black hat USA 2016

www.blackhat.com

July 2016

2016 Black Hat Attendee Survey

The Rising Tide of Cybersecurity Concern

In our second annual survey of top security professionals, Black Hat finds that the expectation of major breaches is even higher than last year.

Next

EXECUTIVE SUMMARY

In 2015, we set out to get an insider's view of the current cybersecurity environment by speaking to the most knowledgeable information security professionals in the industry. To achieve that goal, we surveyed one of the most security-savvy audiences in the industry: those who have attended the annual Black Hat USA conference. Black Hat, a forum that features some of the most advanced security research in the world, is a destination for discussion among top security minds, including leading ethical hackers, IT security management, and technology developers. The 2015 Black Hat Attendee Survey was the first of its kind, featuring responses from full-time IT security professionals — some two-thirds of whom had been credentialed as Certified Information Systems Security Professionals (CISSP).

The results of that study were alarming, as nearly three-quarters (72%) of respondents felt it likely that their organizations would have to deal with a major data breach in the year ahead. Approximately two-thirds of respondents said they did not have enough staff, budget, or training to meet those challenges. With so many security experts holding pessimistic attitudes about the coming year, it seemed as though the cybersecurity problem could not get much worse.

Unfortunately, it has. The 2016 Black Hat Attendee Survey results are in — and as a rule, the most expert security professionals in the industry are even more concerned this year than they were last year.

In the 2016 Black Hat Attendee Survey, the percentage of respondents who say they have "no doubt" that they will need to respond to a major security breach in the next 12 months (15%) is slightly higher than it was in 2015. The percentage of respondents who say it is "very likely" that they will face a major breach in the next year (25%) is up one percentage point. (See **Figure 1**.)

Despite these growing concerns, security departments are still facing an alarming shortage of resources. When asked if they have enough staff to face the threats they expect to see in the

ABOUT US

For more than 18 years, Black Hat has provided attendees with the very latest in information security research, development, and trends. These high-profile global events and trainings are driven by the needs of the security community, striving to bring together the best minds in the industry.

More information is available at: http://www.blackhat.com.

coming year, 74% of respondents said no — an even higher figure than in 2015. Sixty-two percent said they do not have enough budget to defend their organizations against coming threats. And 67% say they themselves do not have enough training to do their jobs — more than who expressed this concern in 2015.

Of all the problems that security organizations face, the shortage of skilled staff is the most acute. When asked the reason why security initiatives fail, "a shortage of qualified people and skills" was by far the top response (37%), outpacing a lack of management support (22%) and a lack of integration among security products (14%). And the pool of available security pros continues to shrink: only 11% of security professionals say they are actively looking to change jobs (down from 12% in 2015), and only 24% said they are even updating their resumes (down from 30% in 2015).

But a shortage of resources is not the only problem that enterprise security organizations face today. With staffing, budget, and training all in short supply, security professionals are being forced to prioritize their activities— but frequently, the priorities set by the business are not the priorities considered most important by security professionals.

When we asked security pros what they considered the most important threats and concerns that they face today, they overwhelmingly answered with two emerging threats: social engineering attacks such as phishing (46%) and sophisticated attacks targeted directly at their organization (43%). But when we asked those same security professionals how they spend their time, their top answers were measuring risk (35%), managing compliance with industry and regulatory requirements (32%), and troubleshooting security vulnerabilities in internally developed applications (27%). Clearly, there is a gap between the issues and challenges that security professionals consider the most concerning and the issues and challenges that they spend the most time working on — and that gap is larger in 2016 than it was in 2015.

In the pages that follow, we offer deeper details on the survey results and the significant challenges that security professionals face today — not only in defending against attacks from outside the organization, but in finding the time, people, and resources they need to maintain those defenses.

SYNOPSIS

RESEARCH

Survey Name The 2016 Black Hat Attendee Survey

Survey Date June 2016

Region North America

Number of Respondents 250

Purpose To gauge the attitudes and plans of one of the IT security industry's most experienced and highly-trained audiences: attendees of the Black Hat conference.

Methodology In June 2016 Dark Reading and Black Hat conducted a survey of the Black Hat USA conference attendees. The online survey yielded data from 250 management and staff security professionals, predominantly at large companies, with 60% working at companies with 1,000 or more employees.

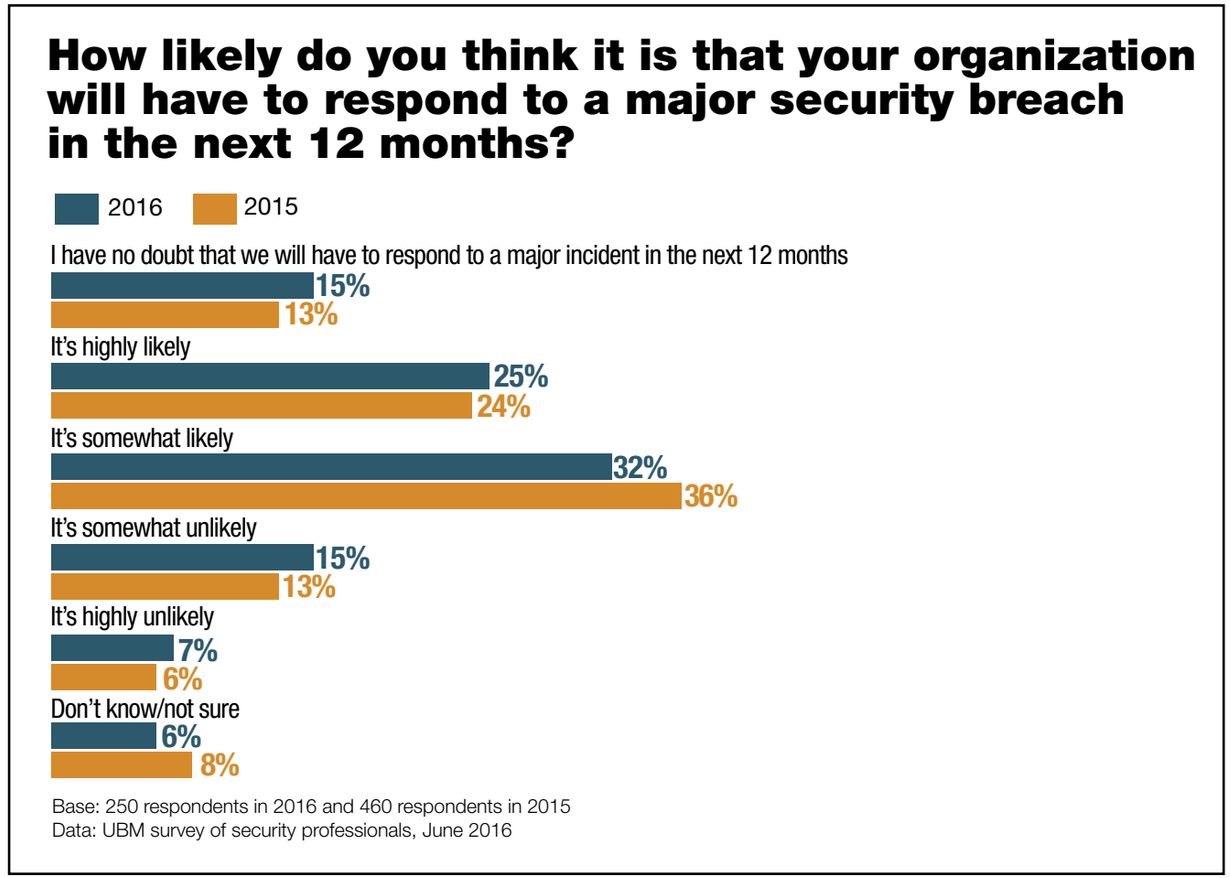
The greatest possible margin of error for the total respondent base (N=250) is +/- 4.5%. UBM was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices

