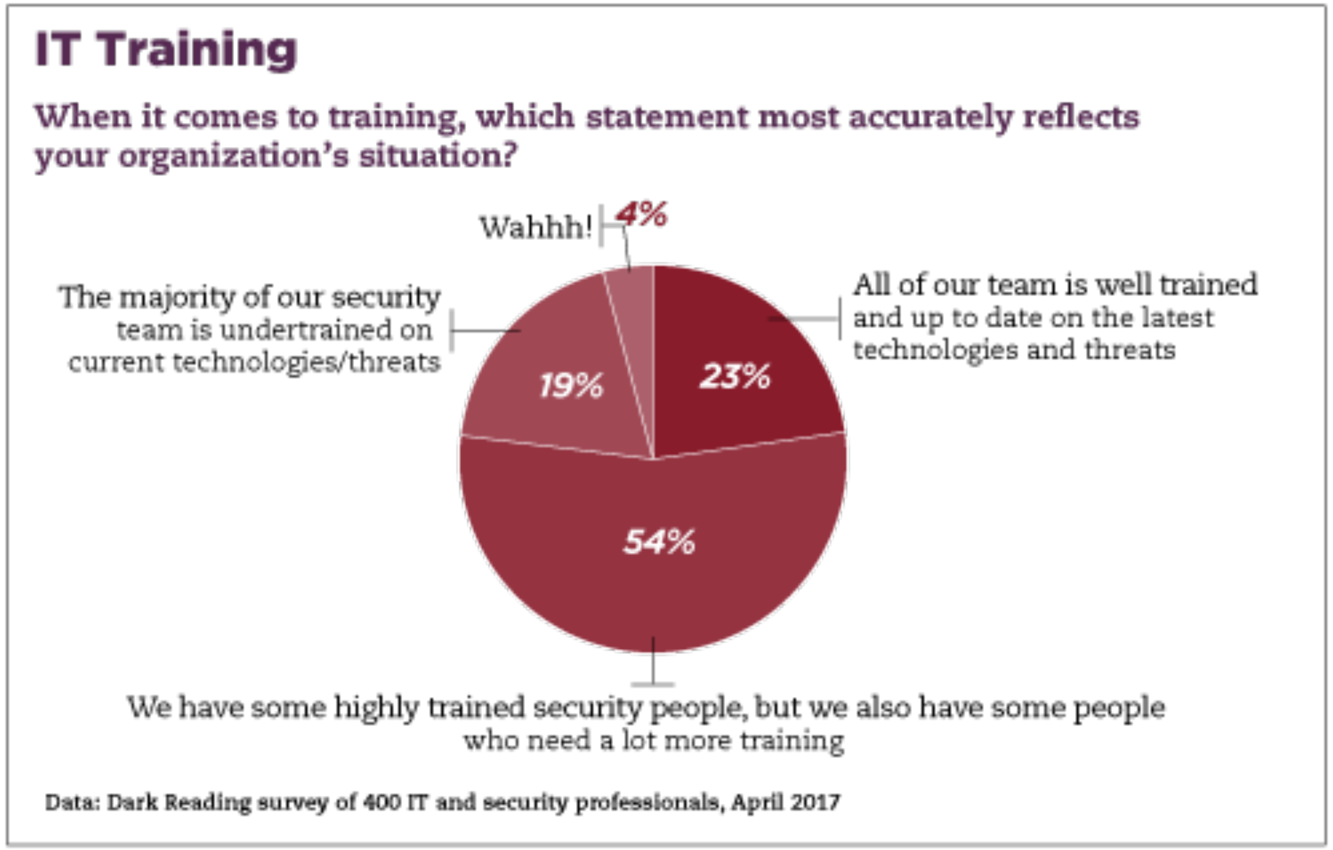
Enterprises should also consider how the hiring process itself may be signaling a lack of prioritization for security. In many cases, very qualified security staff might be scared off by the hiring bureaucracy and glacial pace of hiring processes.

"I can't tell you how many organizations have lost out on qualified candidates simply by dragging their feet in making an offer," Bestman says. "This industry moves so quickly that organizations must be able to cut through the bureaucracy if they want to hire top talent."

Could This Job Be Outsourced?

Organizations can avoid the difficulty of filling some security jobs by outsourcing them.

Figure 10



IT Training

When it comes to training, which statement most accurately reflects your organization's situation?

Data: Dark Reading survey of 400 IT and security professionals, April 2017

According to the Dark Reading survey, 27% of organizations outsource the hardest to find specialized roles rather than hiring for those positions (see Figure 9).

Other organizations are attempting to solve the skills shortage by training the people they already have, says Seth Robinson, senior director of technology analysis at CompTIA. He says that organizations may have to recognize that for certain positions or skills, it may not be possible to find the ideal candidate.

"And so organizations in the short term may have to think about bearing a little bit more of the burden when it comes to training – taking a candidate who might not be perfectly where they want them to be but being willing to invest in training to get them there," Robinson says. "In the medium and long term, I think organizations should continue to be proactive in working with educational institutions, with training organizations, to describe the skills they're looking for so that that supply can be properly built up."

Training is a huge weak spot for organizations, according to the Dark Reading survey. Fewer than one in four respondents describe their teams as well trained and up to date on the latest technologies and threats (see Figure 10). That's a big missing component in the skills challenge. Not only must organizations ensure that employees have the knowledge they need to perform at a high level, but the training itself can be a big carrot for recruiting and retention.

"My suggestion is to ensure that there is enough time and budget for training," Alexander says. "If organizations want to retain quality talent, they need to ensure that they provide those opportunities to gain the knowledge and stay sharp. Much like making investments in technology and business, if you make the right investments in staff, the payoff will be great."

Of course, many organizations fear that newly trained employees will walk out the door looking for greener pastures.

