black hat USA 2017

www.blackhat.com

July 2017

2017 Black Hat Attendee Survey

Portrait of an Imminent Cyberthreat

Cyber attacks on US enterprises and critical infrastructure are coming soon, according to some of the industry's most experienced and highly informed security professionals. And in most cases, defenders are not prepared.

TABLE OF CONTENTS

Figures

EXECUTIVE SUMMARY

Most information security professionals believe that the US critical infrastructure will be breached by a cyber attack within the next two years. Most also believe that their own enterprises will be breached in the next 12 months. And most believe that the defenders of those infrastructures are not ready to respond.

These are some of the conclusions drawn by 580 respondents to the 2017 Black Hat Attendee Survey, a poll of top-level cybersecurity professionals who have attended the annual Black Hat USA conference in the last two years. Black Hat, a forum that features some of the most advanced security research in the world, is a destination for discussion among the industry's most experienced information security pros, including leading ethical hackers, IT security management, and technology developers.

The survey results offer a dark picture of tomorrow's cyber defenses, which are being increasingly tested by sophisticated hacking and social engineering exploits, including ransomware worms such as WannaCry and nation-state-sponsored hacks such as those emanating from Russia and North Korea. In essence, the survey is a warning from the industry's most experienced and responsible IT security professionals that successful cyber attacks on essential infrastructure and business could be imminent, but defenders do not have the resources and training they need to efficiently respond.

The 2017 Black Hat Attendee Survey also polled cybersecurity professionals on their attitudes, concerns, and strategic plans for the coming year. We looked at the threats they are facing, their budgets and staffing plans, and their feelings about the latest developments in cyberspace.

EXECUTIVE SUMMARY

The survey reveals a wide range of insights, including:

- 60% of respondents believe that a successful cyber attack on US critical infrastructure will occur in the next two years. Only 26% are confident that U.S. government and defense forces are equipped and trained to respond appropriately.
- 69% of IT security professionals believe that state-sponsored hacking from countries such as Russia and China has made US enterprise data less secure.
- Only 26% of information security pros believe that the new White House administration will have a positive impact on cybersecurity policy, regulation, and law enforcement over the next four years.
- About two-thirds of respondents think it's likely that their own organizations will have to respond to a major security breach in the next 12 months. Sixty-nine percent say they don't have enough staff to meet the threat; 58% believe they don't have adequate budgets.
- IT security professionals' greatest concerns are around phishing and social engineering (50%) and sophisticated attacks targeted directly at their own organizations (45%).
- The increased use of ransomware remains the most serious new threat faced by cybersecurity professionals, cited by 36% of respondents.

SYNOPSIS

RESEARCH

Survey Name The 2017 Black Hat Attendee Survey

Survey Date June 2017

Region North America

Number of Respondents 580 IT security professionals. The greatest possible margin of error for the total respondent base (N=580) is +/- 4.0%. UBM was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.

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 2017, Dark Reading and Black Hat conducted a survey of the Black Hat USA conference attendees. The online survey yielded data from 580 management and staff security professionals, predominantly at large companies, with 66% working at companies with 1,000 or more employees. Sixty-four percent of the respondents hold the CISSP security professional credential.

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.

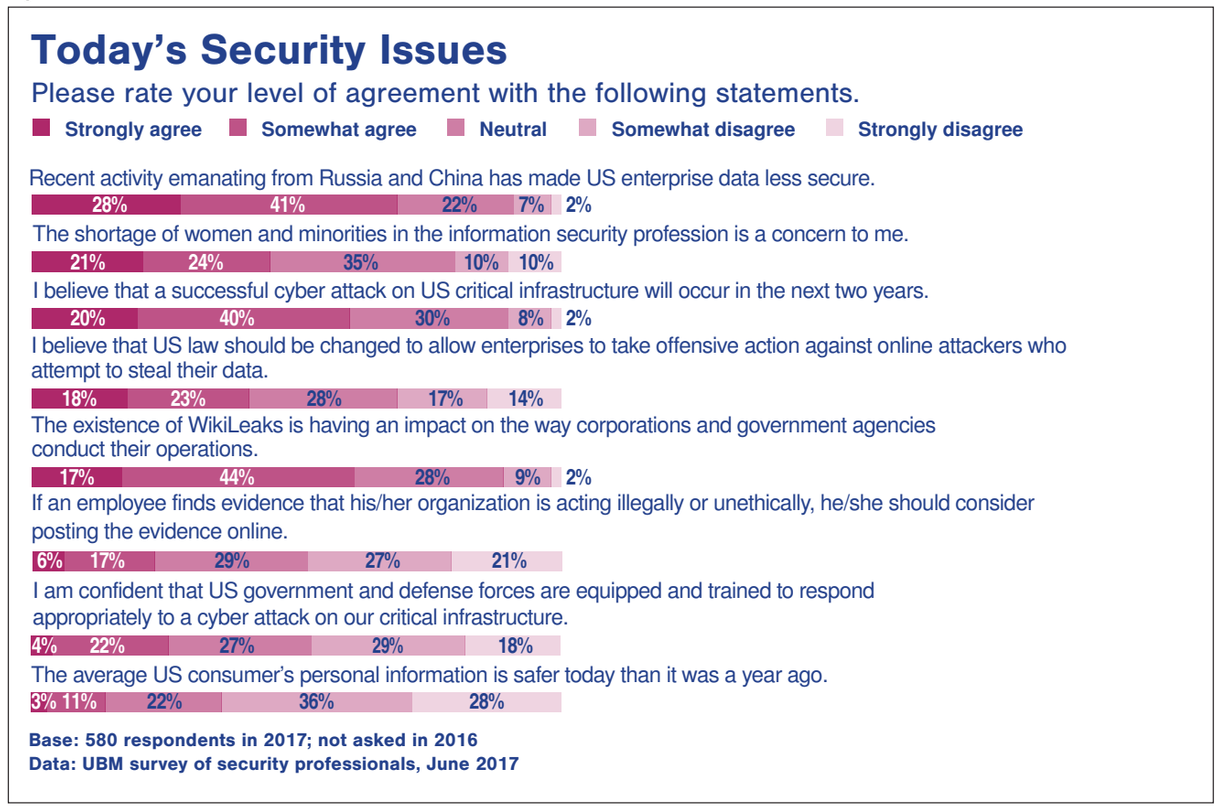
More information is available at: http://www.blackhat.com.

Concerns about IT Security Extend beyond the Enterprise

In past years, respondents to the Black Hat Attendee Survey have expressed concern about the high likelihood of online attacks and their organizations' ability to respond. These concerns have turned out to be well-founded, as the frequency and cost of major data breaches have increased each year, as reported by Verizon's Data Breach Investigations Report and Ponemon's Cost of a Data Breach report.

This year, the Black Hat Attendee Survey respondents offer a clear warning that critical infrastructure in the United States is at risk. In fact, 60% of security professionals said they believe a successful cyber attack on US critical infrastructure will occur in the next two years (**Figure 1**). Thirty percent remained neutral; only 10% said they do not believe a successful attack will occur.

Figure 1



This strong opinion is surprising, given that so few real online attacks have affected US critical infrastructure to date. Although there have been examples of critical infrastructure incidents over the past decade — including Havex, BlackEnergy, and a series of attacks on the SWIFT global bank transfer system in late 2016 — reported compromises of critical infrastructure systems have been relatively rare. Yet the majority of Black Hat Attendee Survey respondents believe that another successful attack is likely to occur in the next 24 months.

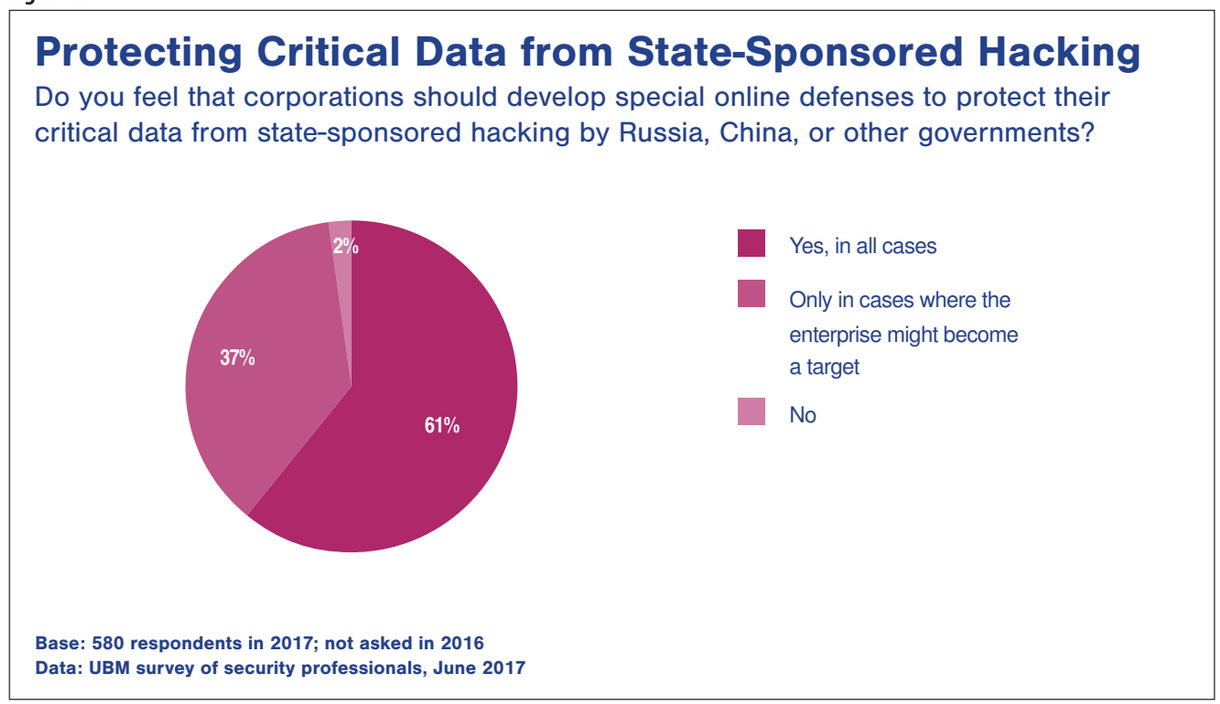
Is the United States prepared to respond to such an attack? Most security professionals don't believe so. In our survey, only 26% of respondents expressed confidence that US government and defense forces are equipped and trained to respond appropriately to a cyber

attack on critical infrastructure. Again, the figures are surprising and concerning, given that some 40% of respondents play an IT security role in critical-infrastructure industries, including government, financial services, healthcare, energy, telecommunications, and utilities.

The data is a clear warning from the nation's top cybersecurity professionals that US critical infrastructure is at risk. Much of respondents' concern seems to stem from recent developments in the geopolitical situation in cyberspace, and their lack of confidence that the current White House administration will be able to meet the challenge.

Recent state-sponsored cyber attacks — including alleged Russian interference in US elections, Chinese cyber espionage on US corporations, and the alleged connection between North Korea and the spread of the WannaCry ransomware worm in May — have eroded IT security professionals' confidence in critical infrastructure security. In fact, almost 69% of Black Hat Attendee Survey respondents said that recent activity emanating from Russia and China has made US enterprise data less secure (**Figure 1**). Sixty-one percent said they believe corporations should develop special online defenses to protect their critical data from state-sponsored hacking (**Figure 2**).