Cybersecurity in Crisis

Security professionals fear they are losing the war against cybercrime — and the intensity of that fear is growing. In this year's Black Hat Attendee Survey, nearly three-quarters of security pros (72%) said they think it likely that they will have to respond to a major data breach in the next 12 months. Fifteen percent said they have "no doubt" that a major breach will occur — up from 13% in 2005. Twenty-five percent said it is "highly likely"— up from 24% last year.

There is good reason for this concern. Despite record levels of spending — Gartner estimates that businesses spent some $75.4 billion on security technology last year — the incidence of breaches continues to grow. Risk Based Security's Data Breach QuickView Report cited 3,930 incidents in 2015, representing more than 736 million records — all-time highs both for incidents and records. And the annual Ponemon Cost of a Data Breach report found that the average cost of a major data breach has jumped past $4 million per incident — a 29% increase since 2013 and 5% increase over last year.

Figure 1



By almost every measure, the cybersecurity problem is worse this year than it was the last.

Why are the enterprise defenders losing ground? The chief concern is a lack of resources. In the 2016 Black Hat Attendee Survey, nearly three-quarters (74%) of respondents said they

feel they do not have enough security staff to defend their organizations against current threats — even more than in 2015. Nineteen percent said they are "completely underwater" when it comes to staffing. (See **Figure 2**.)

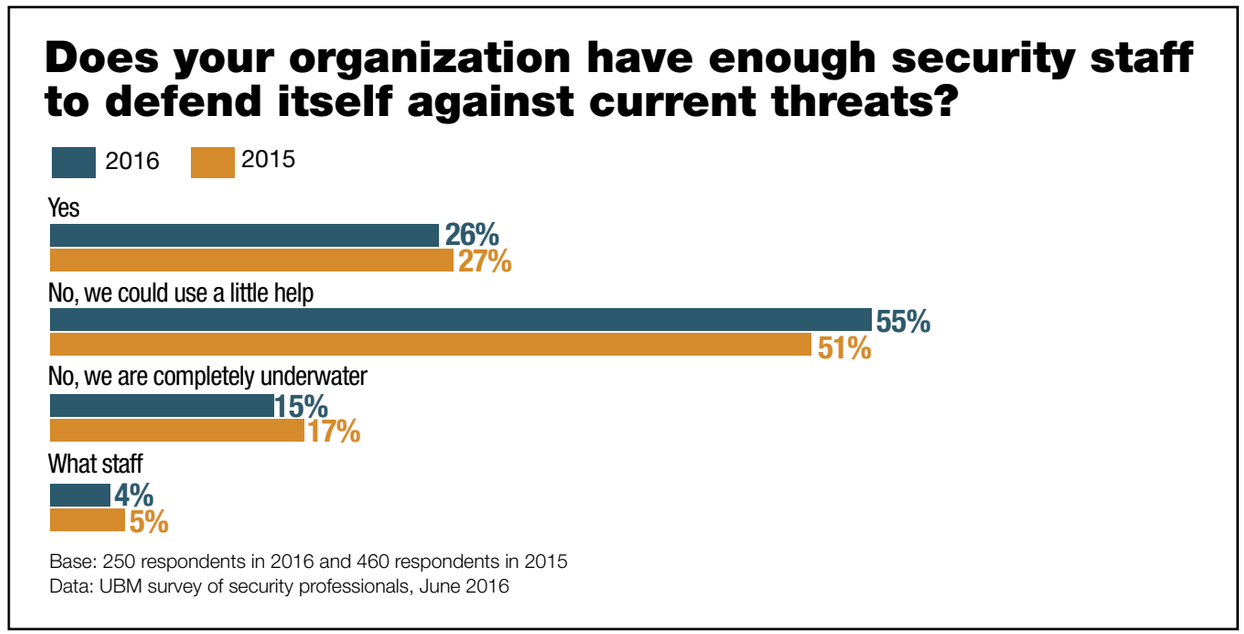
Funding also continues to be a problem. Despite record spending by the industry in 2015, some 63% of security professionals who responded to the survey in 2016 say their departments do not have enough budget to defend their organizations against current threats. Twenty percent said they are "severely hampered" by a lack of funding.

Training is also a major resource issue in security. In our survey, more than two-thirds of respondents (67%) said they feel they do not have enough training and skills they need to perform all of the tasks for which they are responsible — up from 64% last year. Ten percent of respondents said they feel "ill-prepared" for many of the threats and tasks they face each day.

This shortage of resources is the primary reason why IT security efforts continue to come up short, according to the Black Hat Attendee Survey responses. When asked why security initiatives fail, some 37% of respondents said a shortage of qualified people and skills is the culprit— the number one answer. A lack of commitment and support from top management was the second-most frequently cited response with 22%. (See **Figure 3**.)

While security teams are struggling with a lack of resources, the attackers continue to improve their game. In our survey, security professionals ranked social engineering as their most frequently cited concern (46%). Sophisticated and targeted attacks were the second most cited concern (43%). The growing use of ransomware by attackers was cited as the most serious new threat to emerge in the past 12 months (37%), while social engineering attacks on specific individuals was rated the number two emerging threat (20%). (See **Figure 4**.)