Larry Hurtado of Digital Defense has been engaged in building teams of security specialists – and retaining them – for years. One of the most important ways to manage the risk of attrition is to build systems that emphasize shared knowledge among team members, he says.

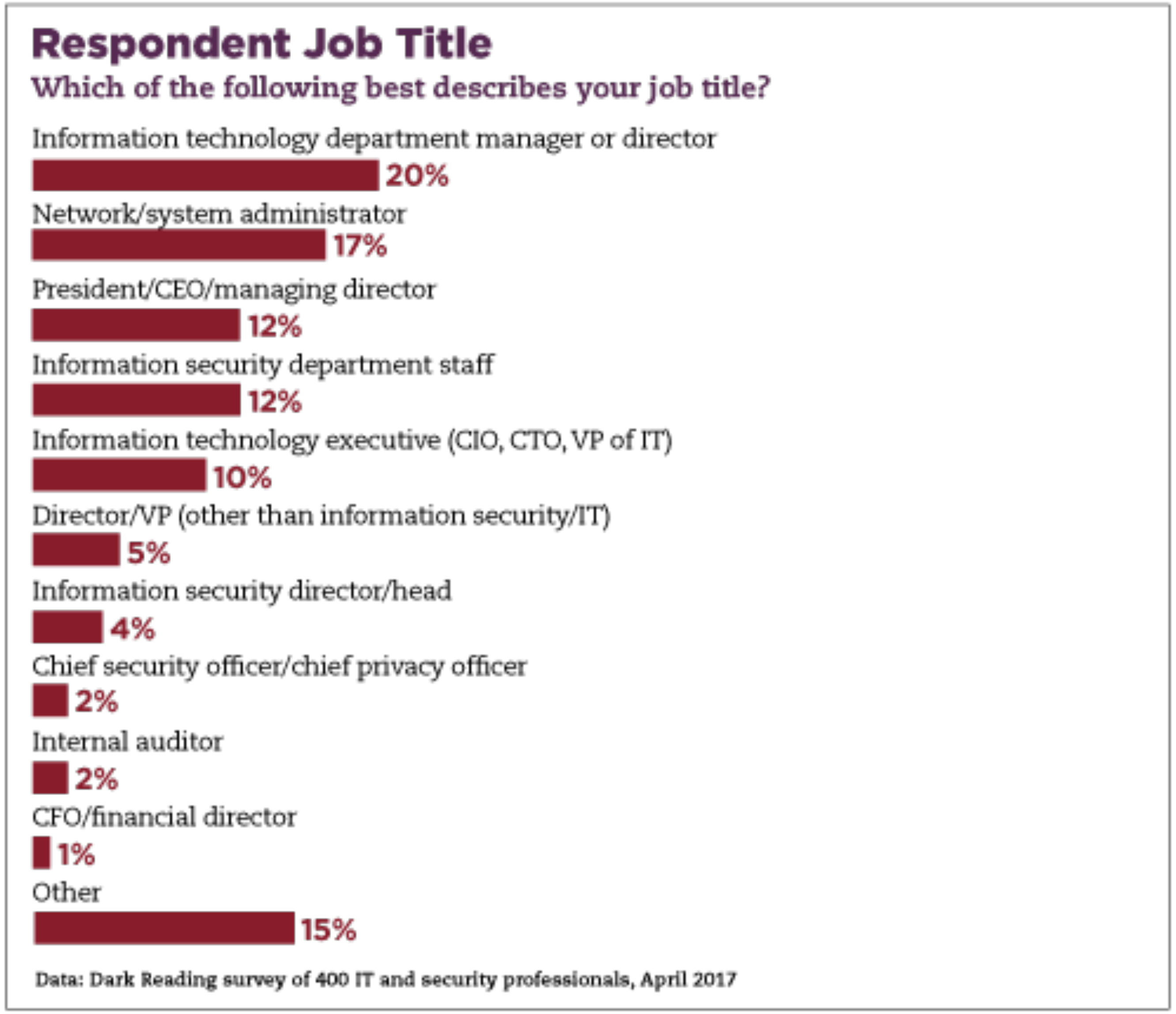
"If you can figure out a way to build that team, then it definitely helps you mitigate some of the risk," he says. "That approach allows us to bring in lower-skilled resources, put them to work, and build up that learning curve."

The toughest part of building a security team is not hiring, but retention, says Kushner. "I'll tell a lot of clients that the most important component they have in recruiting is retention," he says. "If you're looking at what's happening in the market, and you're looking at what new people require – and if you don't adjust that for people who are already on staff that are doing well for you – then shame on you."

It's not rocket science, says Alexander. Organizations must continue to pay people well. They've got to provide opportunity for growth through training and advancement. And most importantly, they should provide an encouraging environment that acknowledges they're making a difference for the organization. Those are the ingredients for creating a loyal workforce that really wants to stick around.