Figure 2



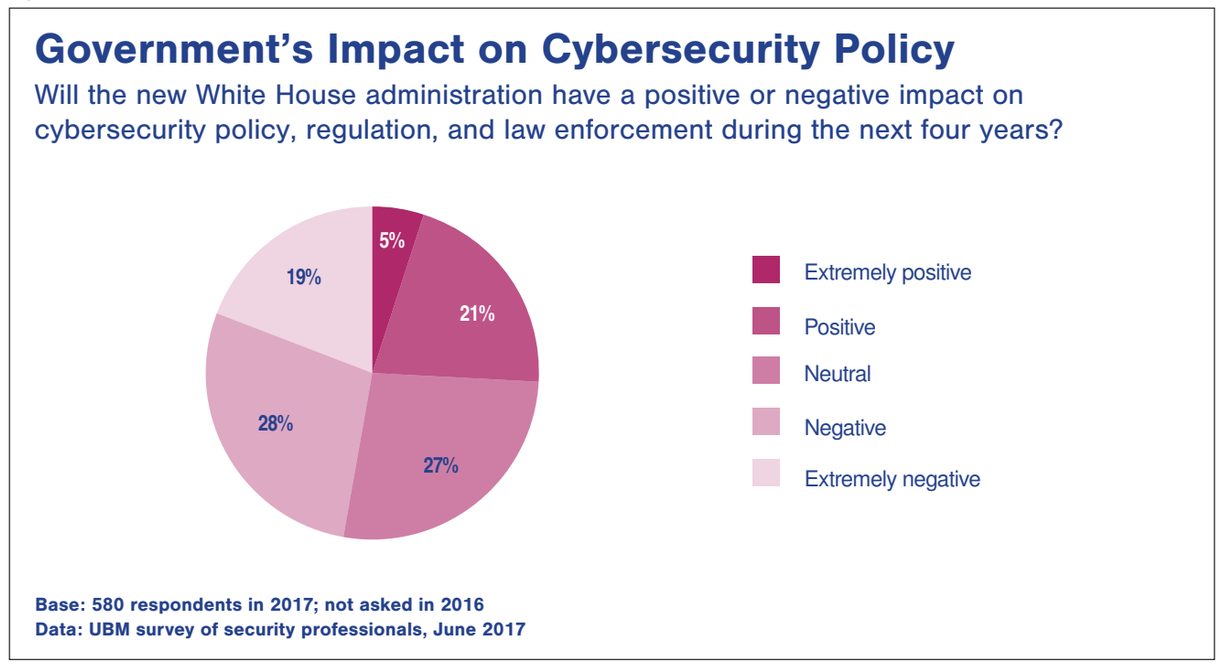
The recent election of Donald Trump as president of the United States has not boosted security professionals' confidence in the federal government's cybersecurity leadership. In our survey, only 26% of respondents said they believe the new White House administration will have a positive impact on cybersecurity policy, regulation, and law enforcement over the next four years (**Figure 3**). Twenty-seven percent were neutral; 47% said the administration's impact will be negative (28%) or extremely negative (19%).

The erosion of confidence in broader data security has also been affected by attackers' growing use of the WikiLeaks site to publish stolen information. From the release of

Democratic National Committee emails during the 2016 election to the Shadow Brokers' April dump of CIA hacking tools to the public, WikiLeaks has become a frequent outlet for exposure of critical information by online attackers and whistle-blowers. Some 61% of respondents to the survey said they believe WikiLeaks is having an impact on the way corporations and government agencies conduct their operations (**Figure 1**). Thirty-two percent of IT security pros oppose the work done by WikiLeaks; 31% are in favor of it, with 37% remaining neutral.

The combination of increased nation-state hacking, a lack of cyber preparedness in government, and the availability of sites that publish stolen data, including WikiLeaks, is a recipe for concerns about an imminent, successful cyber attack on US infrastructure, the Black Hat Attendee Survey data indicates. And most respondents feel that government and defense agencies are ill-equipped to respond to such an attack when it happens.

Figure 3



Enterprise IT Security Remains at Risk

While security professionals' concerns about the broader critical infrastructure are heightened, their concerns about their own enterprises remain high as well. Just as they expect hackers to crack key institutions in the very near future, they also expect their own organizations to be breached as well.

More than two-thirds (67%) of the respondents to the Black Hat Attendee Survey believe it likely that their organizations will have to respond to a major security breach in the next 12 months (**Figure 4**). While this figure is down slightly from 2016's 72%, it indicates that the vast majority of enterprise security professionals remain resigned to the conclusion that their defenses will fail at least once in the coming year, potentially leading to the compromise of critical data and intellectual property.

And, as in past Black Hat surveys, the most savvy security professionals continue to feel unprepared to respond to these expected breaches. In the 2017 survey, 71% of security

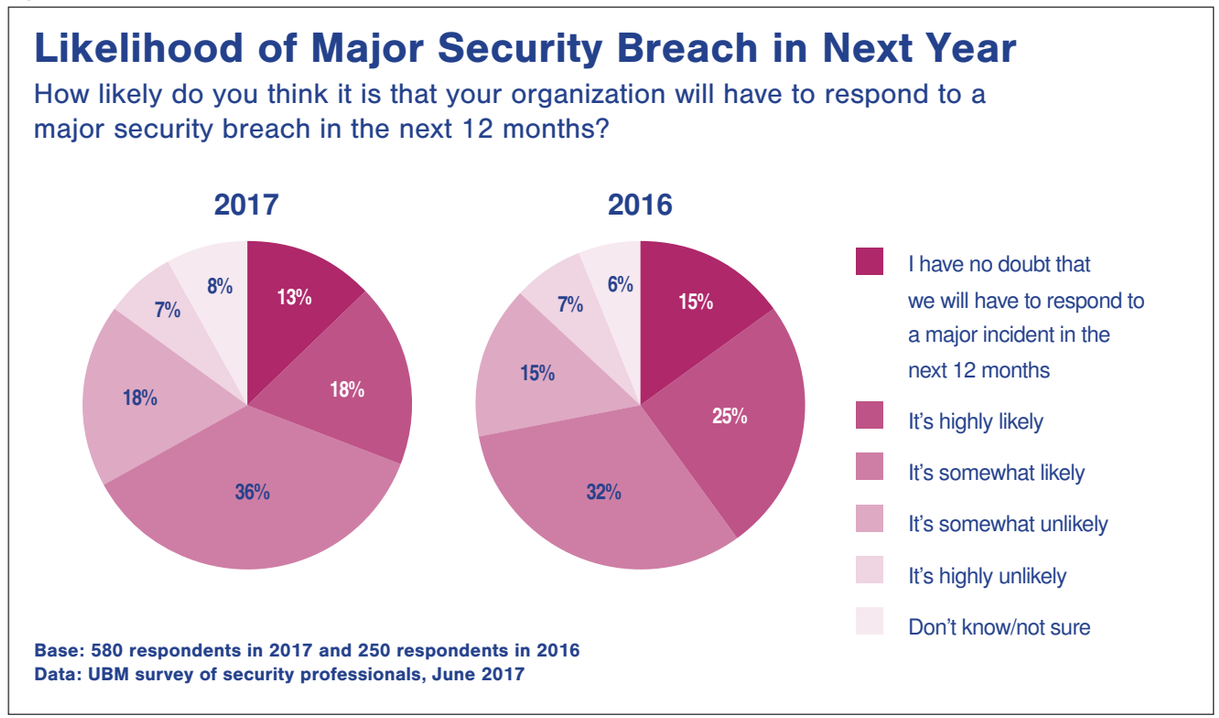
pros said they don't feel they have enough staff to defend their organizations against current threats, down only slightly from 2016's 74% (**Figure 5**). Fifty-eight percent said they don't have enough in the budget to meet the current threat, down slightly from 2016's 63%. And 67% said they do not have enough training to perform the security functions required of them, the same percentage as last year.

The concerns of these security professionals are not unwarranted. According to the Identity Theft Resource Center, there were 698 major data breaches reported by US-based organizations as of May 30, 2017, representing more than 10.2 million compromised records. At their current rate, data breaches this year could outpace those reported in 2016, which were up over 2015. Clearly, most enterprises still have not solved their IT security problems, and huge breaches such as those reported by Dun & Bradstreet (33 million records) and OneLogin (more than 2,000 companies and over 300 application vendors) may only be the beginning of this year's list of data breach headlines.

Security pros don't uniformly agree on which threats they see as most potentially dangerous or on their priorities for defense. When asked which threats cause the greatest concern (and with as many as three responses allowed), 50% of Black Hat survey respondents cited phishing, social network exploits, or other forms of social engineering, up from 46% in 2016 (**Figure 6**). Forty-five percent cited sophisticated attacks aimed directly at the organization (up from 43% last year). Aside from those two categories of threats, however, respondents were mixed in their concerns: accidental data leaks (21%) finished third in order (up from 15% in 2016), and polymorphic malware (20%) finished fourth (up from 15% percent last year).

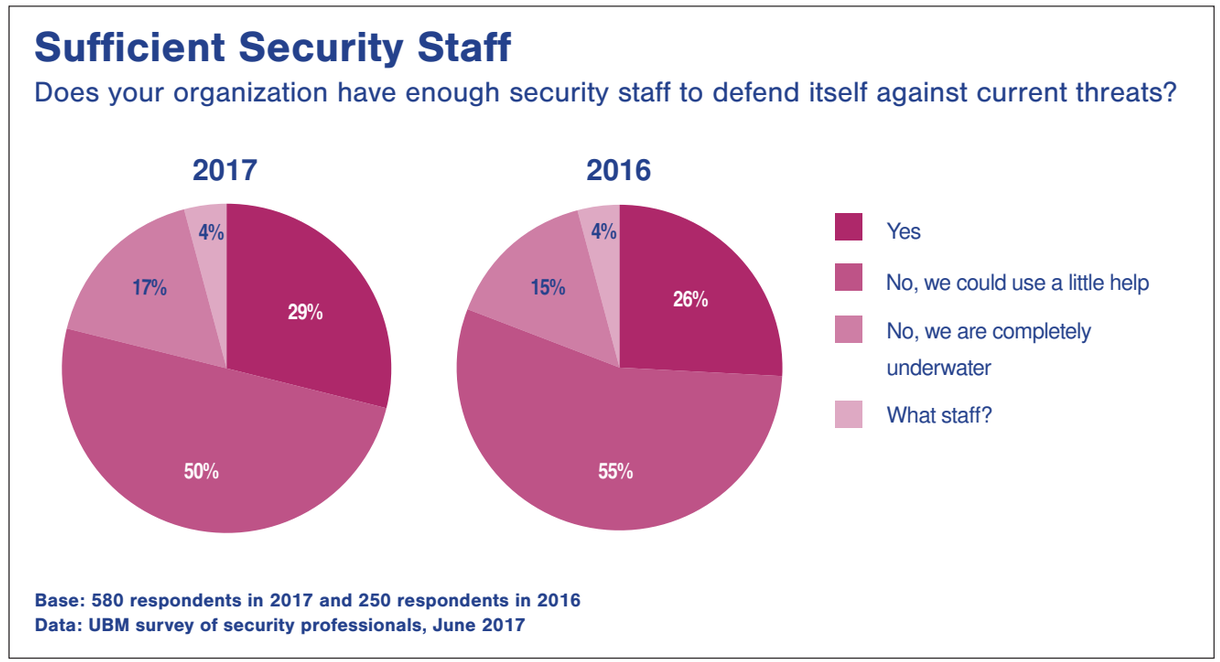
And these aren't the only threats that concern Black Hat survey respondents. The rapid

Figure 4



increase in the spread of ransomware, as epitomized by the release of the WannaCry worm in May, was cited by 36% as the most serious new threat to emerge in the past 12 months, down slightly from 37% in 2016 (**Figure 7**). Social engineering attacks aimed directly at individuals in a specific enterprise were cited by 19% (down from 20% last year). Although it wasn't listed in the survey, several respondents registered write-in concerns over the release of CIA hacking tools by the Shadow Brokers earlier this year.

Figure 5



What's the Problem?

IT security professionals also disagree on the most common causes of today's threats and breaches. As stated previously, Black Hat survey respondents cited social engineering and targeted attacks as their greatest concerns in the enterprise. But when asked about the weakest links in today's enterprise defenses, 38% pointed to end users who violate security policy and are too easily fooled by social engineering attacks, up 10 points from 2016 (**Figure 8**). The second most frequently cited response was a lack of comprehensive security architecture that goes beyond firefighting — a clear mandate for better, more comprehensive enterprise security strategy and architecture.

