black hat USA 2015

blackhat.com

Next

July 2015

## 2015 Black Hat Attendee Survey

# 2015: Time to Rethink Enterprise IT Security

In first-ever survey, sophisticated security professionals say enterprise security priorities don't address the most serious threats

# SYNOPSIS

RESEARCH

**Survey Name** The 2015 Black Hat Attendee Survey

**Survey Date** July 2015

**Region** North America

**Number of Respondents** 460

**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 2015 Dark Reading and Black Hat conducted a survey of the Black Hat USA conference attendees. The online survey yielded data from 460 management and staff security professionals, predominantly at large companies, with 64% working at companies with 1,000 or more employees.

The greatest possible margin of error for the total respondent base (N=460) is +/- 4.5 percentage points. UBM Tech was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.

## ABOUT US

For more than 17 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.

# 2015: Time to Rethink Enterprise IT Security

**Executive Summary**

In 2015, enterprises will spend more than $71.1 billion on information security – more than they have ever spent before, according to Gartner Group figures. Yet, the incidence of major data breaches – as evidenced by compromises at corporations such as Anthem, Sony, and many others – shows no signs of abating. As enterprises continue to struggle with online attacks and data leaks, many are asking one common question: What are we doing wrong?

This year, we decided to put this question – and many more – to 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 includes responses from 460 top-level security experts, including some of the most IT security-savvy professionals in the industry. More than 61 percent of the respondents carry a full-time "security" job title, and 25 percent are managers of the security effort in their organization. Nearly two-thirds of the respondents have received credentials as Certified Information Systems Security Professionals (CISSP), and many also hold other advanced credentials. Nearly half (47 percent) of the respondents work in organizations that have 5,000 employees or more.

Clearly, these are the individuals who make information security happen in large organizations – the people who spend their days examining online exploits and data leaks and who develop and implement enterprise defenses. Yet, the 2015 Black Hat Attendee Survey reveals a disturbing gap between the priorities and concerns of these security-savvy individuals and the actual expenditure of security resources in the average enterprise.

In short, the survey indicates that most enterprises are not spending their time, budget, and staffing resources on the problems that most security-savvy professionals consider to be the greatest threats.

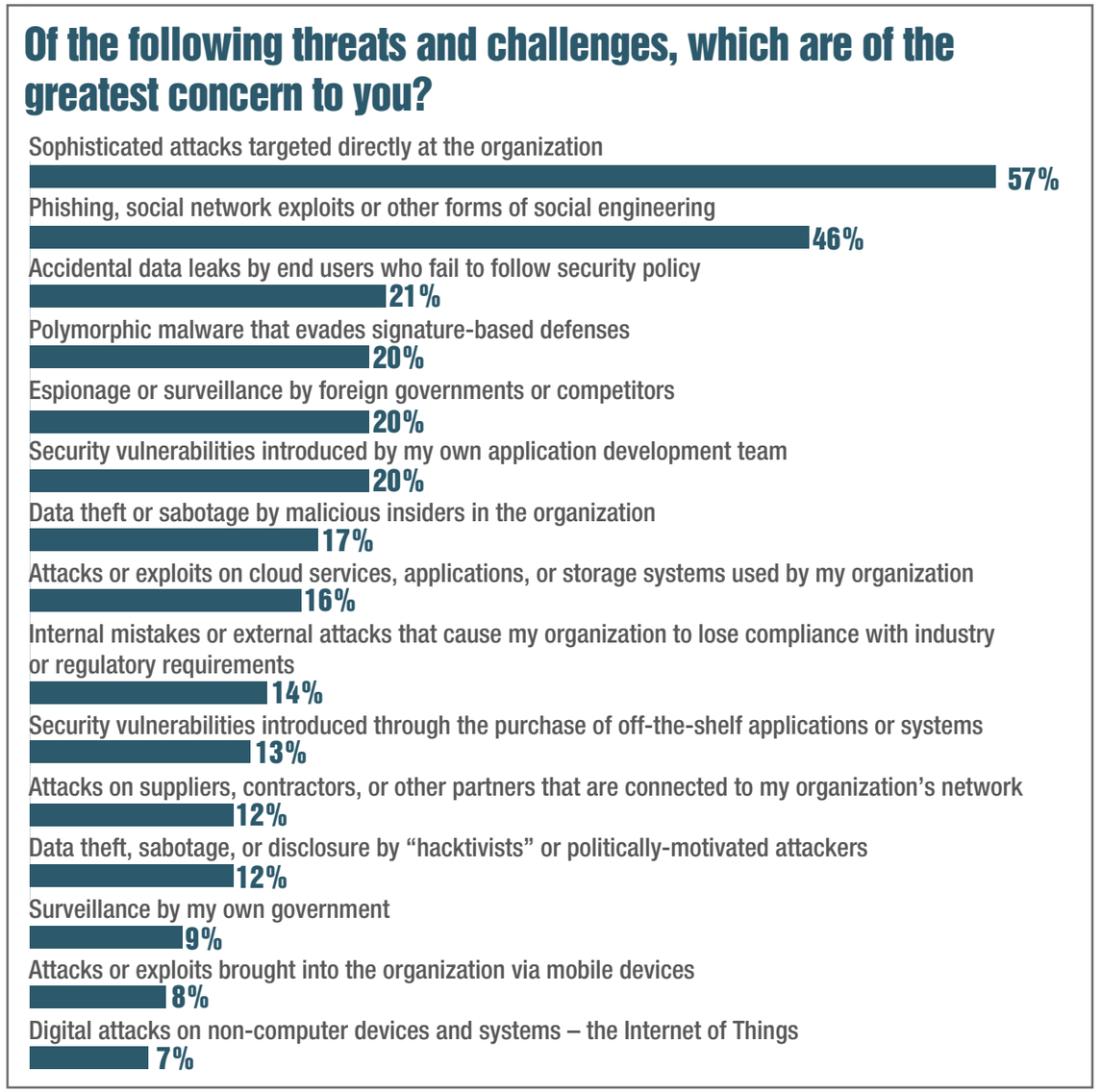
In the study, the vast majority of security professionals – 57 percent – cited sophisticated, targeted attacks as their greatest concern (**Figure 1**). Yet, only 26 percent of respondents indicated that targeted attacks were among the top three IT security