APPENDIX

Figure 11

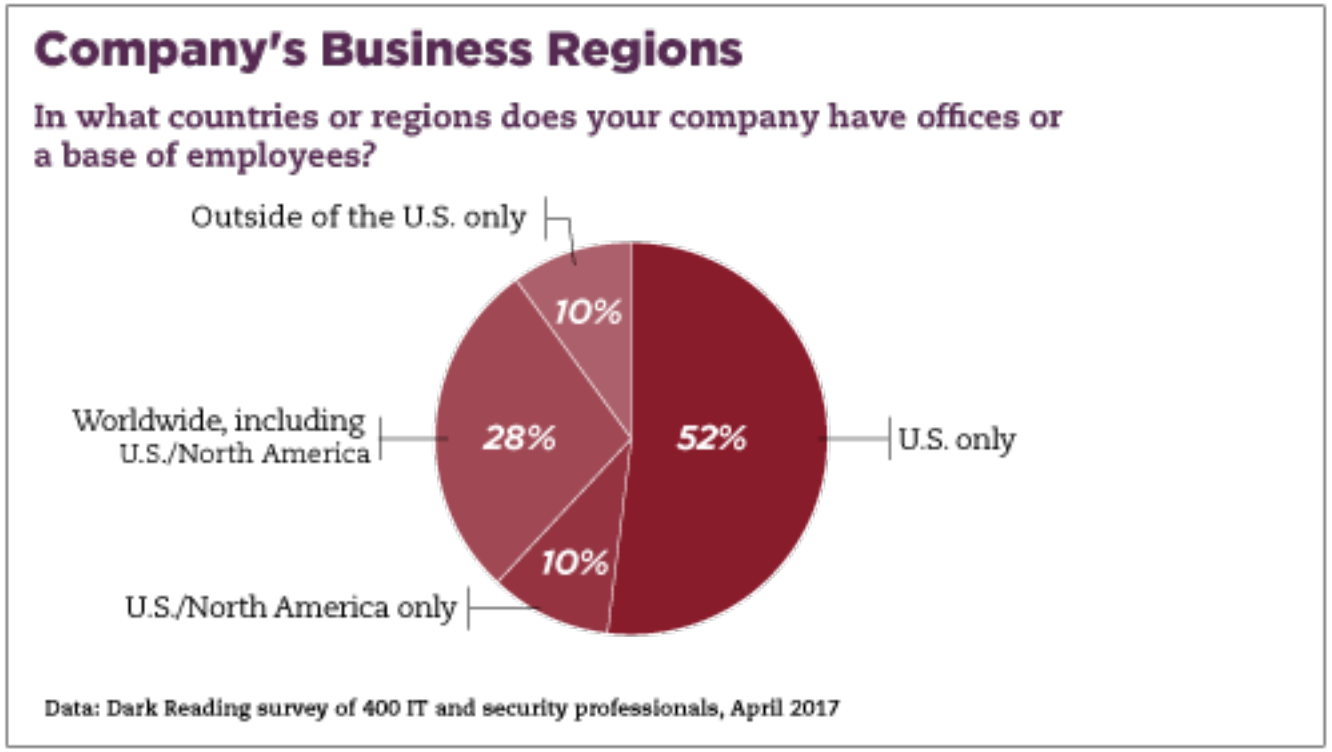

Respondent Job Title

Data: Dark Reading survey of 400 IT and security professionals, April 2017

Previous Next

Table of Contents

Figure 12



Company's Business Regions

In what countries or regions does your company have offices or a base of employees?

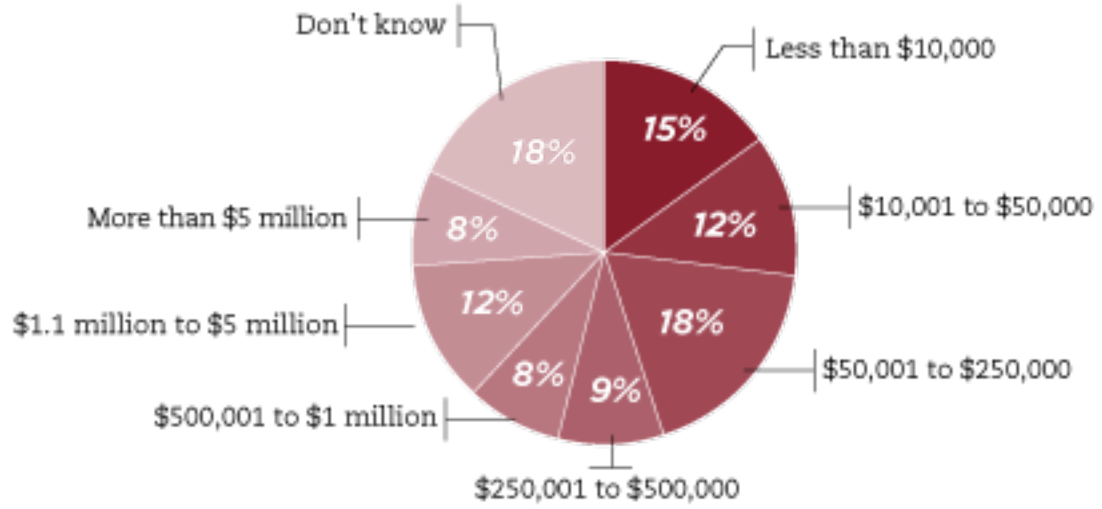
Data: Dark Reading survey of 400 IT and security professionals, April 2017

Previous
Next
Table of Contents

Figure 13

Annual IT Security Budget

Combining technology, services, and in-house staffing, what is your annual budget for IT security?