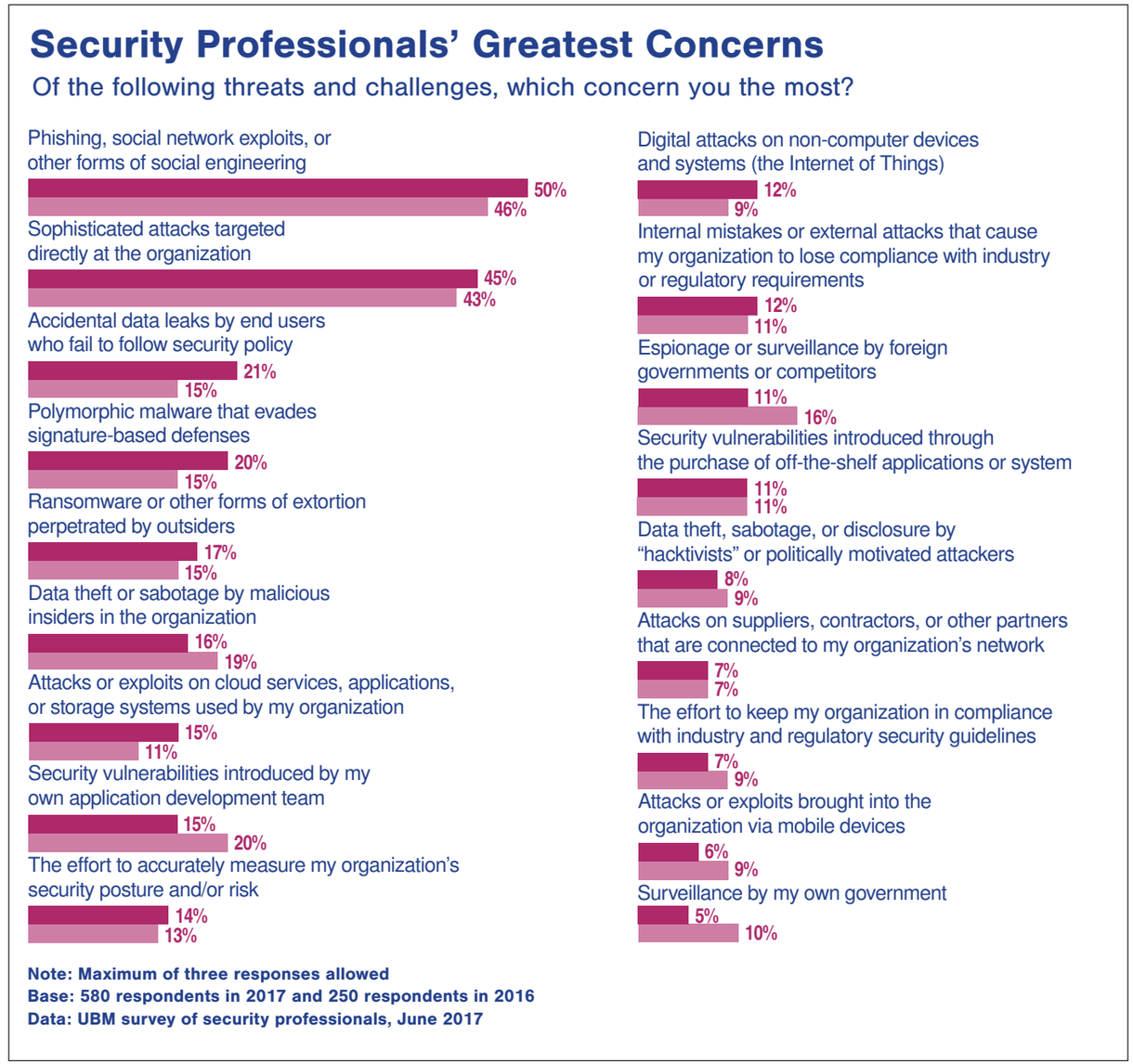
The shortage of skilled security professionals was also a key issue for many respondents. When asked to identify the primary reason why enterprise IT security strategies fail, 31% of Black Hat survey respondents cited a shortage of qualified people and skills (**Figure 9**). This response tracks closely with recent research from the security professional association (ISC)[2], which predicts that there will be a shortfall of 1.8 million cybersecurity workers by 2022.

The second reason cited for security strategy failure was also a common theme among Black Hat survey respondents: the disconnect between the IT security team and corporate upper management. As in past years, security pros say they continue to struggle with corporate management that sets priorities differently than they would.

For example, respondents registered sophisticated, targeted attacks as their #2 concern in our survey. But when they were asked how they actually spend their time, security pros said that the effort to manage security posture and risk (35%) and the effort to keep the organization in compliance with industry and regulatory guidelines (32%) were among the top three most time-consuming tasks (**Figure 10**). Defense against sophisticated, targeted attacks (16%) ranked eighth among the tasks that receive the most time and attention. By contrast, respondents said compliance ranks second in importance among top executives, potentially driving a misallocation of security manpower.

Security budgets and spending, not surprisingly, mirror many of the same priorities as time and manpower. When asked how their IT security budgets are spent, 36% of Black Hat survey respondents said that compliance is the top priority, up from 31% in 2016 (**Figure 11**). The effort to measure security posture and risk — a priority that finished ninth among security professionals but third among top executives — is a top spending priority for 23% of respondents, about the same percentage as last year, making it a tie for #2 as the

Figure 6

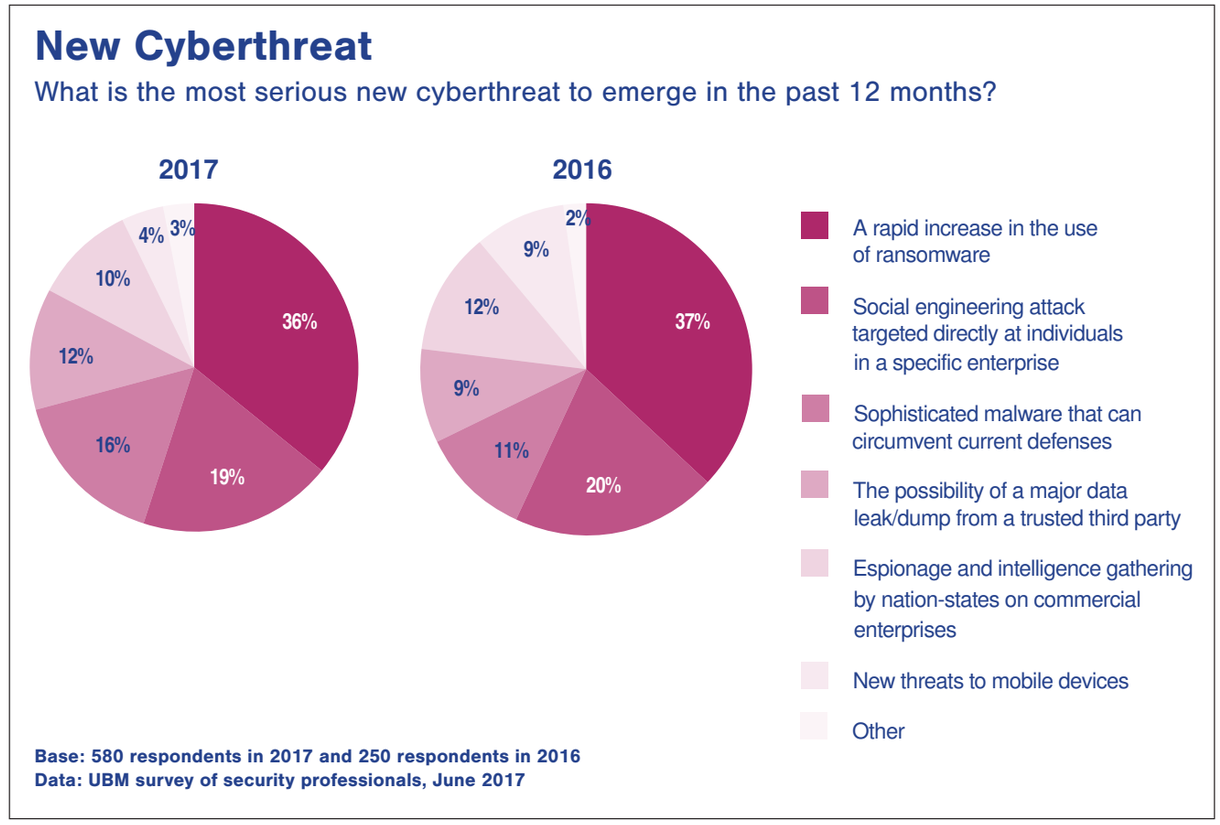


overall security spending priority. Clearly, top management holds the budget purse strings and steers spending toward its own priorities.

Interestingly, some Black Hat survey respondents say that management's understanding of the security threat is getting better. Thirty-three percent of security pros in the 2017 Black Hat survey said that non-security pros in their organizations understand the threat and support IT security initiatives (**Figure 12**). This figure rose from 25% in 2016. Still, with only one in three respondents indicating that their management understands the threat, it is clear that IT security people still have a lot of communicating left to do — and the disconnect between management and IT security departments continues to take a toll on IT security priorities and initiatives.

The problem isn't just educating management, but end users as well. As stated previously, 38% of survey respondents say that end users who violate security policy are the weakest link in enterprise cyber defense. Fifty-six percent of respondents also said that a lack of security awareness about phishing and other social engineering attacks is the most threatening challenge facing the average US consumer (**Figure 13**). These responses suggest that end users are the greatest weakness in enterprise data defense. They may also be the greatest threat: 39% of security pros say that the attacker they fear most is the one who has inside knowledge of their own organization — most frequently, an end user (**Figure 14**).

Figure 7



Hiring Hurdles

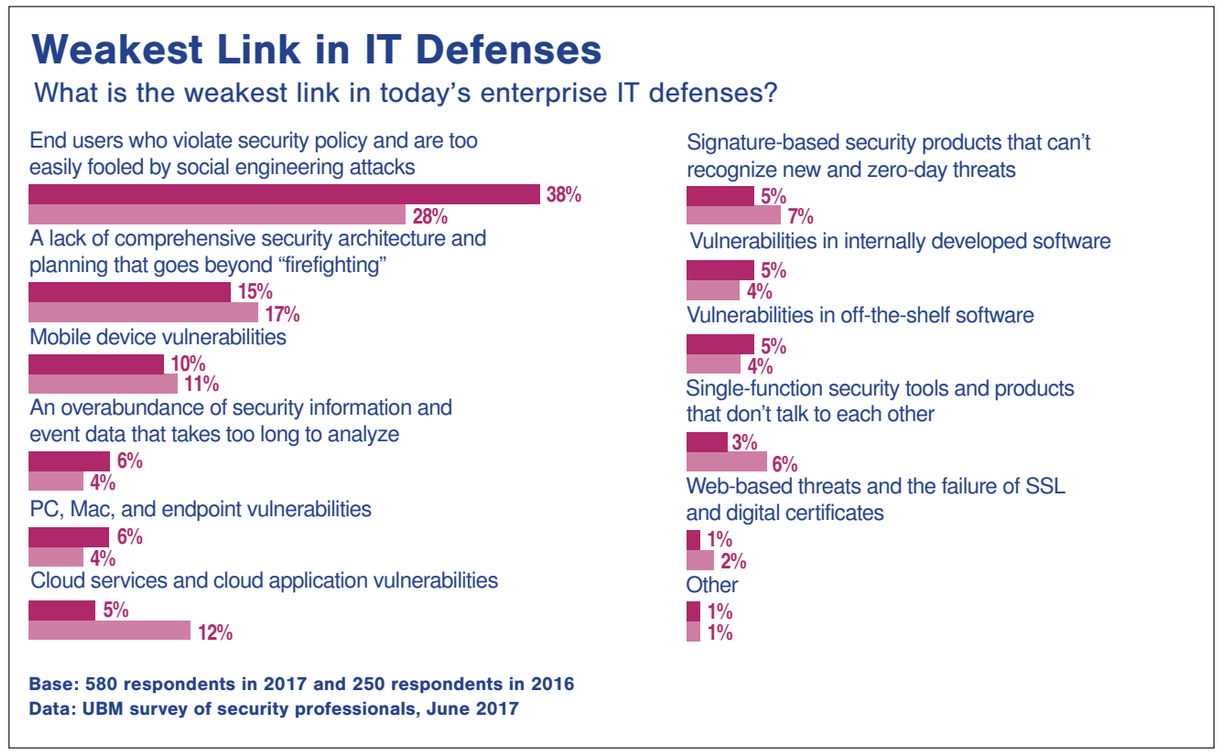
Although non-security-savvy management and end users often inhibit security professionals' defense tactics and strategies, it's the

shortage of skilled professionals in the IT security department itself that was cited most frequently as the top challenge facing Black Hat respondents' organizations. Without enough skilled people, security pros feel they cannot respond quickly enough to current threats, leaving their enterprises vulnerable to attack.