Figure 2

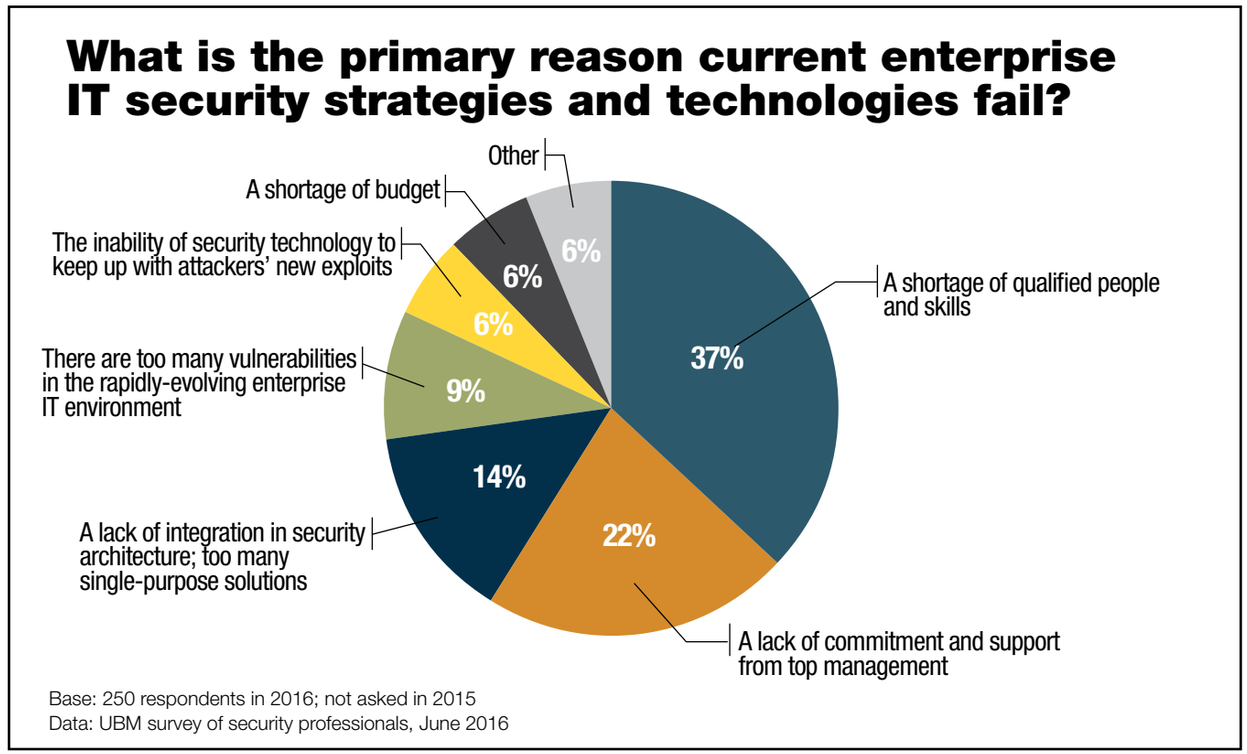


But external attackers aren't the only thing that keeps security professionals awake at night. When asked to identify the weakest link in the IT security chain, 28% of security pros cited end users who violate security policy, making this the top response in our survey. Seventeen percent cited "a lack of comprehensive security architecture and planning that goes beyond firefighting"— a clear indication that many security pros find themselves reacting to emergencies, unable to find the time they need to comprehensively evaluate their overall defense strategies. (See **Figure 5**.)

The Incredible Shrinking Skills Market

Of all the problems and challenges cited in the 2016 Black Hat Attendee Survey, the shortage of security skills is the most critical. While budgets and training continue to be major issues, 74% of respondents said they do not have enough people to manage the threats they face today. These results are supported by Frost & Sullivan in the latest ISC2 Global Information Security Workforce Study, which predicts that there will be a worldwide shortfall of over 1.5 million information security professionals by 2019.

Figure 3



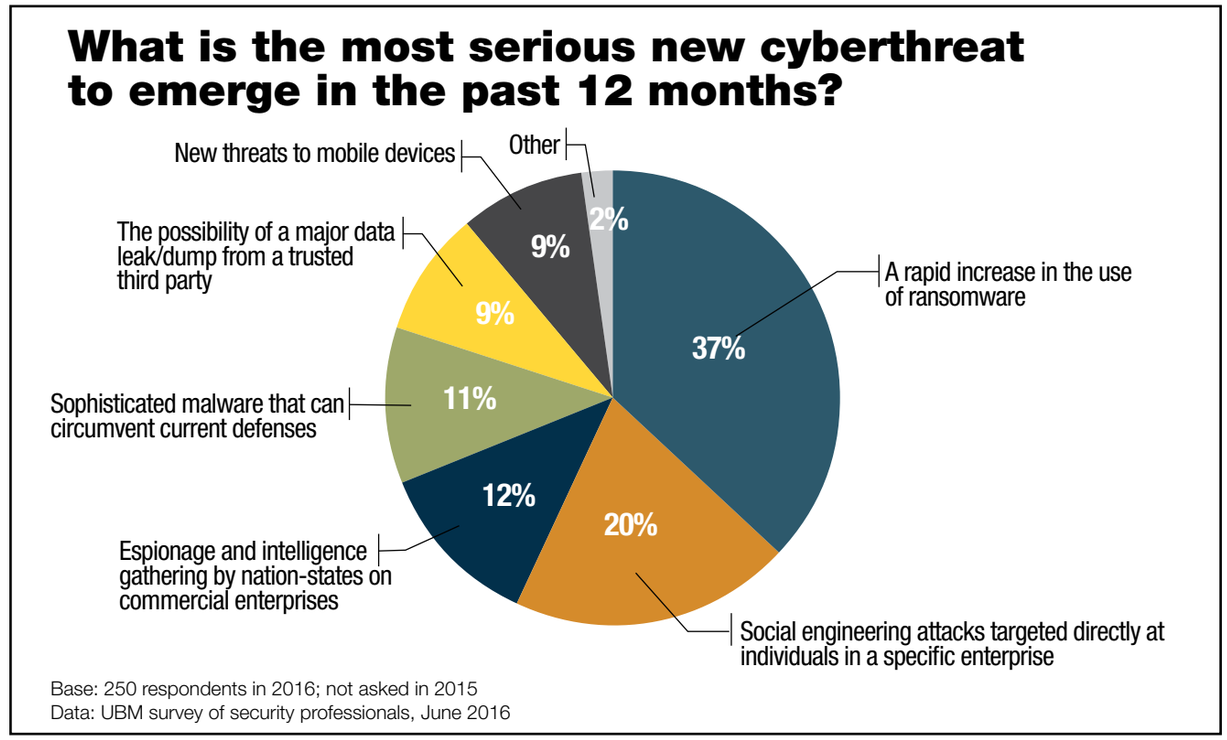
The security skills shortage is the primary reason why security initiatives fail, according to survey respondents, and this answer presents some major challenges for the industry in years to come. Clearly, there is a critical need to identify and quickly train a whole new wave of security professionals. Experts say that colleges and universities must help in this effort, and that professional associations and certification training initiatives will have to be ramped up significantly in coming years.

But even if this training could be done

immediately, and hundreds of thousands of new professionals were brought into the market, it would not solve the need for highly experienced staff. At least for the next several years, it is likely that security initiatives that rely heavily on highly trained and experienced people will continue to fail, simply because there are not enough people who fit these crtria. In the future, then, the security industry will be forced to re-evaluate all technologies and practices that require deep skill sets and look toward automation and technologies that can be operated with a minimum of training and experience.

And if you're trying to hire new security talent this year, it's going to be very hard — even harder than it was last year. Thirty-five percent of the respondents in the 2016 Black Hat Attendee Survey indicated that it would be very hard to convince them to leave their current organization— a substantial increase from 25% last year. Only 11% were actively looking for new work, slightly fewer than last year (12%). Only 24% of respondents said they are updating their resumes and keeping an eye out for job openings — down from 30% in 2015. (See **Figure 6**.)