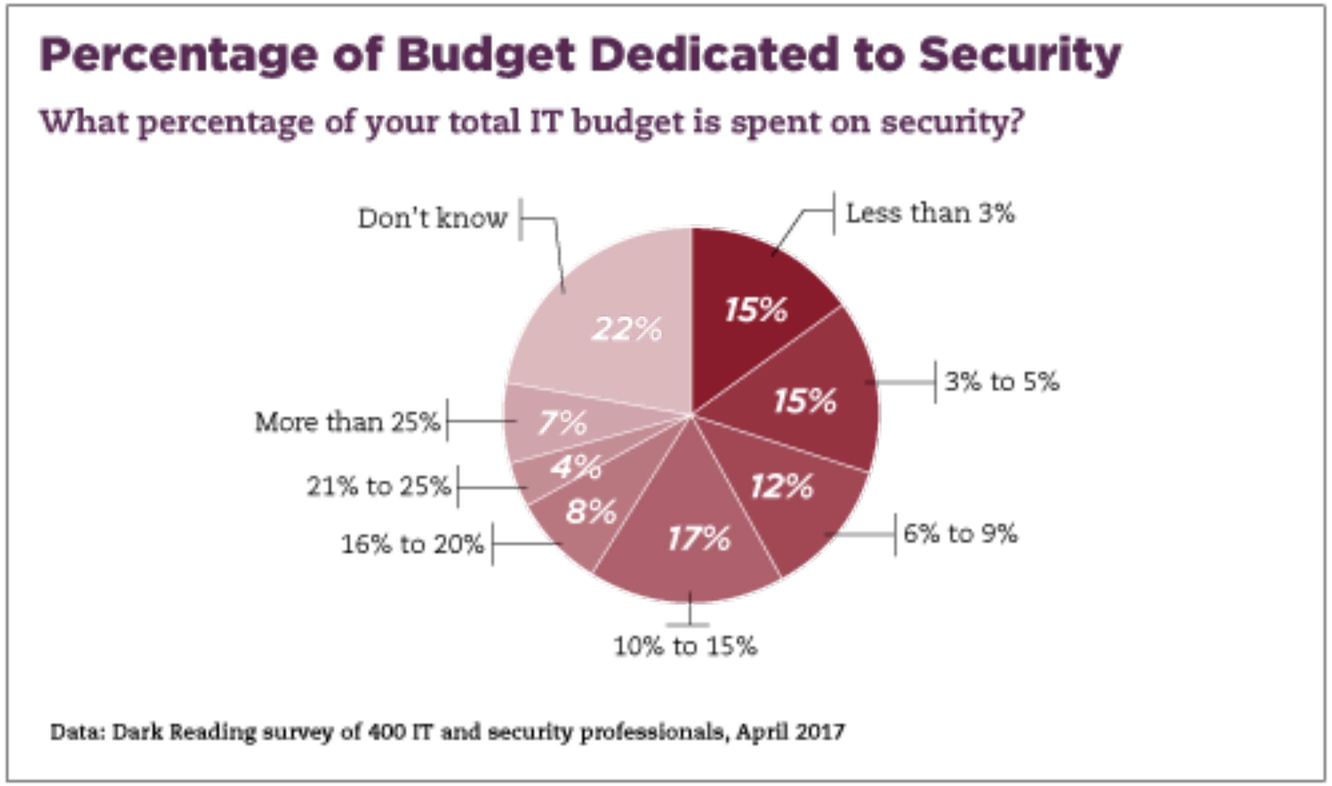


Data: Dark Reading survey of 400 IT and security professionals, April 2017

Previous Next

Table of Contents

Figure 14

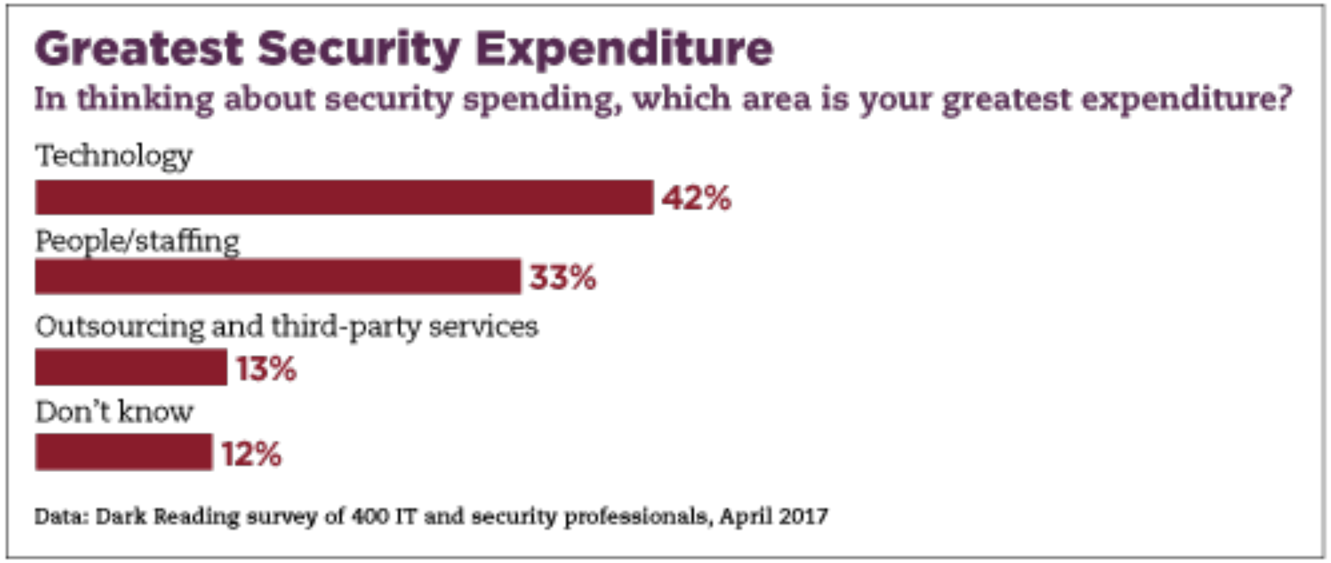


Percentage of Budget Dedicated to Security

What percentage of your total IT budget is spent on security?