Seventy-one percent of Black Hat survey respondents said they don't believe their organizations have enough security staff to defend their organizations' critical data against current threats (**Figure 5**). However, it was also clear that the pool of available security pros is not growing: only 12% of respondents said they are actively pursuing new employment, and just 20% said they are even updating their resumes (**Figure 15**). Most of the security professionals who participated in the survey said they're happy in their current positions, and they have no immediate plans to do any job-hunting.

Another reason for the shortage of IT security professionals is a critical shortage of women and minorities entering the field. In its study, (ISC)^2 estimated the percentage of women in information security positions at about 11% — a figure that has stayed fairly constant over the last three years.

Figure 8



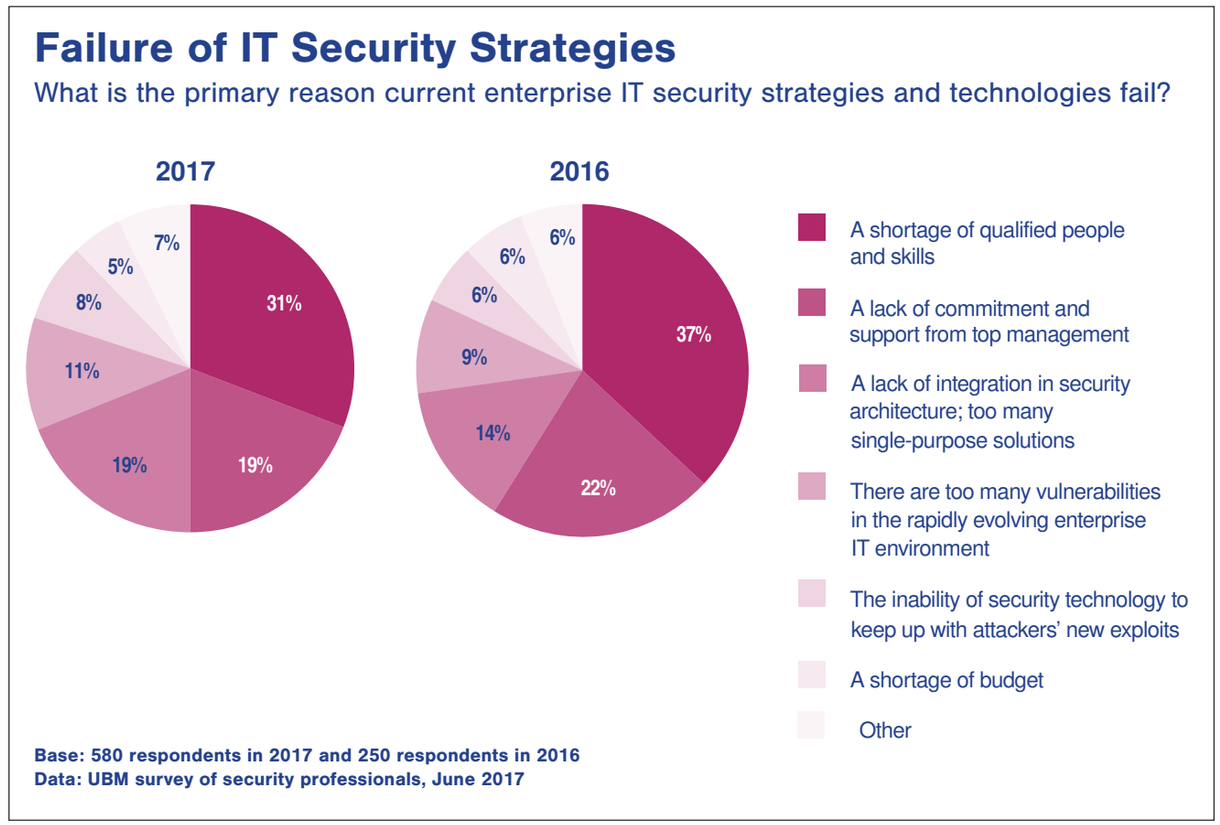
Although there has been significant discussion around the effort to increase diversity in IT security over the past few years, this does not yet appear to be a mandate. Only 45% of respondents to the Black Hat survey said they're concerned about the shortage of women and minorities in the profession; 20% said they're unconcerned (**Figure 1**). When asked why diversity is so low in IT security, most blamed society (57%) or schools (45%) for not doing enough to encourage women and minorities to consider a career in the field.

Future Issues

Interestingly, although respondents to the Black Hat survey today are most concerned with social engineering and targeted attacks, the majority believe that their priorities will change in the not-too-distant future. Digital attacks on non-computer systems — the Internet of Things — currently ranks tenth among security professionals' chief worries; but when asked what they believe they will be most concerned about two years from now, IoT security ranks first on the list, at 34% (up from 28% in 2016) (**Figure 16**).

These concerns would appear to be well-founded, as security researchers continue to prove vulnerabilities in non-computer systems such as automobiles and medical devices. In October 2016, cyber attacks on the company Dyn, which services many Internet websites, effectively jammed IP-connected devices such as closed-circuit TV cameras, DVRs, and routers, effectively clogging Internet services for many users. Many experts also worry that attacks on industrial control systems — the intelligent, non-computer devices that run industry-specific systems in industries such as energy, utilities, and telecommunications — could be at the heart of any new attack on US critical infrastructure.

Figure 9



Conclusion

Most of the most experienced and best-informed IT security professionals in the industry believe that a successful breach of US critical infrastructure will occur in the next two years and that major breaches of their own organizations will occur within the next 12 months. A majority of those security professionals also believe that US defense, government, and their own organizations are ill-prepared to meet the threat. Clearly, this data is a call to action for those who manage and

fund critical-infrastructure IT systems — and a warning that all enterprises need to take a closer look at their defenses and their incident response initiatives.