spending priorities in their organization, and only 20 percent of respondents said that targeted attacks were among the top three tasks where they spend the most time. Social engineering attacks, which were cited as a top concern by 46 percent of respondents, are similarly shortchanged in time and budget. And potential threats posed by the Internet of Things, which ranked as the greatest concern two years from now, are barely being addressed in current time or budget expenditures.

The 2015 Black Hat Attendee survey also reveals a serious shortage of IT security resources in the days ahead. While nearly three quarters (73 percent) of respondents think it likely that their organizations will have to deal with a major data breach in the year ahead, a majority also feel that they do not have enough budget, staff, and training to handle the load.

And, for good or ill, this shortage of staffing and skilled resources has created a seller's market for the most security-savvy professionals. Some 94 percent of security professionals believe they would have little trouble finding another job, and while most are happy in their

Figure 1 The 2015 Black Hat Attendee Survey




Note: Maximum of three responses allowed
Data: UBM survey of 460 security professionals, June 2015

current positions, nearly two thirds (63 percent) say they would listen to a job opportunity posed by another employer.

This report summarizes some of the results from the survey and offers some insight on how the industry's most knowledgeable security professionals regard the current state of the industry – and their own situations. Clearly, the IT security industry has some significant challenges ahead.

**FAST FACT**

**57%**

Consider sophisticated attacks to be one of their 3 greatest concerns.

## Priorities and Resources: A Troubling Disparity

As organizations struggle to find better, more efficient defenses against attack, perhaps the most significant result from the 2015 Black Hat Attendee survey is the disparity between the threats that keep security professionals awake at night and the tasks that keep them occupied during the day.

At 57 percent, the list of security pros' greatest concerns was headed by sophisticated attacks targeted directly at the organization. Phishing and social engineering constituted the second-greatest concern at 46 percent. Issues such as accidental data leaks (21 percent), vulnerabilities in software developed in-house (20 percent), polymorphic malware (20 percent), and cyber espionage (20 percent) finished a mixed bag of third concerns (respondents were allowed to choose up to three). The data suggests that Black Hat attendees are aware of potential exploits and attacks that could be created by outsiders, and this knowledge causes significant concern.

Yet, when asked which defensive tasks consume the most time in the course of their workday, security professionals offered a very different picture. In response to this question, more than a third of Black Hat attendees said that their most time-consuming tasks are in addressing vulnerabilities introduced by internally developed software (35 percent) and vulnerabilities introduced by off-the-shelf software (33 percent). The data suggests that application flaws across the enterprise consume a great deal of time for the IT staff, yet are seldom considered the greatest threats. (**Figure 2**)

By contrast, only 20 percent of security professionals counted targeted attacks as one of the top three areas where they spend the most time, and only 31 percent said that social engineering attacks are among their top three tasks.