Figure 4



Why are most security pros so happy in their jobs? Some of it has to do with knowing where they're going. When asked "Do you have a clear upward career growth path in your current place of employment," 44% of respondents said "Yes, I know the next step or level I can get to and I am working toward it now"— a hefty jump from 38% last year. Another 31% say they at least have some ideas about their options and they're "pretty sure I'll be here a while." (See **Figure 7**.)

With so many companies clamoring to hire

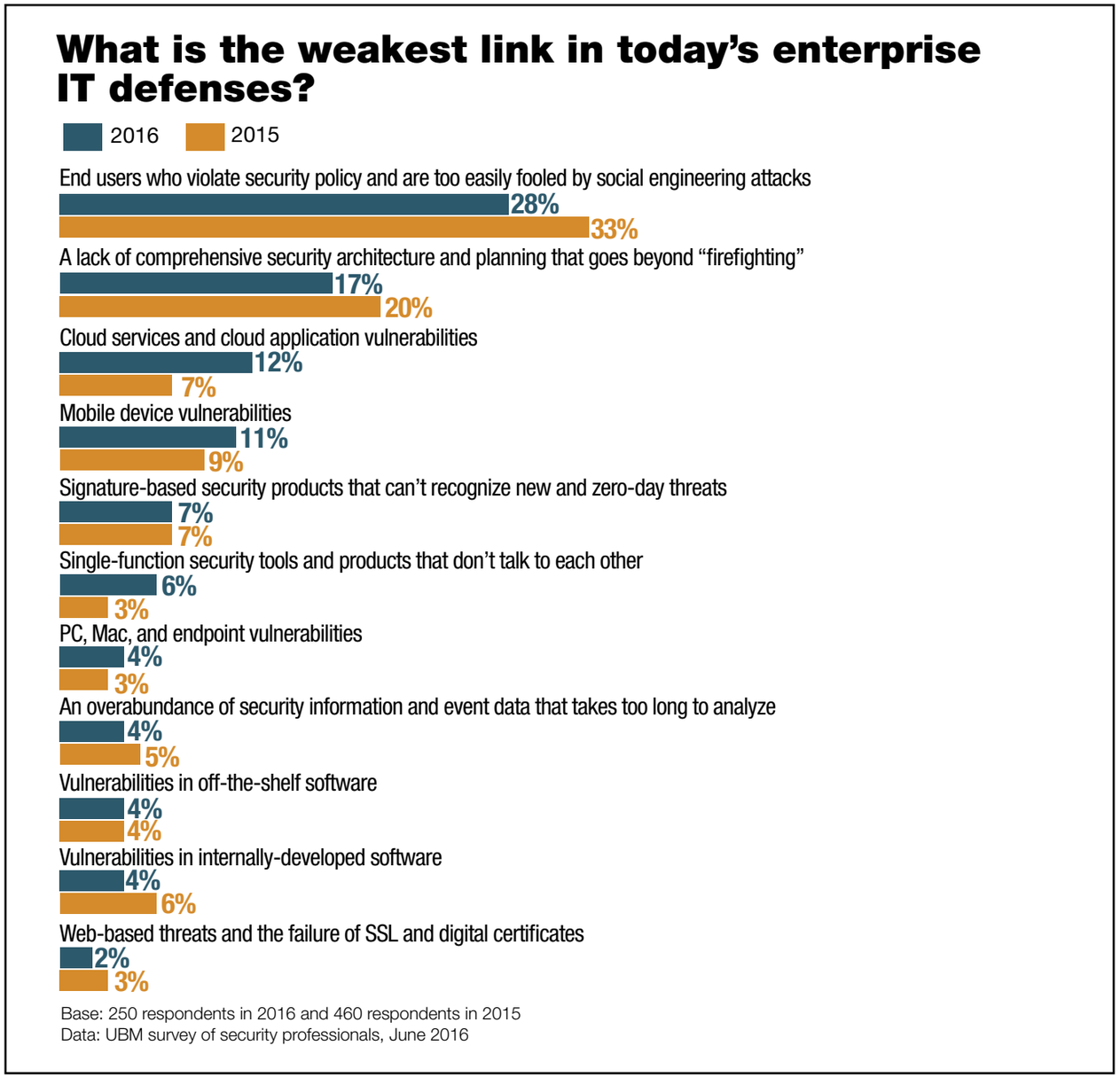
more people — and with the pool of available applicants shrinking — it has become a seller's market for the skilled cybersecurity professional. If they had to leave their current position, 95% of survey respondents said they believe they could find new work either "very quickly" (61%) or "without too much trouble" (34%). That's quite a leap from most other Americans, who currently take 27.8 weeks, on average, to find new work, according to the US Bureau of Labor Statistics.

The Security Priorities Gap

For the second year running, security professionals' top concerns are social engineering (46%) and sophisticated attacks targeted directly at their organization (43%). In 2015, 57% of respondents cited sophisticated, targeted attacks as one of their three main worries, earning it first place on the list. This year, that percentage tumbled to 43%, but these targeted attacks only slipped to second place in the ranks; it's still one of the most critical security issues. Social engineering held fast at 46% from 2015 to 2016, and thus rose from second place to first. (See **Figure 8**.)