APPENDIX

Figure 10

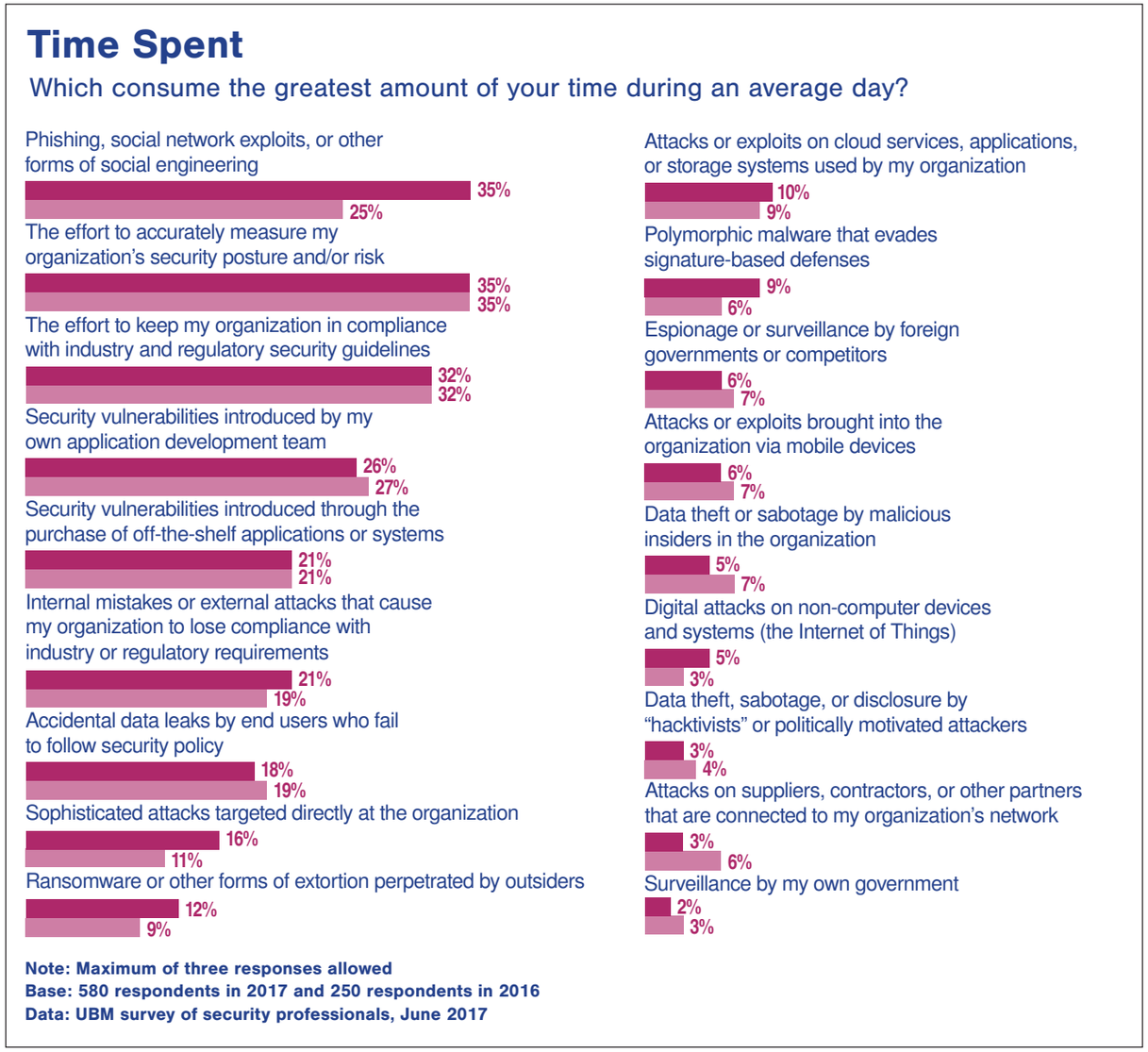


Figure 11

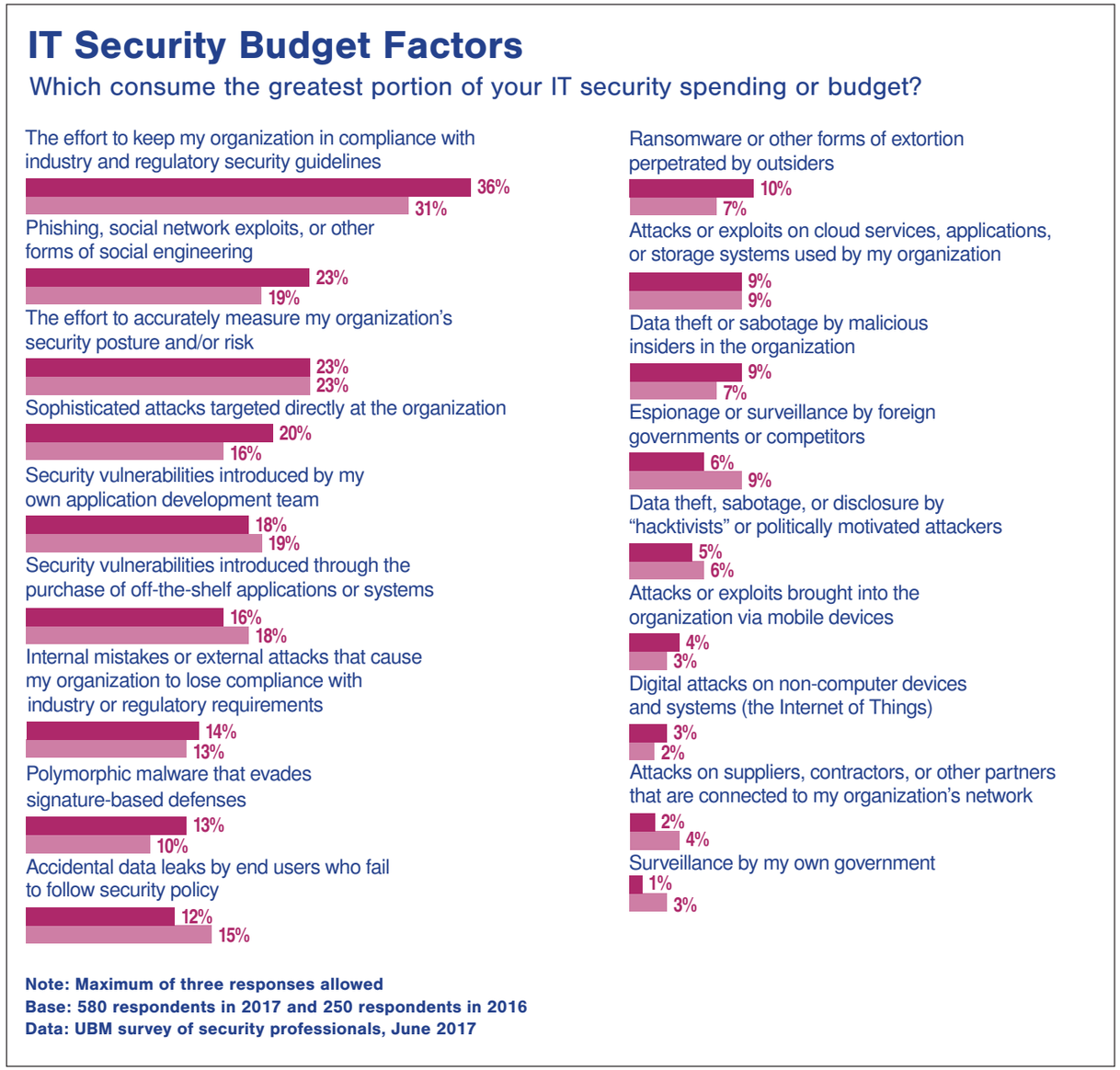
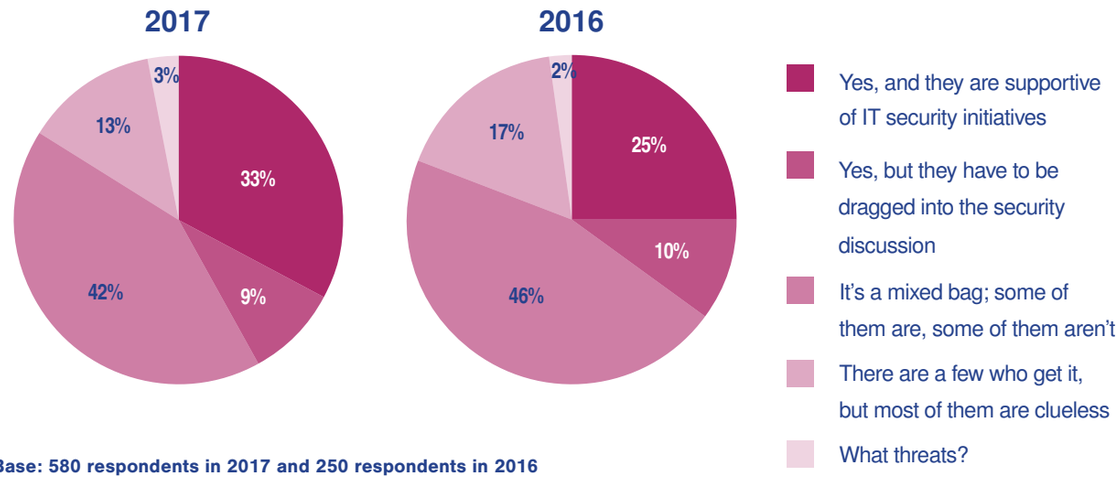

IT Security Budget Factors
Which consume the greatest portion of your IT security spending or budget?
The effort to keep my organization in compliance with industry and regulatory security guidelines
36%
31%
Phishing, social network exploits, or other forms of social engineering
23%
19%
The effort to accurately measure my organization's security posture and/or risk
23%
23%
Sophisticated attacks targeted directly at the organization
20%
16%
Security vulnerabilities introduced by my own application development team
18%
19%
Security vulnerabilities introduced through the purchase of off-the-shelf applications or systems
16%
18%
Internal mistakes or external attacks that cause my organization to lose compliance with industry or regulatory requirements
14%
13%
Polymorphic malware that evades signature-based defenses
13%
10%
Accidental data leaks by end users who fail to follow security policy
12%
15%
Ransomware or other forms of extortion perpetrated by outsiders
10%
7%
Attacks or exploits on cloud services, applications, or storage systems used by my organization
9%
9%
Data theft or sabotage by malicious insiders in the organization
9%
7%
Espionage or surveillance by foreign governments or competitors
6%
9%
Data theft, sabotage, or disclosure by "hacktivists" or politically motivated attackers
5%
6%
Attacks or exploits brought into the organization via mobile devices
4%
3%
Digital attacks on non-computer devices and systems (the Internet of Things)
3%
2%
Attacks on suppliers, contractors, or other partners that are connected to my organization's network
2%
4%
Surveillance by my own government
1%
3%
Note: Maximum of three responses allowed
Base: 580 respondents in 2017 and 250 respondents in 2016
Data: UBM survey of security professionals, June 2017

Figure 12

Understanding IT Security Threat to Organization

Do non-security professionals in your organization understand the IT security threat that your organization faces today?

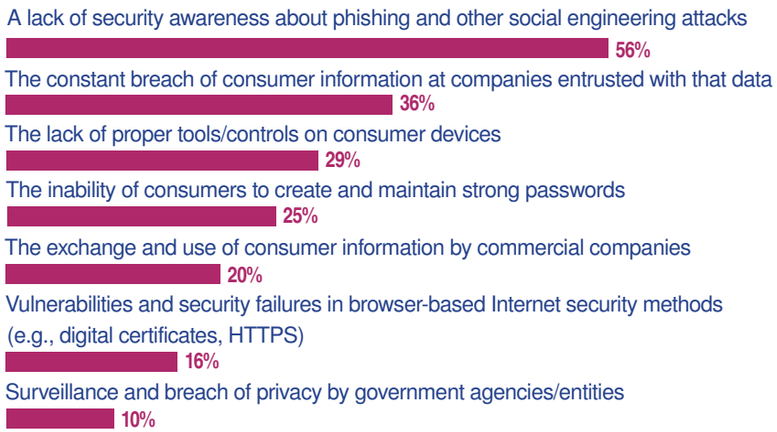


Base: 580 respondents in 2017 and 250 respondents in 2016
Data: UBM survey of security professionals, June 2017

Figure 13

Most Significant Threats to Average Consumer

Which IT security challenges do you see as most threatening to the average US consumer?



Note: Maximum of two responses allowed
Base: 580 respondents in 2017; not asked in 2016
Data: UBM survey of security professionals, June 2017

Figure 14

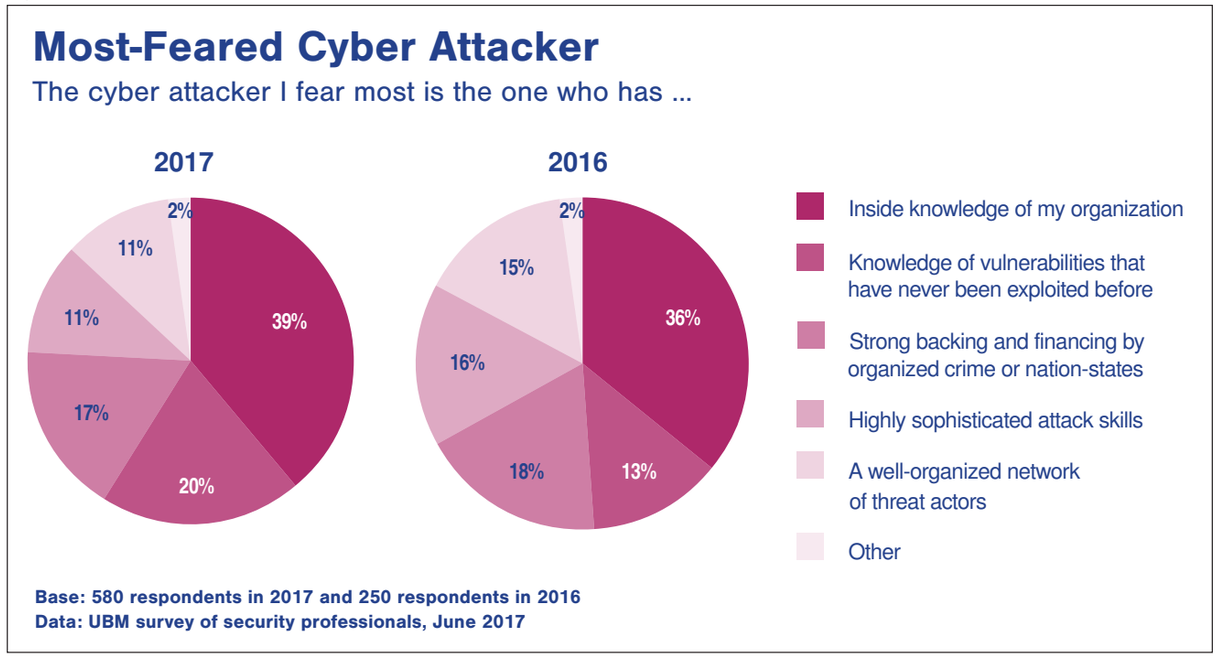
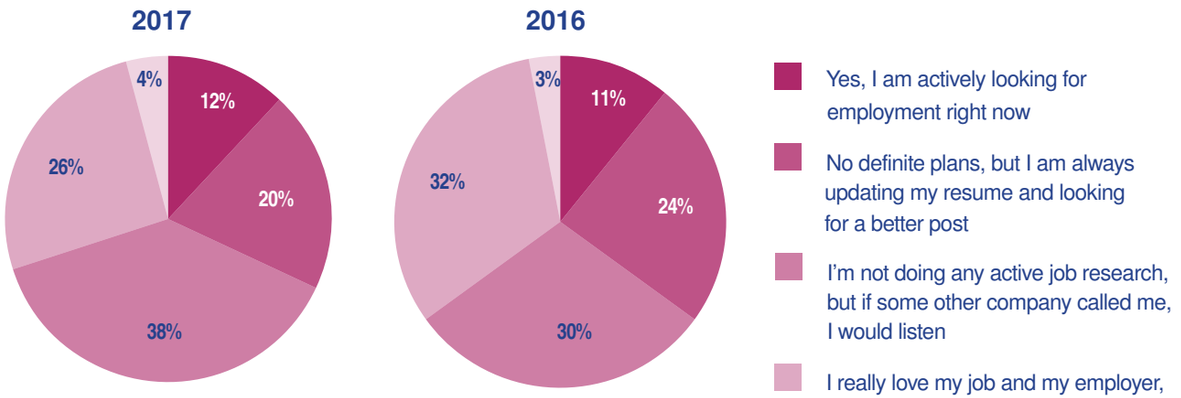

Most-Feared Cyber Attacker
The cyber attacker I fear most is the one who has ...
2017
2016
39%
20%
17%
11%
11%
2%
36%
13%
18%
16%
15%
2%
Inside knowledge of my organization
Knowledge of vulnerabilities that have never been exploited before
Strong backing and financing by organized crime or nation-states
Highly sophisticated attack skills
A well-organized network of threat actors
Other
Base: 580 respondents in 2017 and 250 respondents in 2016
Data: UBM survey of security professionals, June 2017

Figure 15

Plans to Seek an IT Security Position

Do you have plans to seek an IT security position anytime in the near future?