Similarly, IT security spending priorities differ significantly from the level of concern among security-savvy professionals. Just 26 percent of respondents ranked targeted attacks as one of their top three priorities for spending. Accidental leaks (26 percent), potential regulatory compliance issues (25 percent), and security vulnerabilities introduced by internally developed applications (23 percent) also ranked most frequently among the top three spending priorities. The widespread range of spending priorities in the survey shows that budgets may be failing to keep up with the latest threats, and that security professionals are not able to tune that spending to meet their most current concerns. (**Figure 3**)

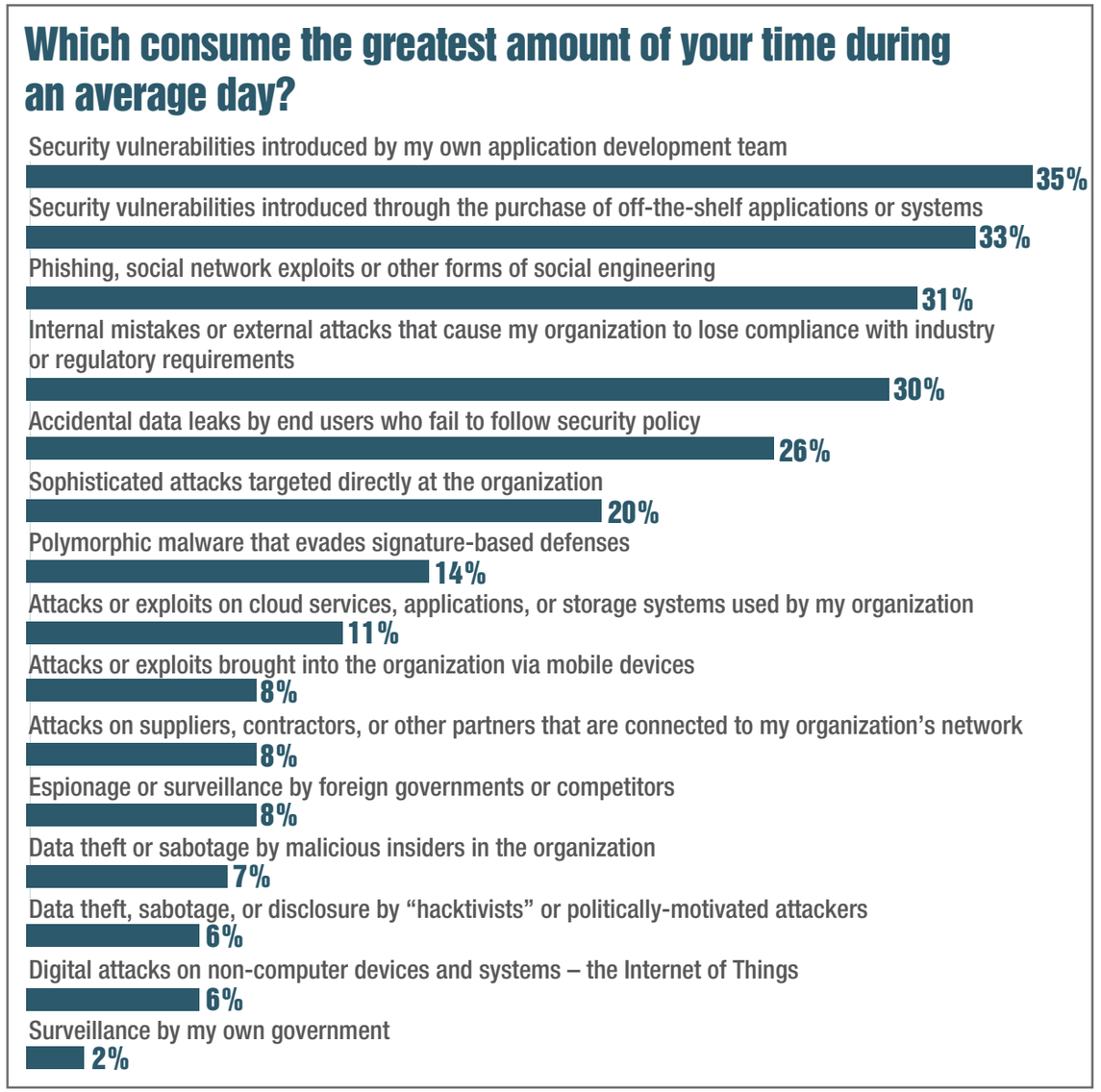
Many security professionals feel that the perception of current threats – both in the media and among their managers and supervisors — is different from their own. Close to half (41 percent) of respondents believe that the media has overplayed the issue of

domestic government surveillance, and more than a quarter (27 percent) say the media focuses too heavily on hacktivists and politically motivated attackers. Among management, security professionals perceive a high rate of concern (29 percent) over malicious insiders, which was a top concern for only 17 percent of security professionals. And while many security professionals believe their management has mirroring concern for targeted attacks (44 percent) and social engineering (29 percent), they still indicate a difference between their own level of concern and those of their managers.