These threats may be the things that keep

Figure 5

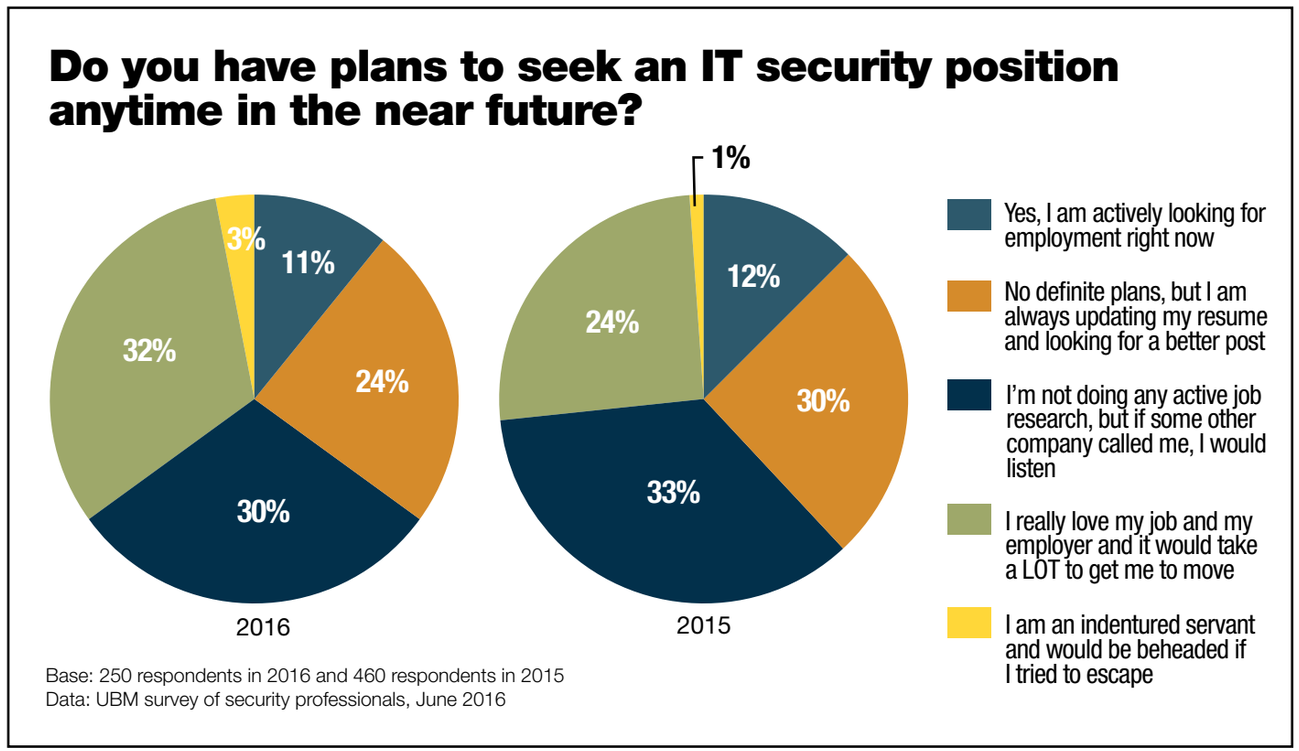


security professionals awake at night— but they aren't necessarily the things they spend the most time and money on during the day. For the second straight year, the Black Hat Attendee Survey revealed some clear differences between the priorities of the security pro and the priorities of those who make the schedules, plans, and budgets.

When asked how they spend most of their time on in an average day, security professionals cited measuring security posture and risk (first place, 35%) and maintaining compliance (second place, 32%) — both new options in the 2016 survey — as the top two time-consumers. "Security vulnerabilities created by my own internal application development team"— last year's first-place answer to this question — took third place (27%). Addressing social engineering and sophisticated, targeted attacks only made it to fourth place and eighth place, respectively. (See **Figure 9**.)

When asked how they spend most of their budget, security pros gave much the same report. Compliance took a big chunk out of the most respondents' budgets (31%), while risk measurement finished second (23%). Fixing the internal dev team's errors was third (19%). Social engineering and sophisticated targeted attacks fared only slightly better at getting funding than they did getting man-hours, garnering fourth place (19%) and sixth place (16%), respectively.

Figure 6



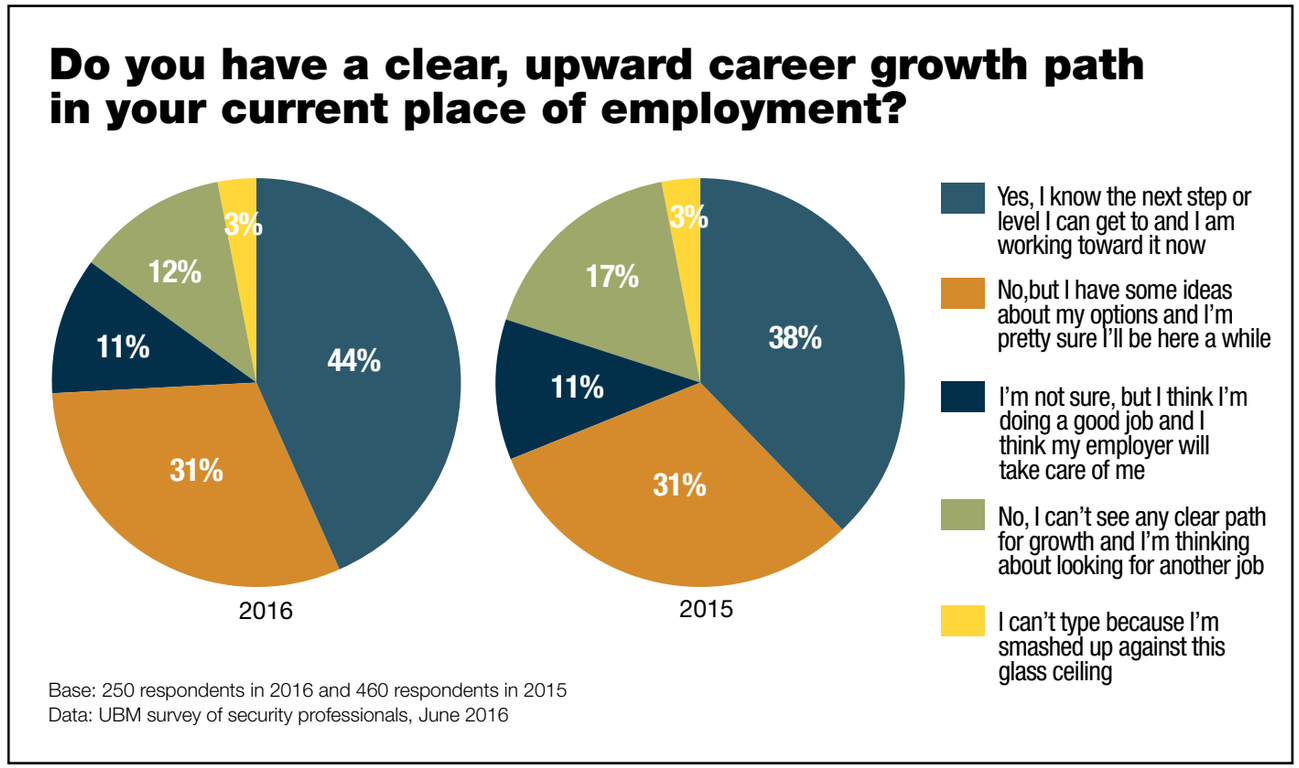
These results are stark in the context of the other data collected by the 2016 Black Hat Attendee Survey, which showed a clear shortage of resources such as human capital and funding. The data suggest that security professionals, already underfunded and understaffed,

are often unable to devote those limited resources to their most important priorities.

Interestingly, that dichotomy is not always driven by a lack of understanding among upper management. When asked what they believe are the highest security-related priorities of their top executives, Black Hat Attendee Survey respondents cited both sophisticated, targeted attacks (33%) and social engineering (24%) as being among the top three. Compliance (28%) finished second. This is consistent with last year's data, in which security pros also saw sophisticated, targeted attacks and social engineering as being high on their management's priority lists as well. (See **Figure 10**.)

Yet even though they see management as having many of the same priorities that they do, many security pros are losing faith that their non-security colleagues understand the threat that their organizations face today. Only 25% of respondents said their non-security managers and colleagues understand the current threat and support security efforts at their organization; this is down from 31% last year. An additional 10% said their non-security colleagues understand the threat "but have to be dragged into security conversations" (up from 9% last year). (See **Figure 11**.)