Base: 580 respondents in 2017 and 250 respondents in 2016
Data: UBM survey of security professionals, June 2017

Figure 16

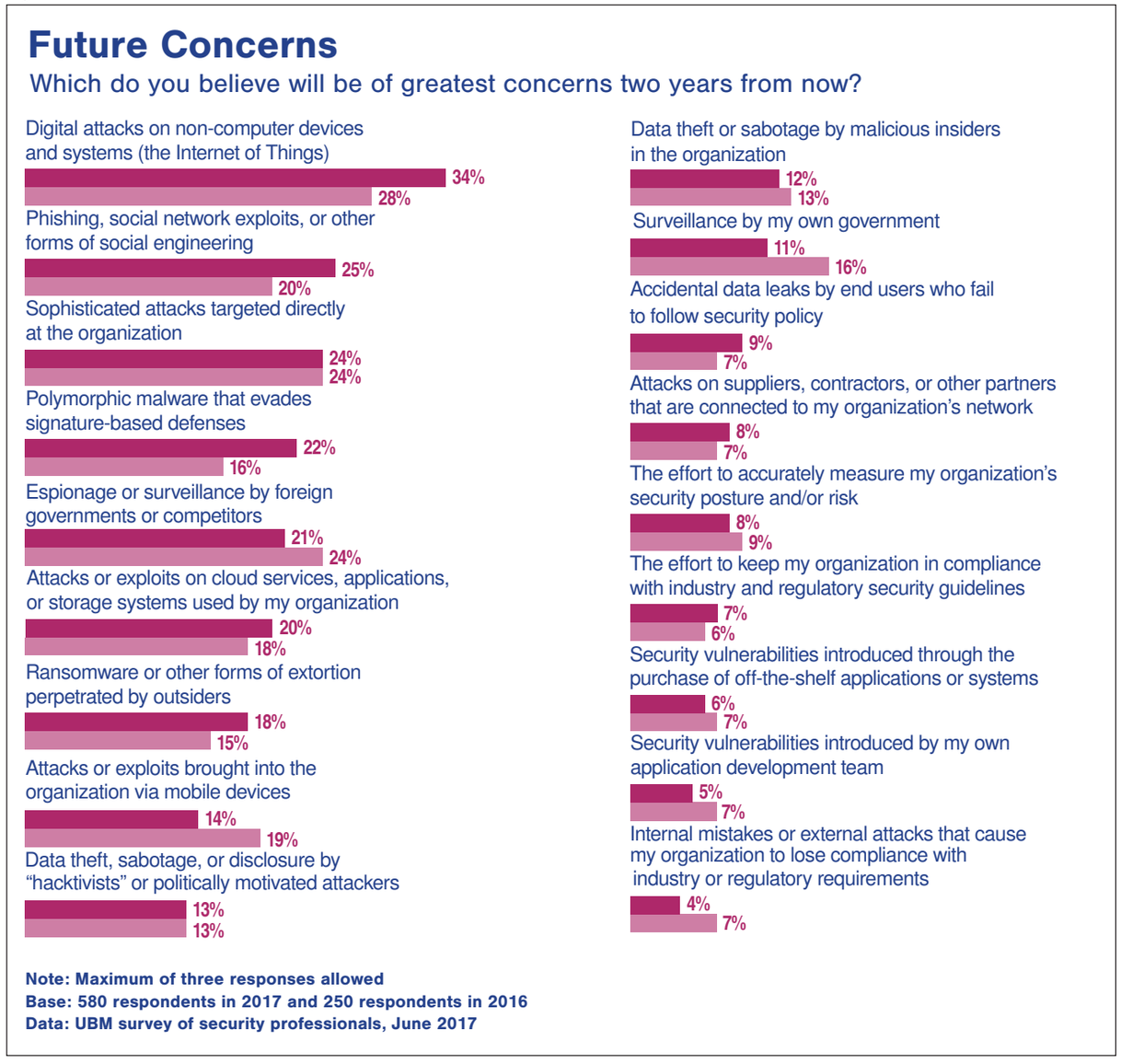

Future Concerns
Which do you believe will be of greatest concerns two years from now?
Digital attacks on non-computer devices and systems (the Internet of Things)
34%
28%
Phishing, social network exploits, or other forms of social engineering
25%
20%
Sophisticated attacks targeted directly at the organization
24%
24%
Polymorphic malware that evades signature-based defenses
22%
16%
Espionage or surveillance by foreign governments or competitors
21%
24%
Attacks or exploits on cloud services, applications, or storage systems used by my organization
20%
18%
Ransomware or other forms of extortion perpetrated by outsiders
18%
15%
Attacks or exploits brought into the organization via mobile devices
14%
19%
Data theft, sabotage, or disclosure by "hacktivists" or politically motivated attackers
13%
13%
Data theft or sabotage by malicious insiders in the organization
12%
13%
Surveillance by my own government
11%
16%
Accidental data leaks by end users who fail to follow security policy
9%
7%
Attacks on suppliers, contractors, or other partners that are connected to my organization's network
8%
7%
The effort to accurately measure my organization's security posture and/or risk
8%
9%
The effort to keep my organization in compliance with industry and regulatory security guidelines
7%
6%
Security vulnerabilities introduced through the purchase of off-the-shelf applications or systems
6%
7%
Security vulnerabilities introduced by my own application development team
5%
7%
Internal mistakes or external attacks that cause my organization to lose compliance with industry or regulatory requirements
4%
7%
Note: Maximum of three responses allowed
Base: 580 respondents in 2017 and 250 respondents in 2016
Data: UBM survey of security professionals, June 2017

Figure 17


Executive Management's Concerns
Which are of greatest concern to your company's top executives or management?
Sophisticated attacks targeted directly at the organization
34%
33%
The effort to keep my organization in compliance with industry and regulatory security guidelines
30%
28%
Phishing, social network exploits, or other forms of social engineering
28%
24%
Data theft or sabotage by malicious insiders in the organization
18%
17%
Ransomware or other forms of extortion perpetrated by outsiders
18%
10%
The effort to accurately measure my organization's security posture and/or risk
18%
19%
Accidental data leaks by end users who fail to follow security policy
18%
20%
Internal mistakes or external attacks that cause my organization to lose compliance with industry or regulatory requirements
14%
16%
Espionage or surveillance by foreign governments or competitors
11%
13%
Data theft, sabotage, or disclosure by "hacktivists" or politically motivated attackers
10%
14%
Security vulnerabilities introduced by my own application development team
9%
9%
Attacks or exploits on cloud services, applications, or storage systems used by my organization
8%
7%
Attacks on suppliers, contractors, or other partners that are connected to my organization's network
6%
4%
Polymorphic malware that evades signature-based defenses
6%
5%
Digital attacks on non-computer devices and systems (the Internet of Things)
5%
3%
Security vulnerabilities introduced through the purchase of off-the-shelf applications or systems
5%
4%
Attacks or exploits brought into the organization via mobile devices
4%
3%
Surveillance by my own government
3%
1%
Note: Maximum of three responses allowed
Base: 580 respondents in 2017 and 250 respondents in 2016
Data: UBM survey of security professionals, June 2017

Figure 18

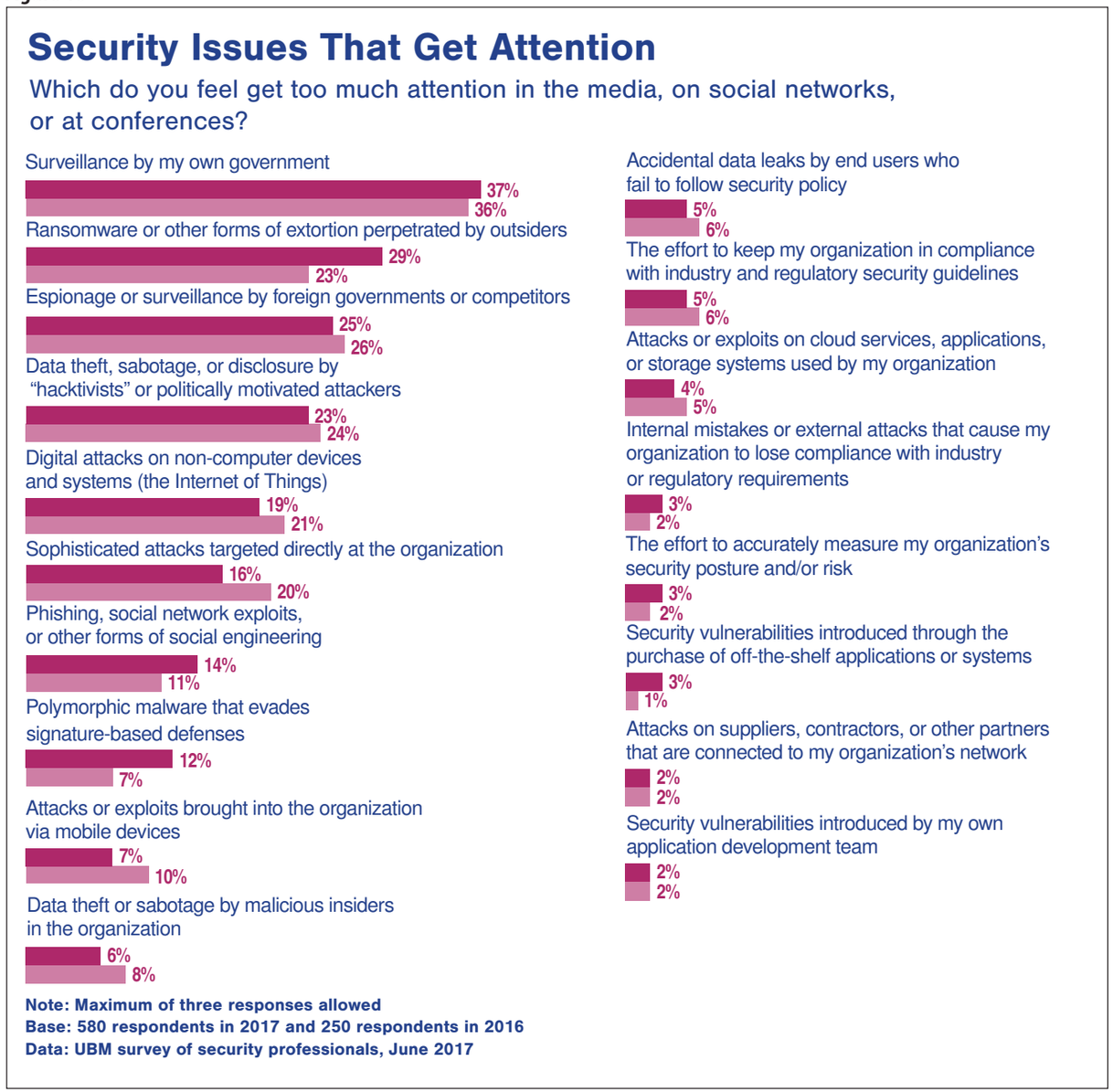

Security Issues That Get Attention
Which do you feel get too much attention in the media, on social networks, or at conferences?
Surveillance by my own government
37%
36%
Ransomware or other forms of extortion perpetrated by outsiders
29%
23%
Espionage or surveillance by foreign governments or competitors
25%
26%
Data theft, sabotage, or disclosure by "hacktivists" or politically motivated attackers
23%
24%
Digital attacks on non-computer devices and systems (the Internet of Things)
19%
21%
Sophisticated attacks targeted directly at the organization
16%
20%
Phishing, social network exploits, or other forms of social engineering
14%
11%
Polymorphic malware that evades signature-based defenses
12%
7%
Attacks or exploits brought into the organization via mobile devices
7%
10%
Data theft or sabotage by malicious insiders in the organization
6%
8%
Accidental data leaks by end users who fail to follow security policy
5%
6%
The effort to keep my organization in compliance with industry and regulatory security guidelines
5%
6%
Attacks or exploits on cloud services, applications, or storage systems used by my organization
4%
5%
Internal mistakes or external attacks that cause my organization to lose compliance with industry or regulatory requirements
3%
2%
The effort to accurately measure my organization's security posture and/or risk
3%
2%
Security vulnerabilities introduced through the purchase of off-the-shelf applications or systems
3%
1%
Attacks on suppliers, contractors, or other partners that are connected to my organization's network
2%
2%
Security vulnerabilities introduced by my own application development team
2%
2%
Note: Maximum of three responses allowed
Base: 580 respondents in 2017 and 250 respondents in 2016
Data: UBM survey of security professionals, June 2017

