Next

black hat®
USA 2018

www.blackhat.com
June 2018

The 2018 Black Hat USA Attendee Survey

Where Cybersecurity Stands

Once seen primarily as a technology question, cybersecurity now involves issues of personal privacy, politics, business, ethics, and risk. Here's a look at the concerns, attitudes, and plans of some of the industry's top IT security professionals.

TABLE OF CONTENTS

Figures

EXECUTIVE SUMMARY

In the early days of computers and the Internet, "computer security" was viewed primarily as a technological question. For decades, it was approached as an arms race between "good geeks" and "bad geeks," where tech-savvy, ethical professionals developed new ways of defending critical data, and tech-savvy cybercriminals found ways to break those defenses.

Today, however, information technology has become the underlying platform for human interaction — the infrastructure for business, for social community, and for political action, both cooperative and confrontational. And today's cybersecurity professionals, once focused primarily on technology and stereotyped as geeks, now find themselves at the heart of some of the most important social, geopolitical, and commercial issues of the new millennium. How can humans safely communicate electronically — and still maintain their privacy? Is it possible to conduct a democratic election without interference from hackers or rival countries? How can businesses safely and universally exchange money or data? These are just a few of the challenges that today's IT security leaders are confronting.

To find out where the cybersecurity community stands — its attitudes, its fears, and its plans — Black Hat, the organization that convenes these top IT security leaders together every year, conducted a survey in May of 2018 to ask about some of the most critical issues of the day. The survey, which has been conducted annually since 2015, interviewed 315 current and former attendees of the Black Hat USA conference. Among the survey respondents were chief executives, CISOs, CIOs, chief technology officers, security specialists and researchers from organizations in more than 20 sectors, ranging from financial services to healthcare to government. Nearly two thirds (63%) of the respondents hold the CISSP security certification; many respondents also hold other certifications, including CEH (35%), CompTIA Security (35%), or MCSE (30%).

The survey asked respondents about their most critical concerns — the things that keep them awake at night — and about their plans for the future. We also asked them about some of their concerns about critical infrastructure, as well as their opinions on current events that involve cybersecurity, including privacy, political elections, international relations, and cryptocurrency.

The survey results suggest that the world's top cybersecurity professionals are becoming increasingly concerned not only about the safety of their own users and data, but about the security of increasingly connected systems, the stability of national and international environments, and the privacy of individuals. In short, the professionals who are most familiar with today's cybersecurity environment are in broad agreement that the systems that today serve as platforms for personal, political, and financial interchange are at significant risk of compromise — or even collapse.

The 2018 Black Hat USA Attendee Survey provides a look at cybersecurity professionals' views and insights on a wide range of topics, including:

- Following recent news of misuse of data, 55% of security professionals are advising internal users and customers to rethink the data they are sharing on Facebook; 65% are limiting their own use of Facebook or avoiding it entirely due to security concerns.
- Following the deadline for the European Union's new privacy regulation (GDPR, the General Data Protection Regulation), 30% say they don't know if their organizations are in compliance, or they haven't started GDPR initiatives and are concerned. Furthermore, more than a quarter (26%) do not believe they are subject to GDPR.

- Most IT security pros (52%) believe that Russian cyber initiatives made a substantial impact on the 2016 U.S. elections; 71 percent believe that cyber activity from Russia, China, and North Korea is making U.S. data less secure.
- Nearly seven out of ten respondents (69%) believe that a successful cyberattack on U.S critical infrastructure will occur in the next two years; only 15% believe that government and private industry are prepared to respond.
- Only 13% of IT security leaders believe that Congress and the White House understand the cyber threat; only 16% approve of President Trump's performance so far.
- Nearly six in 10 of the respondents (59%) believe they will have to respond to a major security breach in their own organization in the coming year; most do not believe they have the staffing or budget to defend adequately against current and emerging threats.

SYNOPSIS

RESEARCH

Survey Name 2018 Black Hat USA Attendee Survey

Survey Date May 2018

Region United States

Number of Respondents 315 IT and security professionals. The greatest possible margin of error for the total respondent base (N=315) is +/- 5.5%. 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 USA conference.

Methodology In May 2018, Black Hat and UBM researchers conducted a survey of IT and security professionals who attended the Black Hat USA conference in 2017 and/or were planning to do so in 2018. The online survey yielded data from 315 management and staff security professionals, predominantly at large companies, with 62% working at companies with 1,000 or more employees. Sixty-three percent of the respondents hold the CISSP security professional credential, 35% were certified ethical hackers (CEH).

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.