Figure 7



Exactly what is the threat that security pros want their colleagues to understand? By far, the attacker that Black Hat Attendee Survey respondents fear most is the one who has inside knowledge of their organization (36%). Some security pros are more worried about attackers who have strong backing by organized crime or nation-states (18%); others are concerned about attackers who

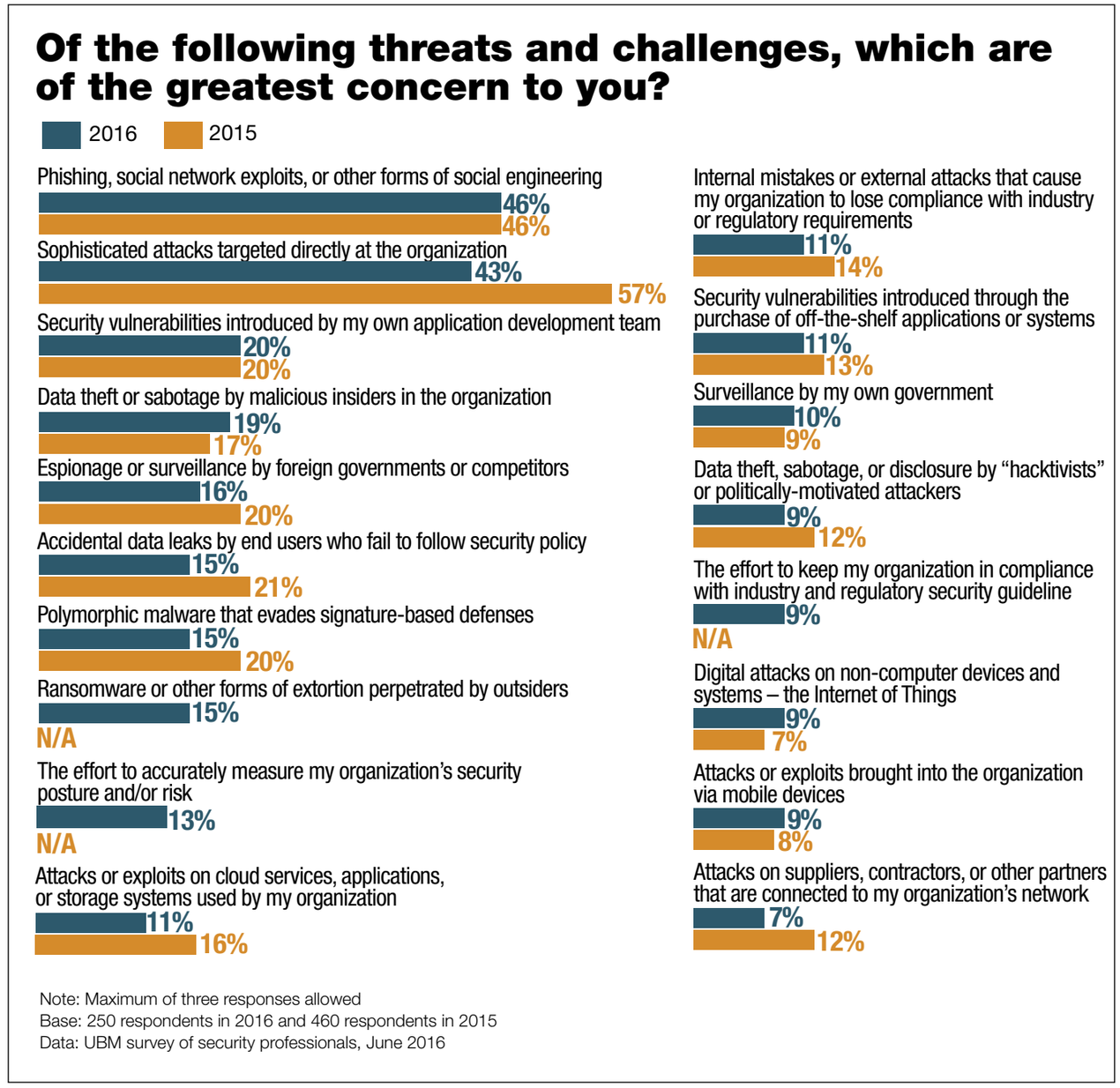
have highly sophisticated attack skills (15%). In general, though, respondents were most concerned about insiders or attackers who know the most about their organizations.

What will security pros worry most about in the future? For the second straight year, the security of non-computer devices and systems — the Internet of Things — was cited as the most critical issue that respondents believe they will worry about two years from now. The percentage of respondents who gave this response dropped significantly — to 28% from 36% a year ago — but IoT remained the most frequently cited concern on the horizon. This is a fascinating response because IoT barely registers as a concern (9%) among current threats. Clearly, security professionals expect IoT security to become a crucial issue over the next two years. (See **Figure 12**.)

Conclusion

Perhaps the most important conclusion we can draw from the 2016 Black Hat Attendee Survey is that the pressures on security professionals are not letting up — in fact, they are intensifying. In nearly every question and