Similarly, many Black Hat attendees feel that key threats are being overlooked. Twenty-six percent of respondents say that phishing and social engineering do not get enough attention in the media and at industry events. Accidental data leaks by end users and new vulnerabilities introduced by off-the-shelf software are also areas that are do not receive adequate attention, respondents said.

And the disparity between security professionals' concerns and mainstream concerns will likely continue to be significant, according to survey data. More than a third of re-

Figure 2




Note: Maximum of three responses allowed
Data: UBM survey of 460 security professionals, June 2015

spondents (36 percent) said they believe that threats borne by non-computer devices – the Internet of Things (IoT) – will be among their top concerns two years from now. Yet at the moment, only 6 percent of respondents say IoT security constitutes a top security priority in time spent, and only 3 percent say it's a budget priority. (**Figure 4**)

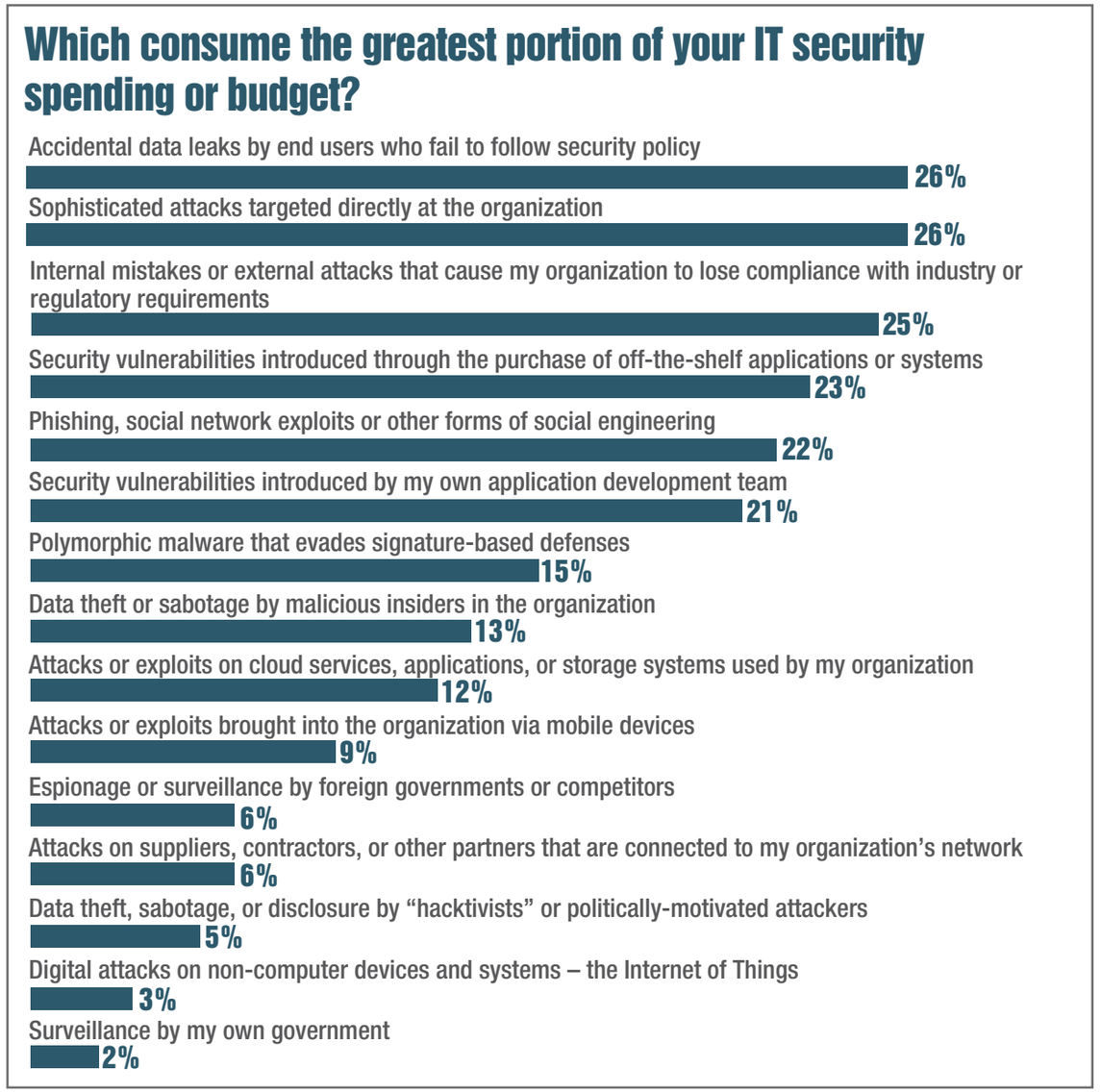
### Increasing Threats Highlight Shortage of Security Resources

How likely is it that a particular enterprise will experience a major breach in the coming year? Business executives may continue to hope to remain unscathed, but security professionals are facing the hard reality that their organizations probably will be next. Some 73 percent of Black Hat attendees say it is likely that they will have to respond to a significant compromise in the coming year: 13 percent say they have "no doubt" about it, 24 percent say that it's "highly likely," and 36 percent say that it's "somewhat likely." Many security experts use the phrase, "It's not a matter of if, but when."