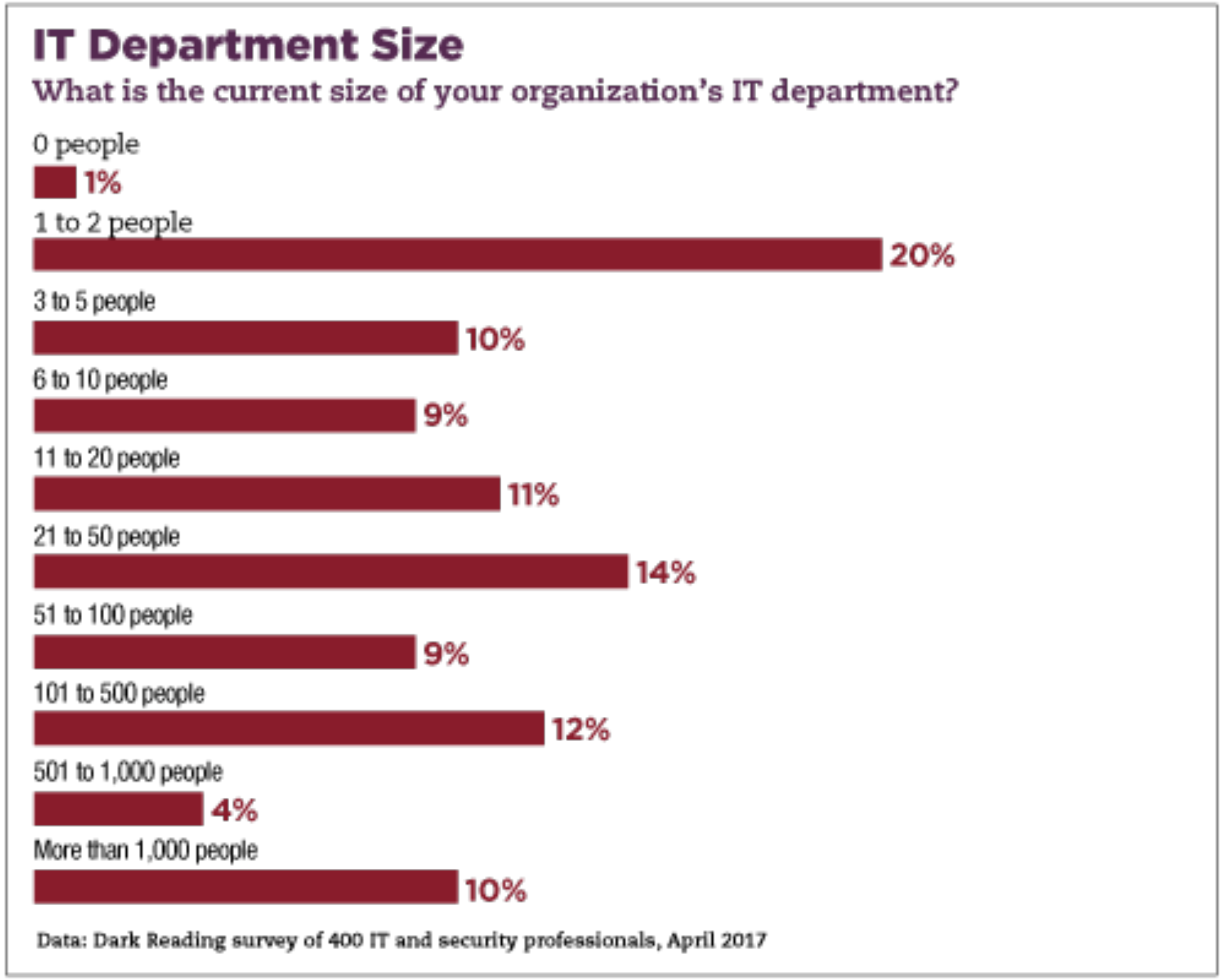
Data: Dark Reading survey of 400 IT and security professionals, April 2017

Figure 15



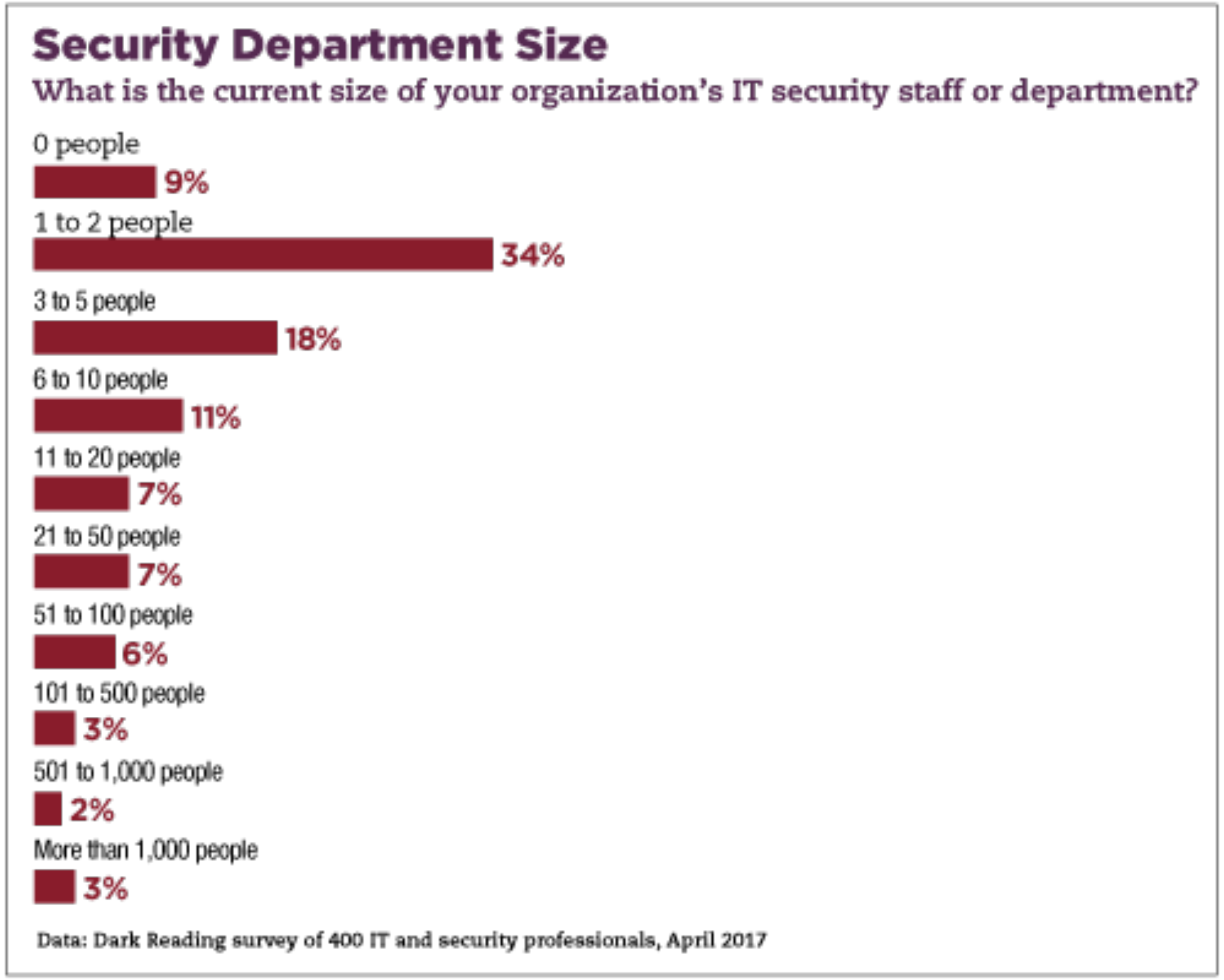
Data: Dark Reading survey of 400 IT and security professionals, April 2017