Figure 19

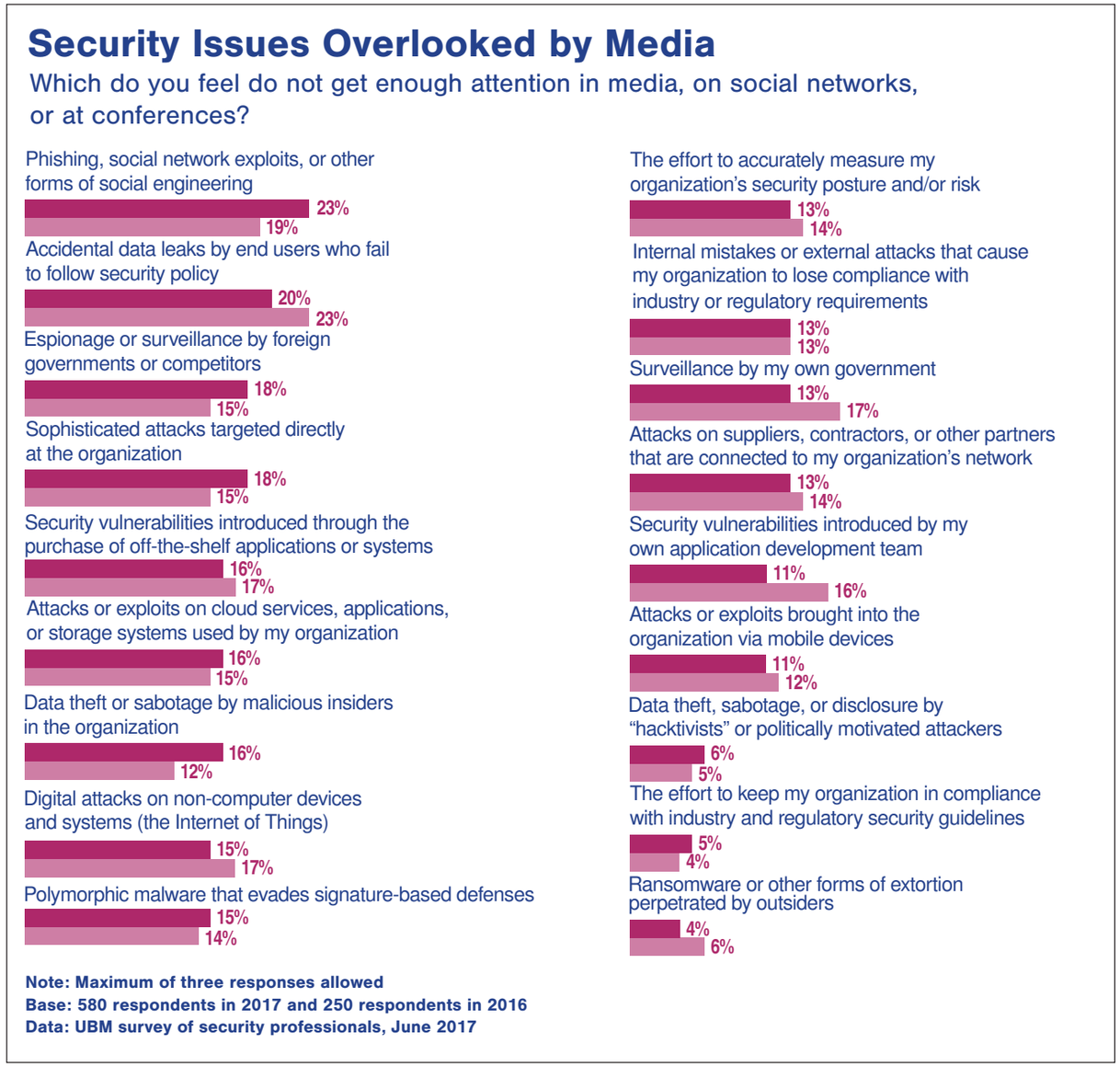
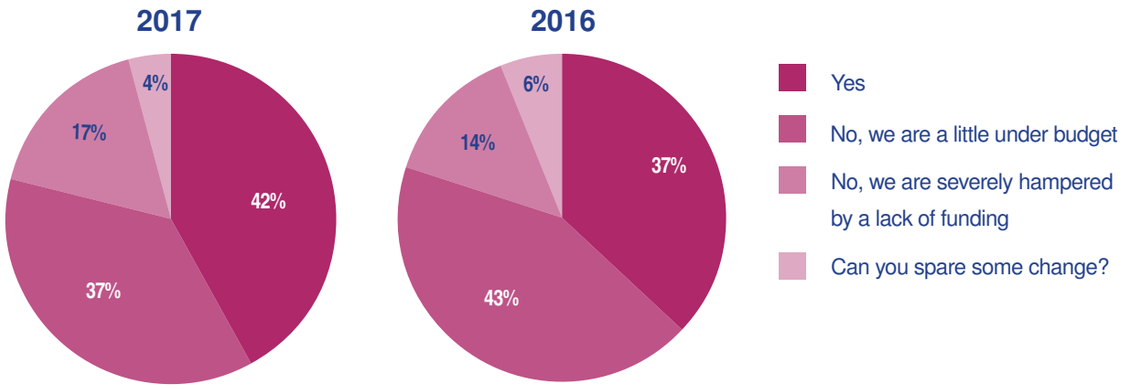

Security Issues Overlooked by Media
Which do you feel do not get enough attention in media, on social networks, or at conferences?
Phishing, social network exploits, or other forms of social engineering
23%
19%
Accidental data leaks by end users who fail to follow security policy
20%
23%
Espionage or surveillance by foreign governments or competitors
18%
15%
Sophisticated attacks targeted directly at the organization
18%
15%
Security vulnerabilities introduced through the purchase of off-the-shelf applications or systems
16%
17%
Attacks or exploits on cloud services, applications, or storage systems used by my organization
16%
15%
Data theft or sabotage by malicious insiders in the organization
16%
12%
Digital attacks on non-computer devices and systems (the Internet of Things)
15%
17%
Polymorphic malware that evades signature-based defenses
15%
14%
The effort to accurately measure my organization's security posture and/or risk
13%
14%
Internal mistakes or external attacks that cause my organization to lose compliance with industry or regulatory requirements
13%
13%
Surveillance by my own government
13%
17%
Attacks on suppliers, contractors, or other partners that are connected to my organization's network
13%
14%
Security vulnerabilities introduced by my own application development team
11%
16%
Attacks or exploits brought into the organization via mobile devices
11%
12%
Data theft, sabotage, or disclosure by "hacktivists" or politically motivated attackers
6%
5%
The effort to keep my organization in compliance with industry and regulatory security guidelines
5%
4%
Ransomware or other forms of extortion perpetrated by outsiders
4%
6%
Note: Maximum of three responses allowed
Base: 580 respondents in 2017 and 250 respondents in 2016
Data: UBM survey of security professionals, June 2017

Figure 20

Sufficient Security Budget

Does your organization have enough security budget to defend itself against current threats?

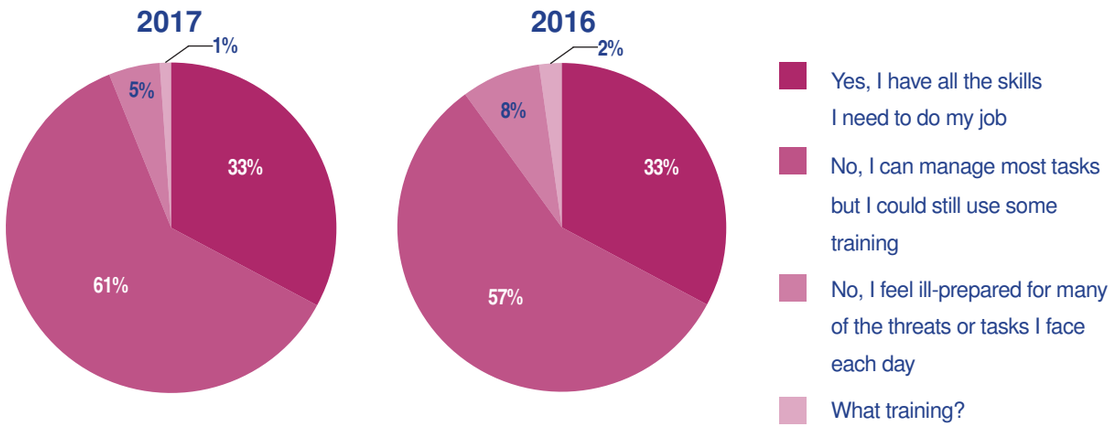


Base: 580 respondents in 2017 and 250 respondents in 2016
Data: UBM survey of security professionals, June 2017

Figure 21

Sufficient Training

Do you personally have enough training and skills to handle current threats and perform all of the security job functions that are required of you?

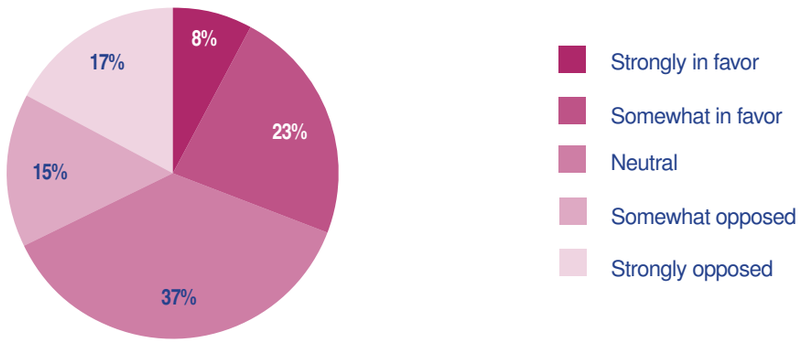


Base: 580 respondents in 2017 and 250 respondents in 2016
Data: UBM survey of security professionals, June 2017

Figure 22

WikiLeaks

What is your opinion of the work done by WikiLeaks?



Base: 580 respondents in 2017; not asked in 2016
Data: UBM survey of security professionals, June 2017

Figure 23

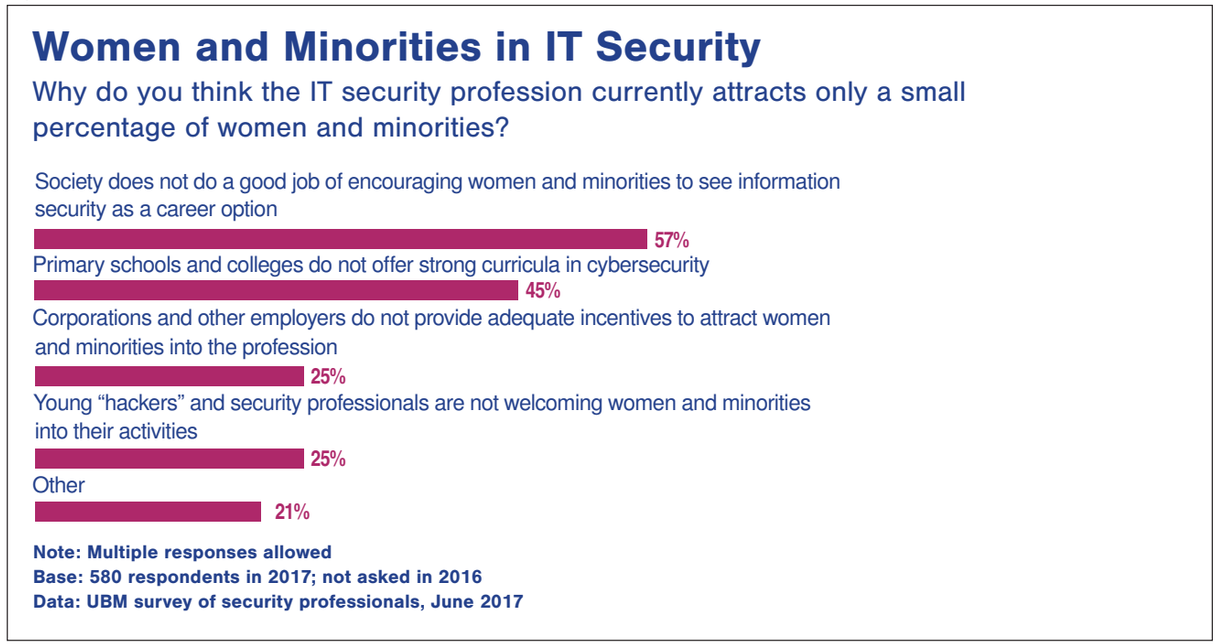

Women and Minorities in IT Security
Why do you think the IT security profession currently attracts only a small percentage of women and minorities?
Society does not do a good job of encouraging women and minorities to see information security as a career option
57%
Primary schools and colleges do not offer strong curricula in cybersecurity
45%
Corporations and other employers do not provide adequate incentives to attract women and minorities into the profession
25%
Young "hackers" and security professionals are not welcoming women and minorities into their activities
25%
Other
21%
Note: Multiple responses allowed
Base: 580 respondents in 2017; not asked in 2016
Data: UBM survey of security professionals, June 2017