What will be the most likely point of entry? Nearly a third (33 percent) of security-savvy

Figure 3





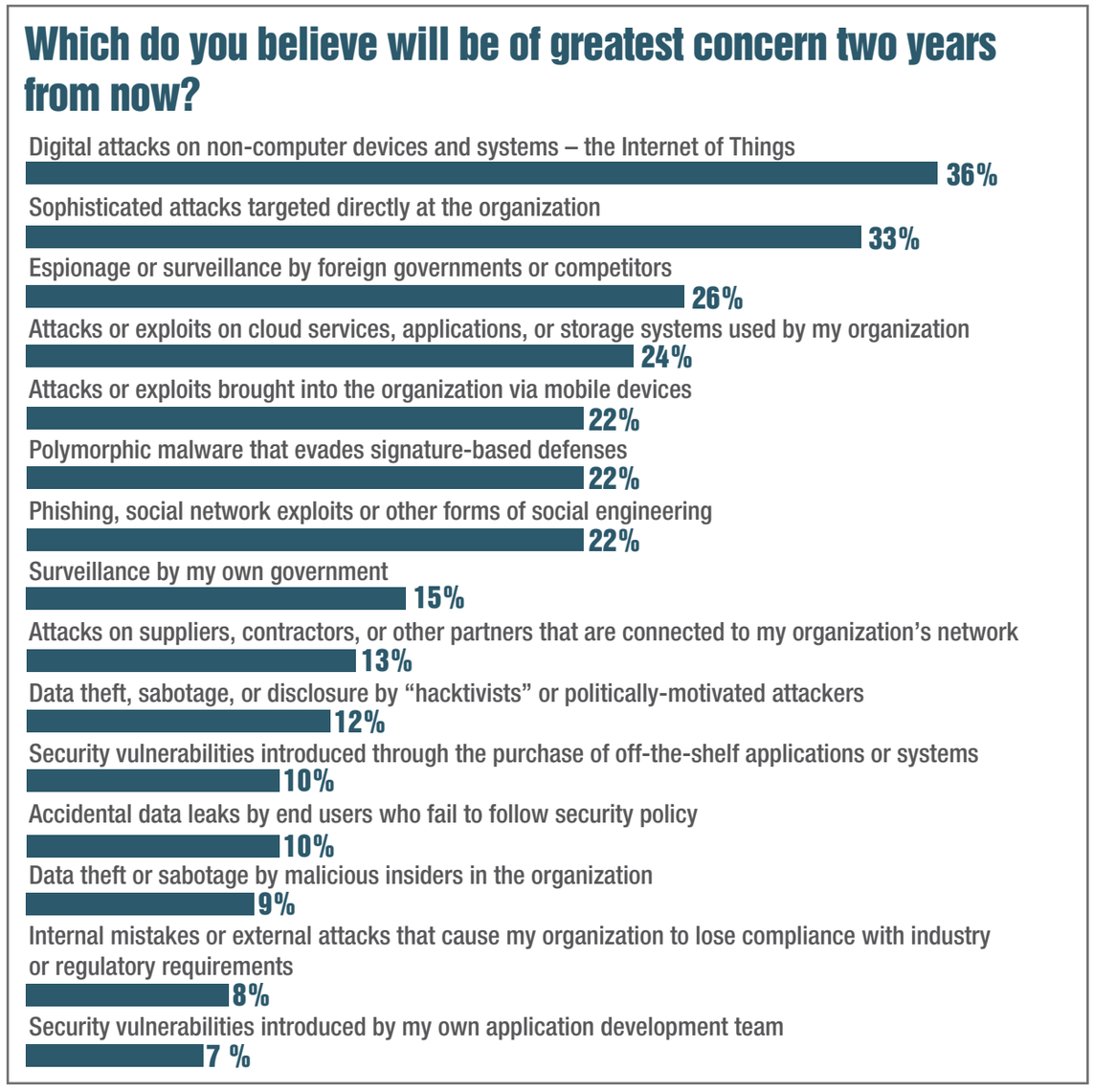

Note: Maximum of three responses allowed
Data: UBM survey of 460 security professionals, June 2015