Figure 8

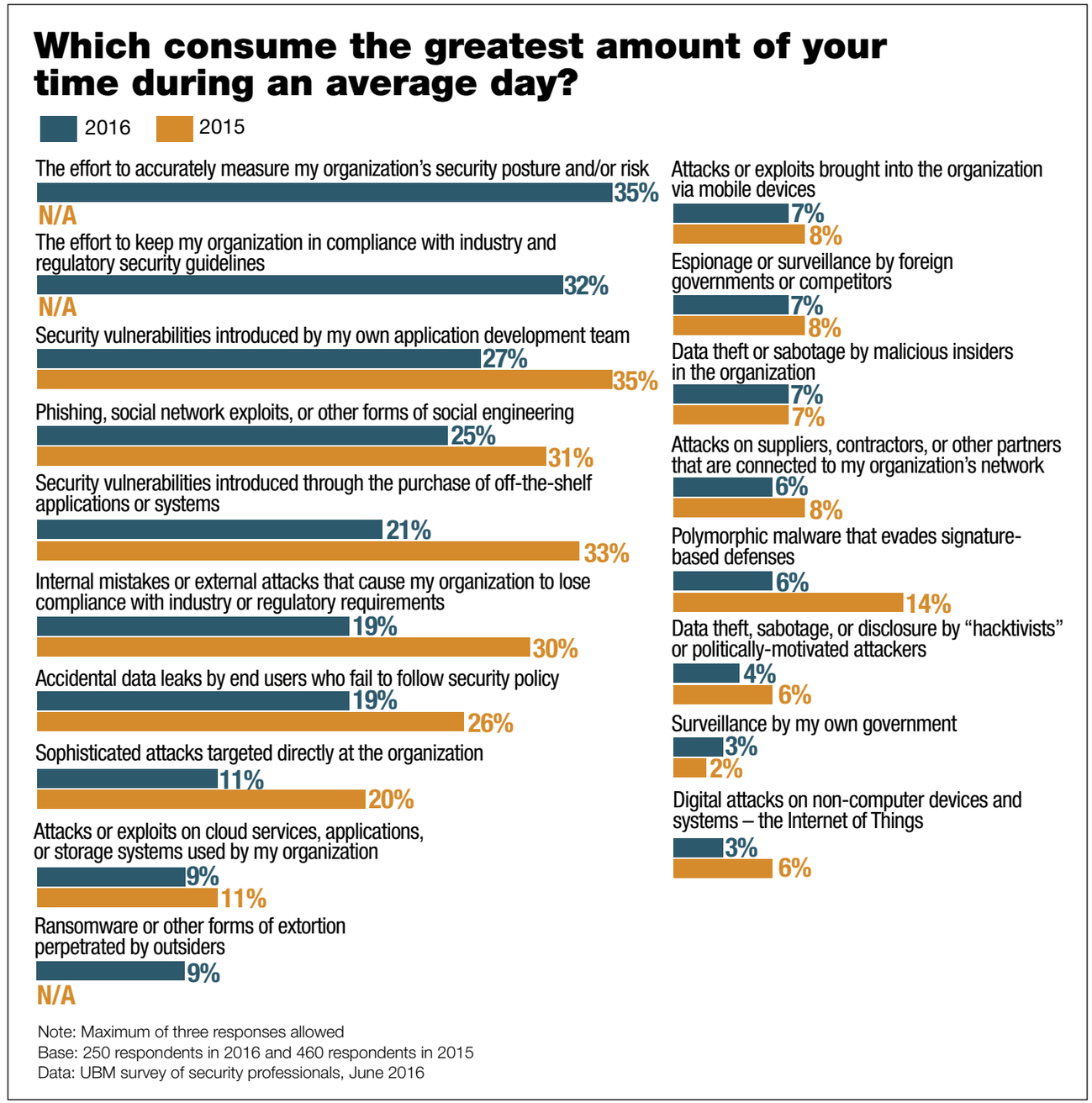


category, Black Hat attendees indicated that their environments are more at risk this year than they were last year—yet the availability of resources and skills has actually decreased. The shortage of people and skills clearly jumped out as the most important issue identified in this year's survey.

To compound the resource shortage, today's security pros are also facing an increasing gap between the priorities they themselves set for the security department and the priorities of those who control their time, people, and budgets. While they might be lying awake nights worrying about social engineering or targeted attacks, their days are spent mostly in more mundane tasks, such as maintaining compliance or troubleshooting internally developed applications.

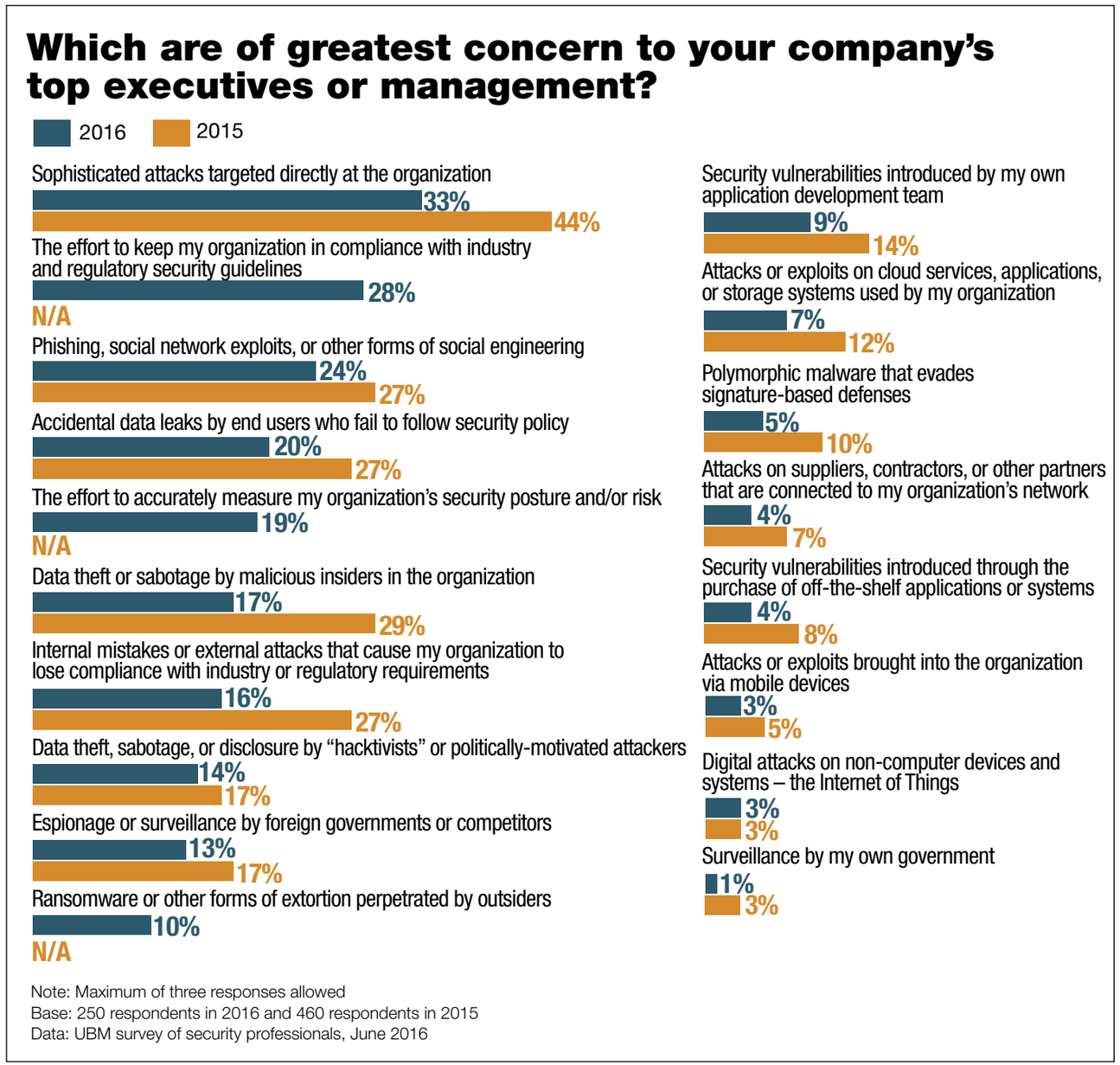
To gain ground on the bad guys, security teams will have to find new ways to staff and fund their initiatives — perhaps through additional automation and by reducing the requirement for highly developed skills. Security pros will also need to examine new technologies and practices that can reduce the need for staffing and budget, as well as new ways to make their existing team more cost-efficient.