Figure 16



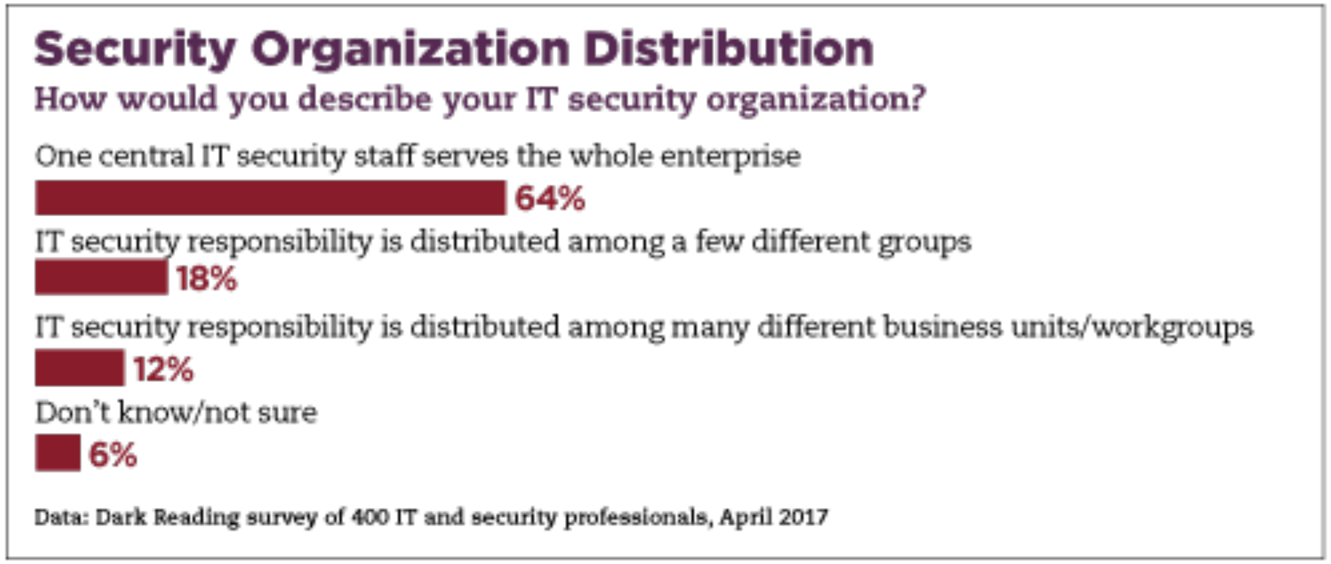
Data: Dark Reading survey of 400 IT and security professionals, April 2017