IT pros say that "end users who violate security policy and are easily fooled by social engineering attacks" are the weakest links in the IT security chain of defense. Interestingly, however, one-fifth of respondents are also worried about their own defense strategies, citing "a lack of security architecture and planning that goes beyond firefighting" as their weakest link. This attitude is also pervasive in IT security discussions: A sense that the "layering" of single-purpose technologies and solutions might be leaving too many cracks for attackers to get through. (**Figure 5**)

A key reason for security professionals' concerns about future attacks is the shortage of resources that they feel in their own organizations. In the Black Hat Attendee Survey, only 27 percent of respondents said they feel their organization has enough staff to defend itself against current threats; nearly a quarter (22 percent) described their security departments as being "completely underwater." (**Figure 6**) Similarly, only one third (34 percent) of security pros said their organization has enough budget to defend itself against current threats; 21 percent said they

Figure 4

The 2015 Black Hat Attendee Survey




Note: Maximum of three responses allowed
Data: UBM survey of 460 security professionals, June 2015

are "severely hampered" in their defenses by a lack of funding.

Even among security pros themselves, there is a sense that a shortage of skills and training may impair the ability to respond to current threats. While 36 percent said they have the skills they need to do their jobs, some 55 percent said they could use some training. Nine percent said they feel they are ill-prepared to handle future attacks or exploits they may encounter in the near future.

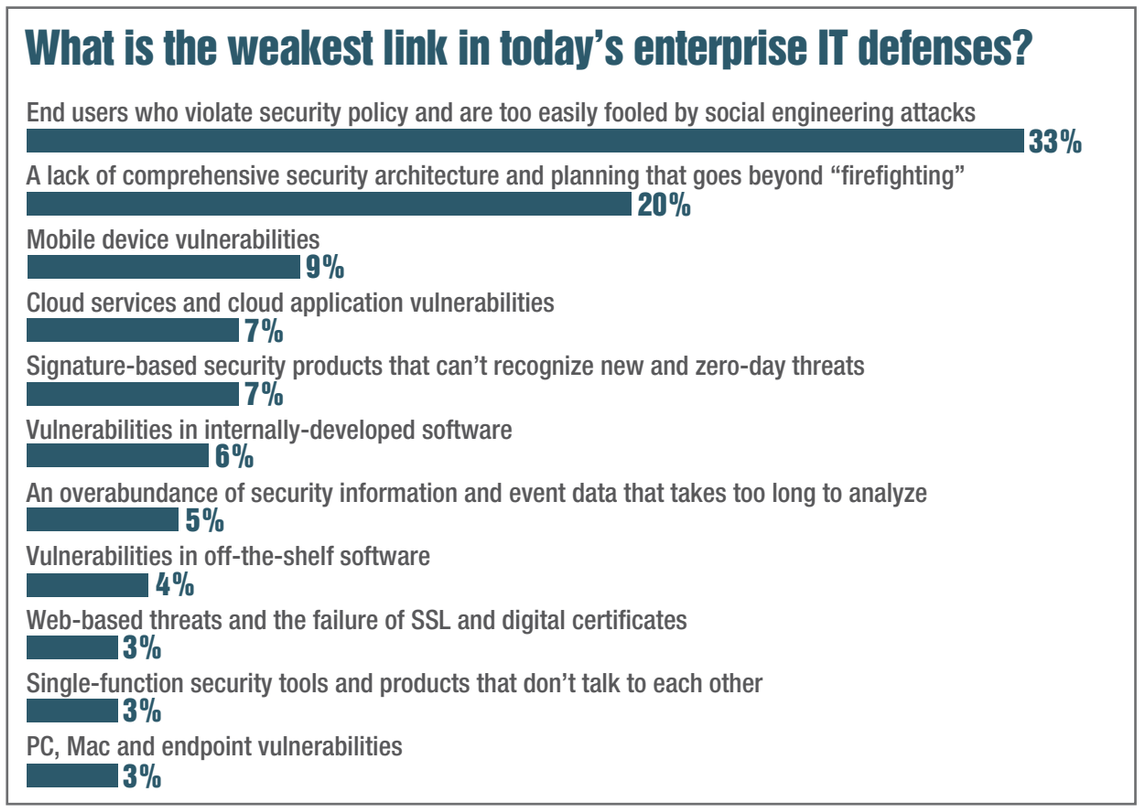
The central message that comes across in all of these questions is that while sophisticated security professionals are increasingly convinced that a major breach is inevitable, most of those security pros do not feel they have the resources and training they need to defend their organizations. The combination of these responses should ring warning bells to the industry that security defense strategies and resources need serious rethinking, and that the people who walk the walls and guard the doors are not confident in their ability to keep online adversaries out of enterprise systems and data.