Figure 9



APPENDIX

Figure 10



Note: Maximum of three responses allowed
Base: 250 respondents in 2016 and 460 respondents in 2015
Data: UBM survey of security professionals, June 2016

Figure 11

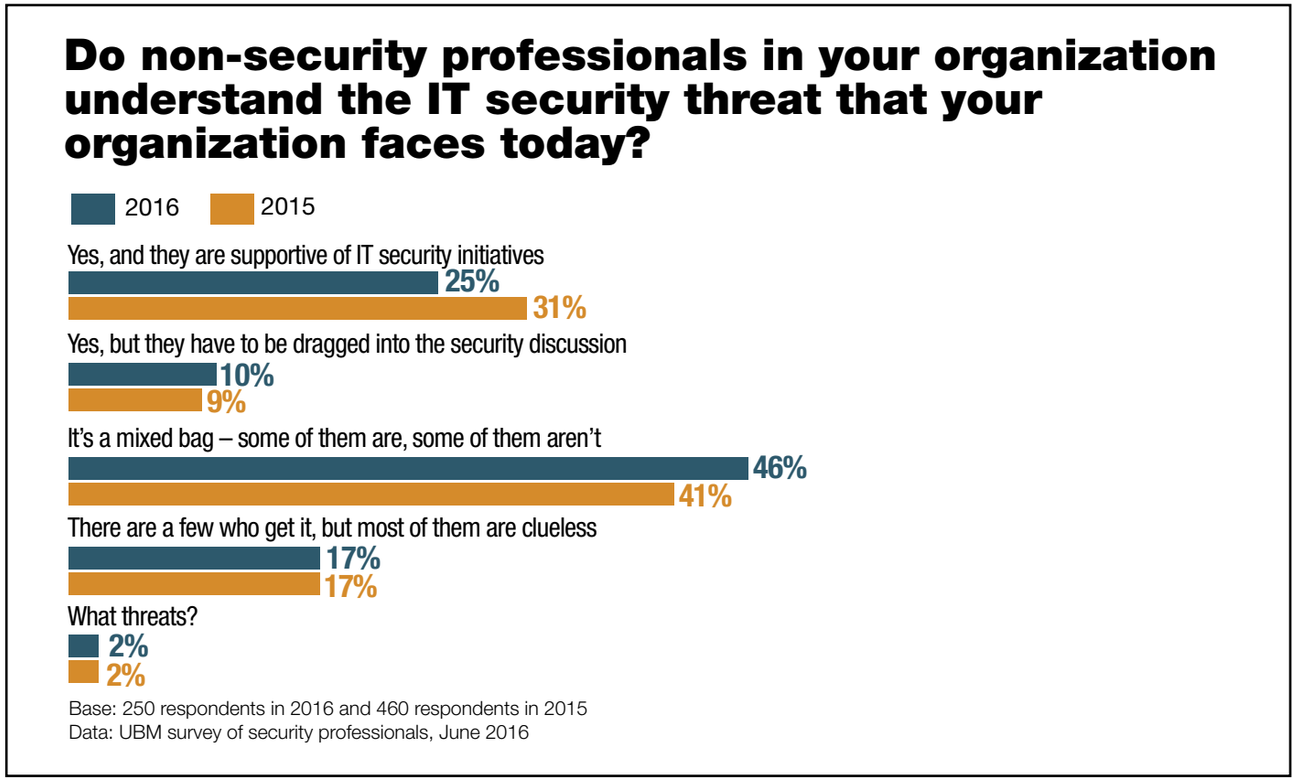
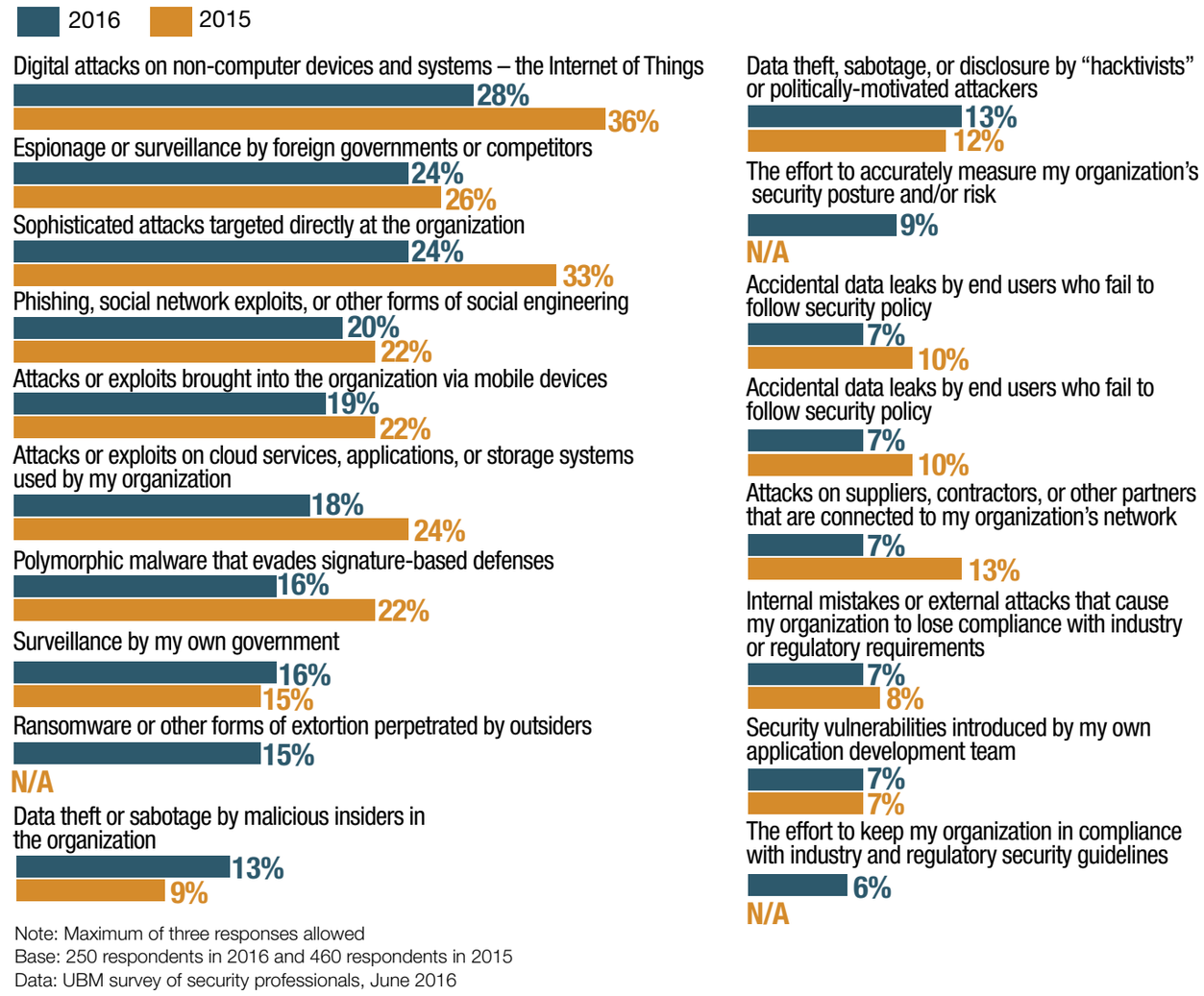

Do non-security professionals in your organization understand the IT security threat that your organization faces today?
2016
2015
Yes, and they are supportive of IT security initiatives
25%
31%
Yes, but they have to be dragged into the security discussion
10%
9%
It's a mixed bag – some of them are, some of them aren't
46%
41%
There are a few who get it, but most of them are clueless
17%
17%
What threats?
2%
2%
Base: 250 respondents in 2016 and 460 respondents in 2015
Data: UBM survey of security professionals, June 2016

Figure 12

Which do you believe will be of greatest concern two years from now?



Note: Maximum of three responses allowed
Base: 250 respondents in 2016 and 460 respondents in 2015
Data: UBM survey of security professionals, June 2016