Figure 17



Data: Dark Reading survey of 400 IT and security professionals, April 2017

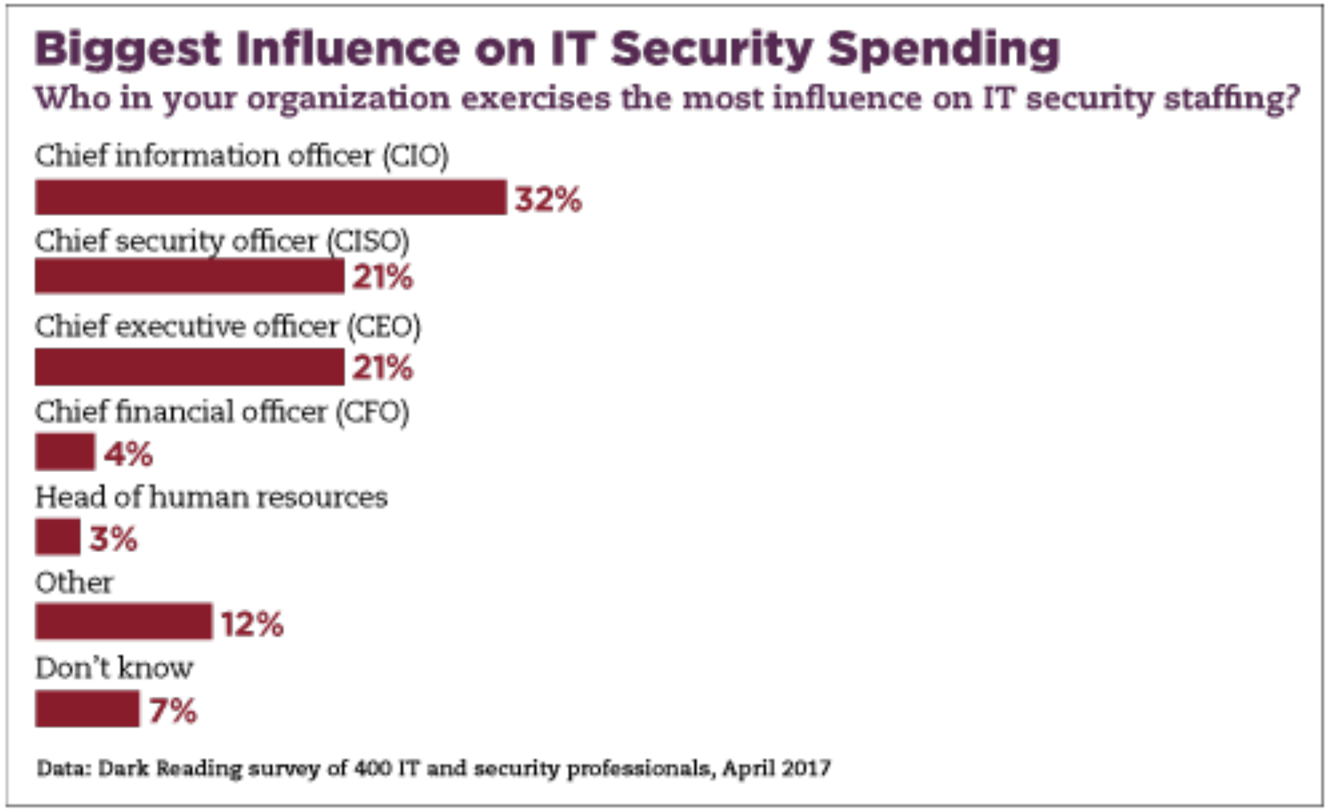
Figure 18



Data: Dark Reading survey of 400 IT and security professionals, April 2017

Previous
Next
Table of Contents

Figure 19

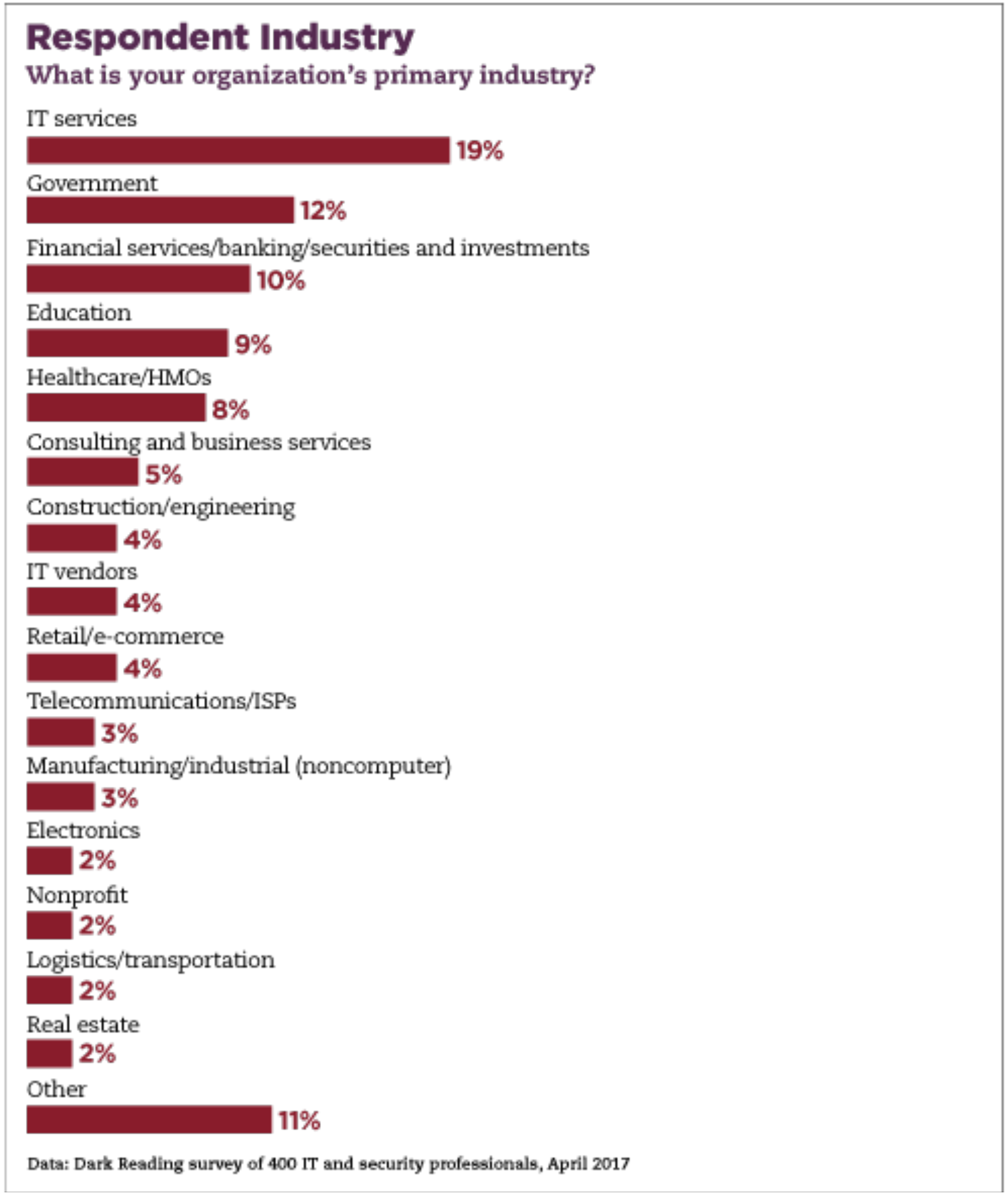


Biggest Influence on IT Security Spending

Who in your organization exercises the most influence on IT security staffing?