**FAST FACT**

**36%**

Predict that IoT security will be a top concern in two years.

Figure 5




Data: UBM survey of 460 security professionals, June 2015

## Enterprise Security Equals Job Security

The combination of a growing threat, perceived weaknesses in cyber defenses, and a shortage of skilled people has created a seller's market for advanced security talent such as those who attend Black Hat. Some 94 percent of survey respondents feel that, should they need to make a change, they could get anoth-

er job "without too much trouble." This indicates that many security professionals feel secure and mobile in their careers.

Interestingly, however, most security pros are happy where they are – in fact, only 12 percent of respondents described themselves as actively job-hunting today. 58 percent are not even updating their resumes, and nearly a quarter (24 percent) say they are happy in their jobs and it would take a lot to get them to change positions. (**Figure 7**)

A key reason for their job satisfaction may be the support security pros are getting from their management. As mentioned earlier, most of the survey respondents felt that their management had roughly the same priorities as they do. Nearly a third of respondents described their non-IT counterparts as supportive of IT security initiatives, and 81 percent indicated that they have at least some support from non-IT management who "get" the security problem. This is a significant shift from a few years ago, when many studies indicated that non-IT managers did not understand the security problem or how to support it.

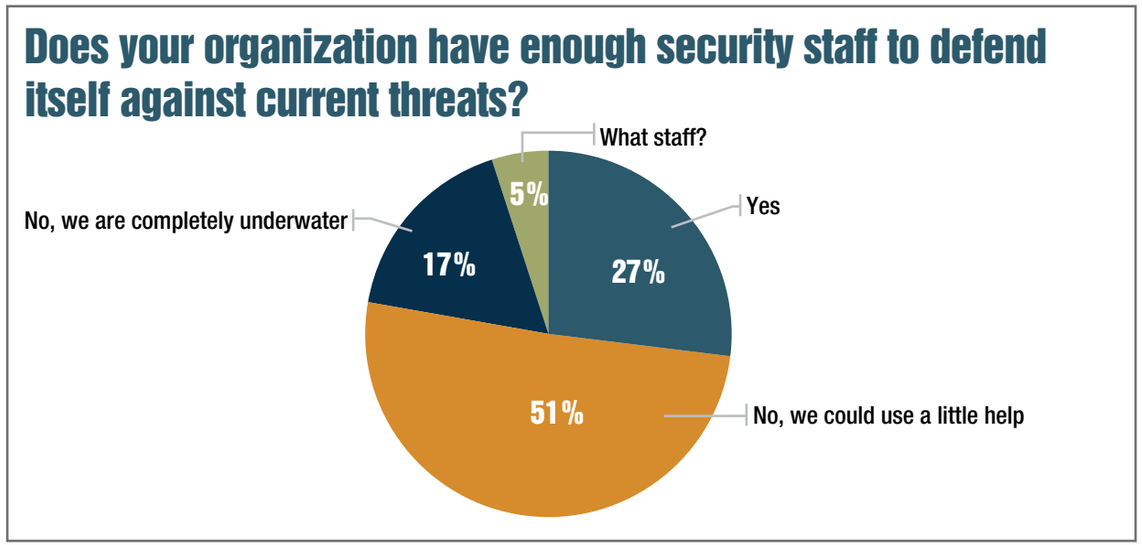
In general, most security pros also feel that their management is offering a growth path for their careers. Some 38 percent said they know the next

**FAST FACT**

**24%**

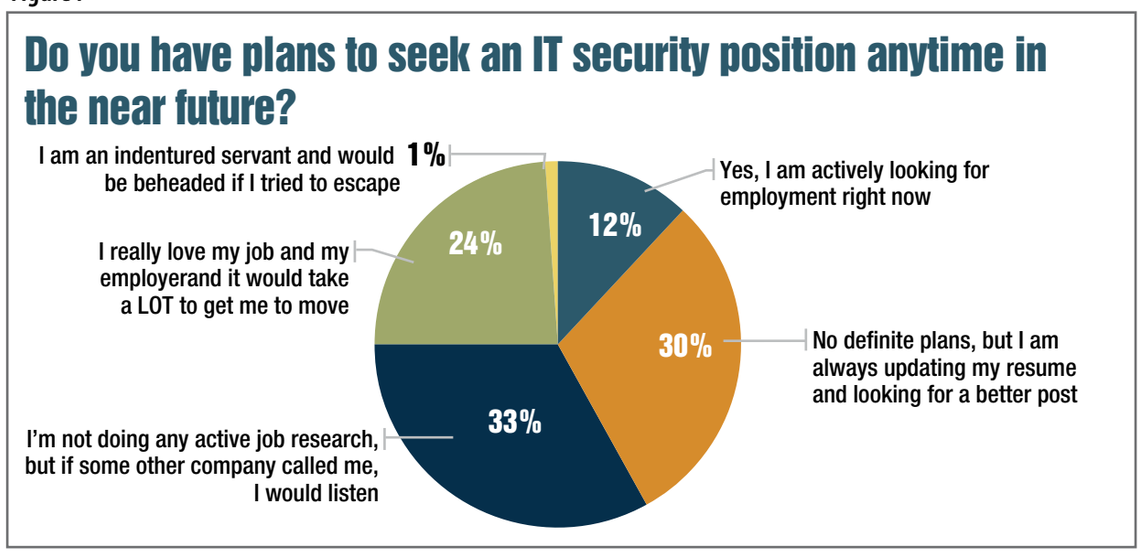
are happy in their jobs and have no plans to change.