Figure 24

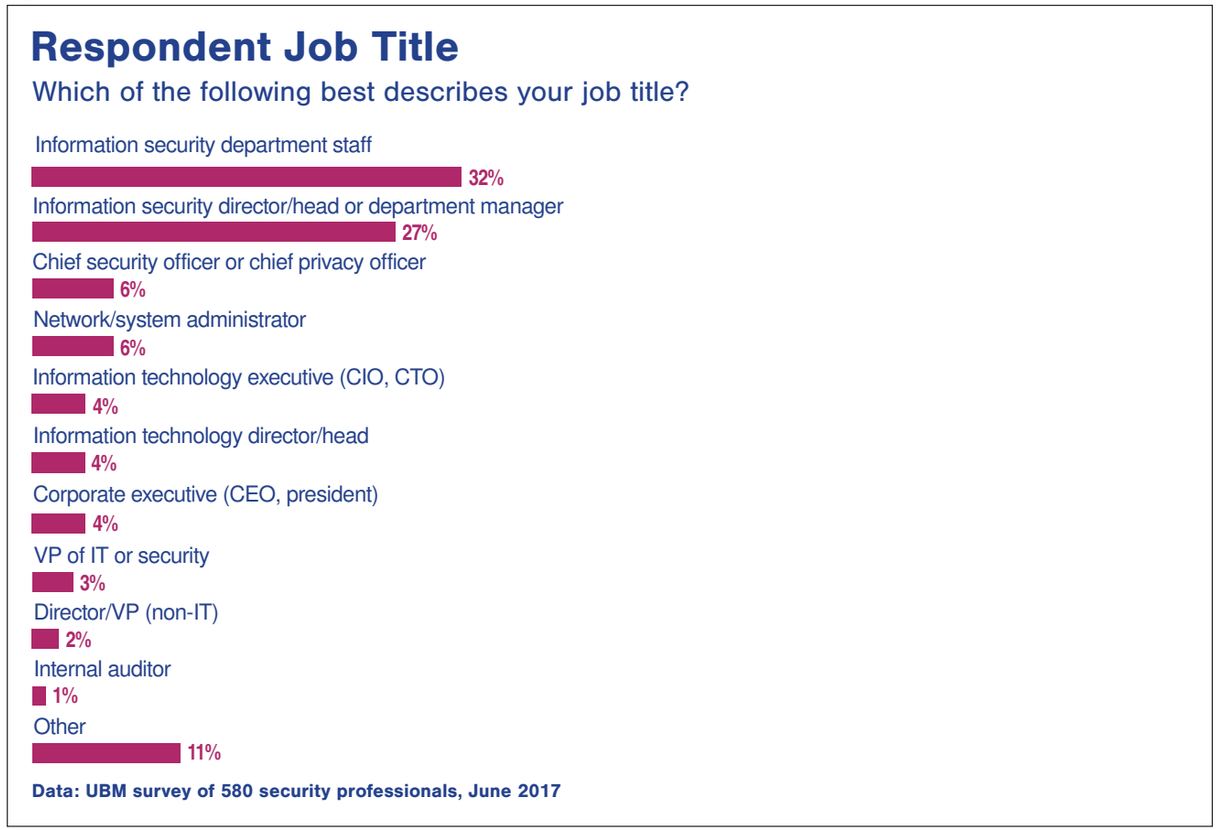
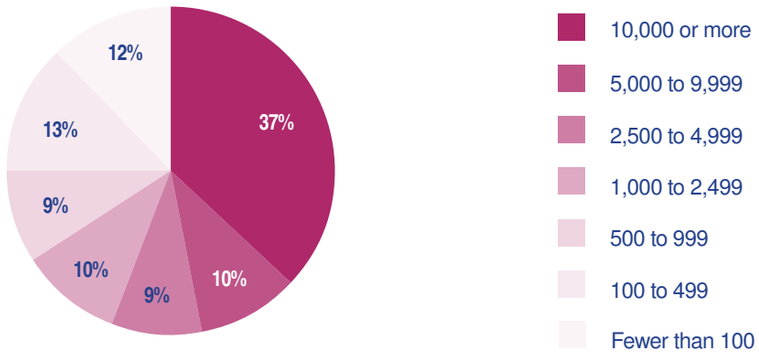

Respondent Job Title
Which of the following best describes your job title?
Information security department staff
32%
Information security director/head or department manager
27%
Chief security officer or chief privacy officer
6%
Network/system administrator
6%
Information technology executive (CIO, CTO)
4%
Information technology director/head
4%
Corporate executive (CEO, president)
4%
VP of IT or security
3%
Director/VP (non-IT)
2%
Internal auditor
1%
Other
11%
Data: UBM survey of 580 security professionals, June 2017

Figure 25

Respondent Company Size

How many employees are in your company in total?



Data: UBM survey of 580 security professionals, June 2017

Figure 26

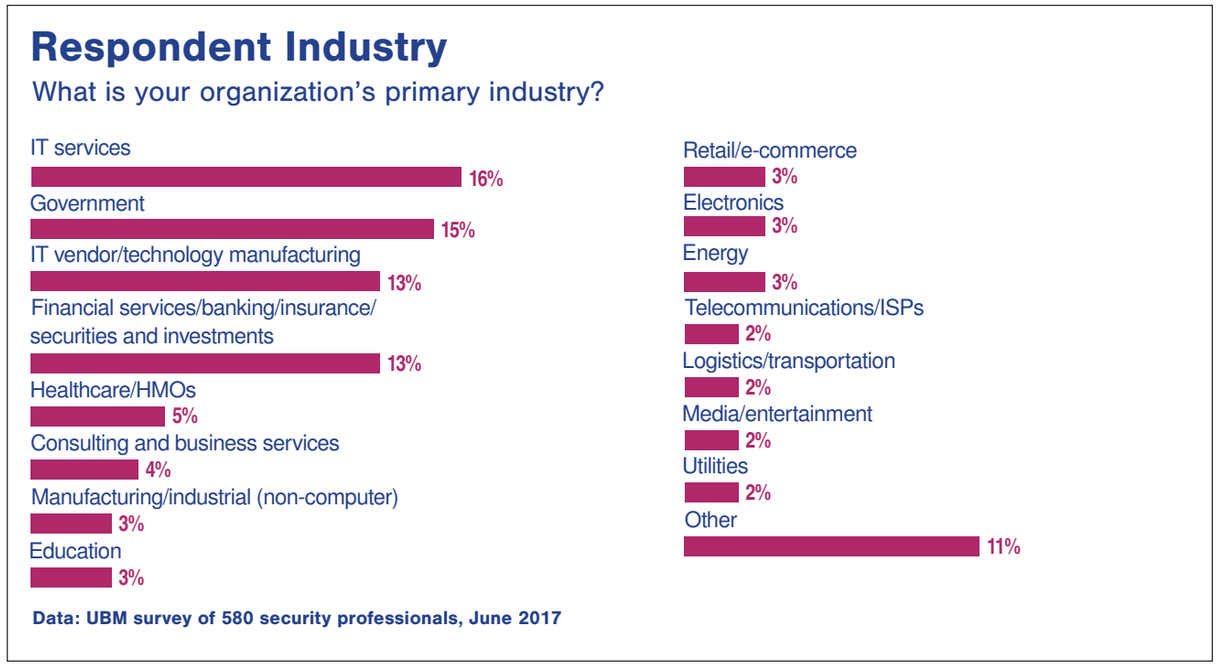
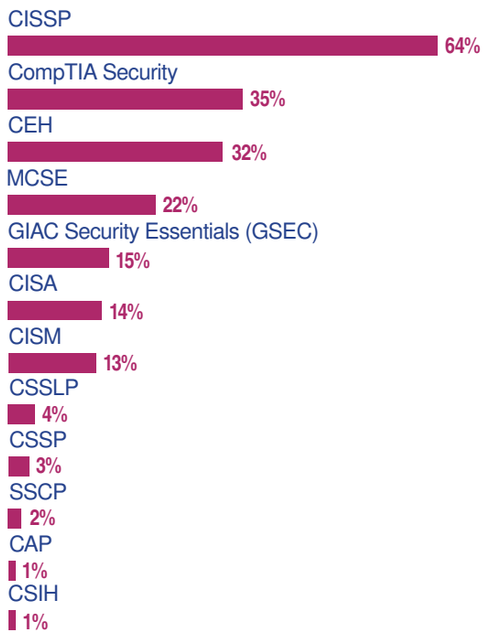

Respondent Industry
What is your organization's primary industry?
IT services
16%
Government
15%
IT vendor/technology manufacturing
13%
Financial services/banking/insurance/ securities and investments
13%
Healthcare/HMOs
5%
Consulting and business services
4%
Manufacturing/industrial (non-computer)
3%
Education
3%
Retail/e-commerce
3%
Electronics
3%
Energy
3%
Telecommunications/ISPs
2%
Logistics/transportation
2%
Media/entertainment
2%
Utilities
2%
Other
11%
Data: UBM survey of 580 security professionals, June 2017

Figure 27

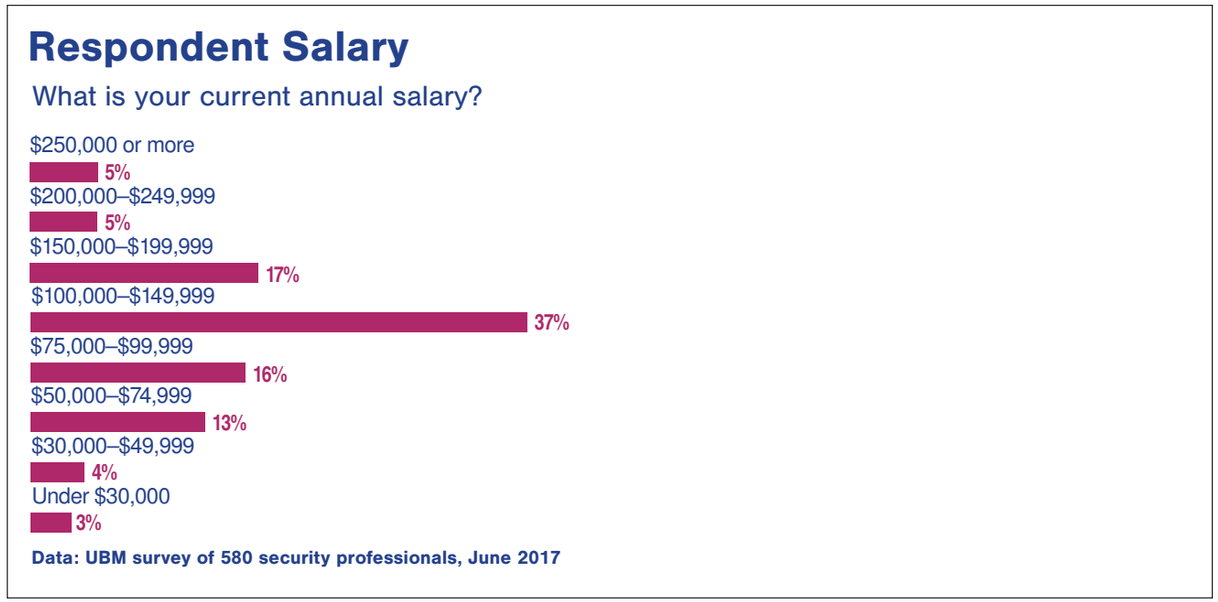
Respondent Security Certifications and Training Certificates

What security certifications/training certificates have you held, either now or in the past?



Note: Multiple responses allowed
Data: UBM survey of 580 security professionals, June 2017

Figure 28


Respondent Salary
What is your current annual salary?
$250,000 or more
5%
$200,000–$249,999
5%
$150,000–$199,999
17%
$100,000–$149,999
37%
$75,000–$99,999
16%
$50,000–$74,999
13%
$30,000–$49,999
4%
Under $30,000
3%
Data: UBM survey of 580 security professionals, June 2017