Data: Dark Reading survey of 400 IT and security professionals, April 2017

Figure 20

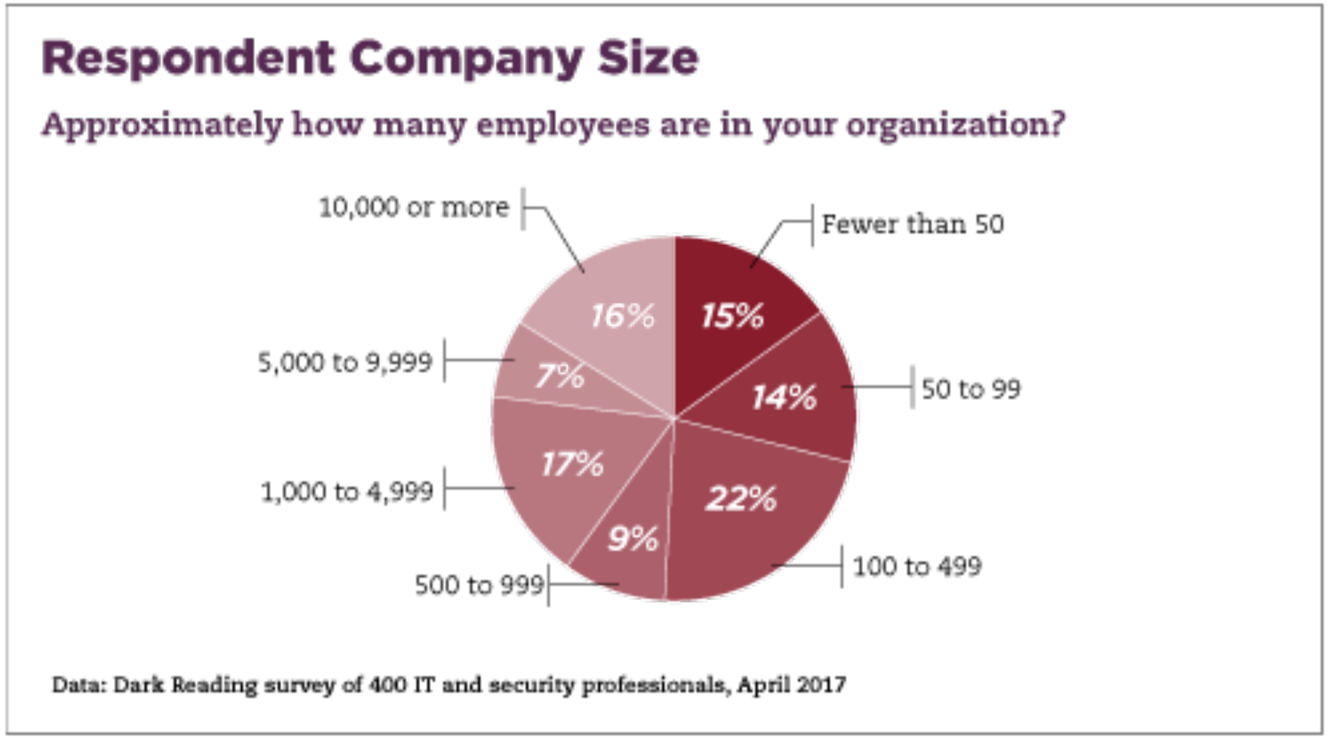


Respondent Industry

What is your organization's primary industry?

Data: Dark Reading survey of 400 IT and security professionals, April 2017

Figure 21



Respondent Company Size

Approximately how many employees are in your organization?

Data: Dark Reading survey of 400 IT and security professionals, April 2017

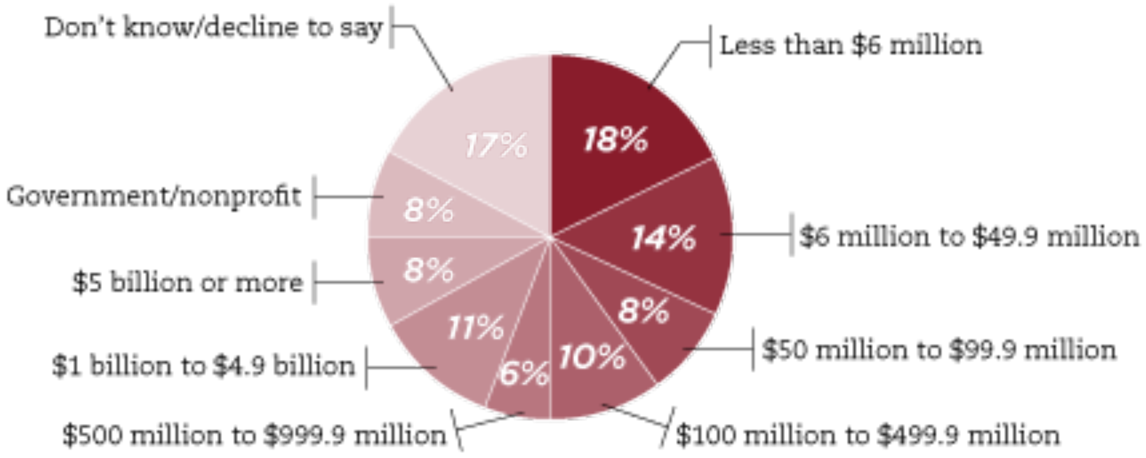
Previous

Table of Contents

Figure 22

Respondent Company Revenue

Which of the following dollar ranges includes the annual revenue of your entire organization?



Data: Dark Reading survey of 400 IT and security professionals, April 2017