Figure 6




Data: UBM survey of 460 security professionals, June 2015

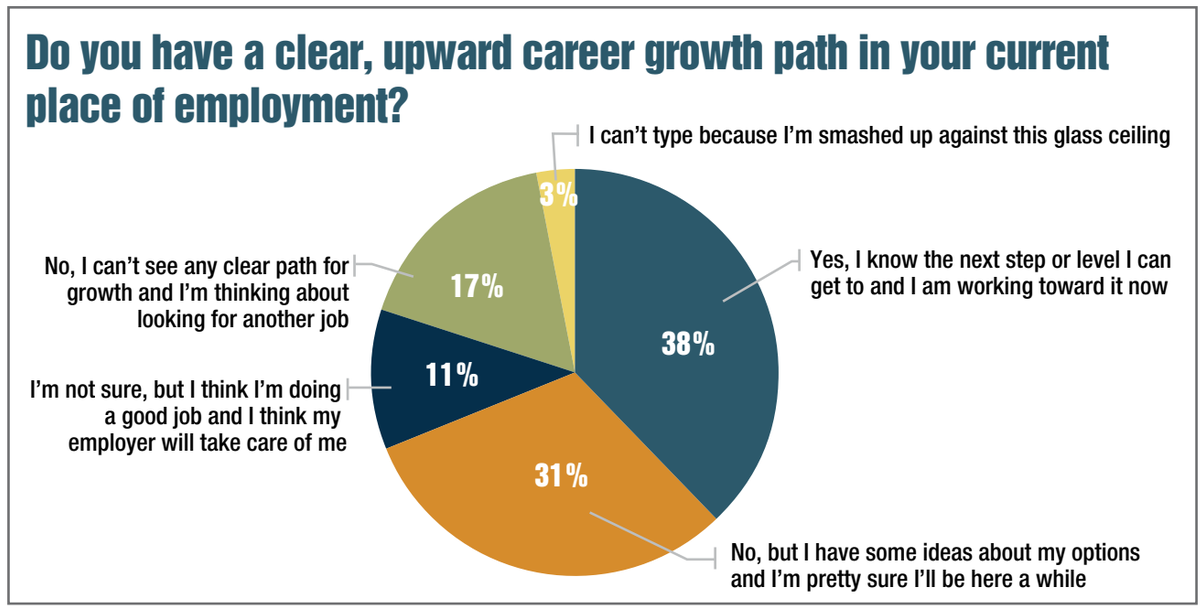
Figure 7




Data: UBM survey of 460 security professionals, June 2015

level they can reach on the corporate ladder and are actively working toward it. Another 42 percent said they feel they know their options and are pretty sure they "will be here for a while." These figures suggest that only 20 percent of security pros are looking for a new position; with numbers like these, it seems likely that it will continue to be difficult to find security job candidates on the open market for some time to come. (**Figure 8**)

Figure 8




Data: UBM survey of 460 security professionals, June 2015

## Conclusions

The 2015 Black Hat Attendee Survey offers several takeaways that indicate a need to rethink the current enterprise IT security model. Perhaps the most important of these is that security pros are not spending their time and budget in a manner that is commensurate with their concerns about current threats. While issues such as compliance and application security take a significant amount of their time, they need greater leeway to focus on emerging threats such as targeted attacks and social engineering exploits that pose the greatest danger to their organizations.

The growing online threat also is putting continuous pressure on security staffs and departments, even in the largest and most security-savvy organizations. Most security pros feel that they do not have enough people, budget, or training to handle the current threat, and most have not yet begun to address what security pros believe will be their greatest concern two years from now: the Internet of Things.

Finally, the shortage of available security talent will likely continue in days to come. While most security pros feel confident in their ability to change jobs, the vast majority are happy in their current positions and feel they are well-supported by management. Finding sophisticated professionals, such as those in the Black Hat attendee base, will not be easy in the future.