Previous Next
Table of Contents

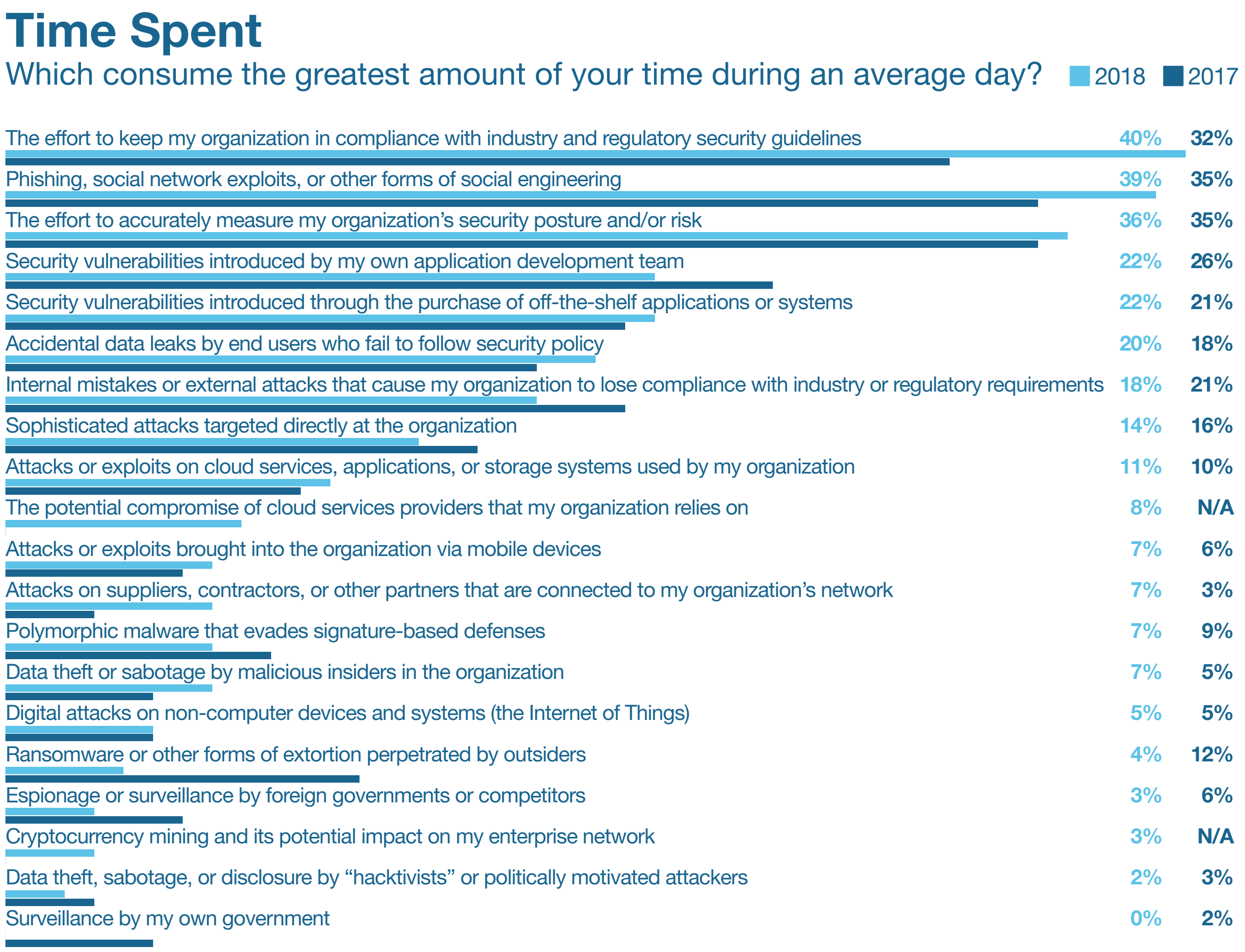
Cybersecurity's New Dimensions

Since the earliest days of telephony and computing, security has generally been seen as a technological problem. When hackers found a way to break into networks or data, security professionals jumped in with new defenses to protect them. Technological attacks were met with technological defenses, and the players on both sides were the most tech-savvy — the "geeks" of IT.

In recent years, however, security professionals — and cyber attackers — have become a part of the mainstream. Politics, international relations, commerce, money, even human relations themselves are now affected by the decisions made — or not made — by security teams. And security professionals, once seen as techno-geeks, are now involved in critical issues such as nationwide elections, global cryptocurrency, and fundamental personal privacy.

The 2018 Black Hat Attendee Survey attempted to provide a snapshot of this sea change by not only asking conference attendees — some of the most highly qualified security professionals in the world —

Figure 1



Note: Maximum of three responses allowed
Base: 315 respondents in 2018 and 580 respondents in 2017
Data: UBM survey of security professionals, May 2018

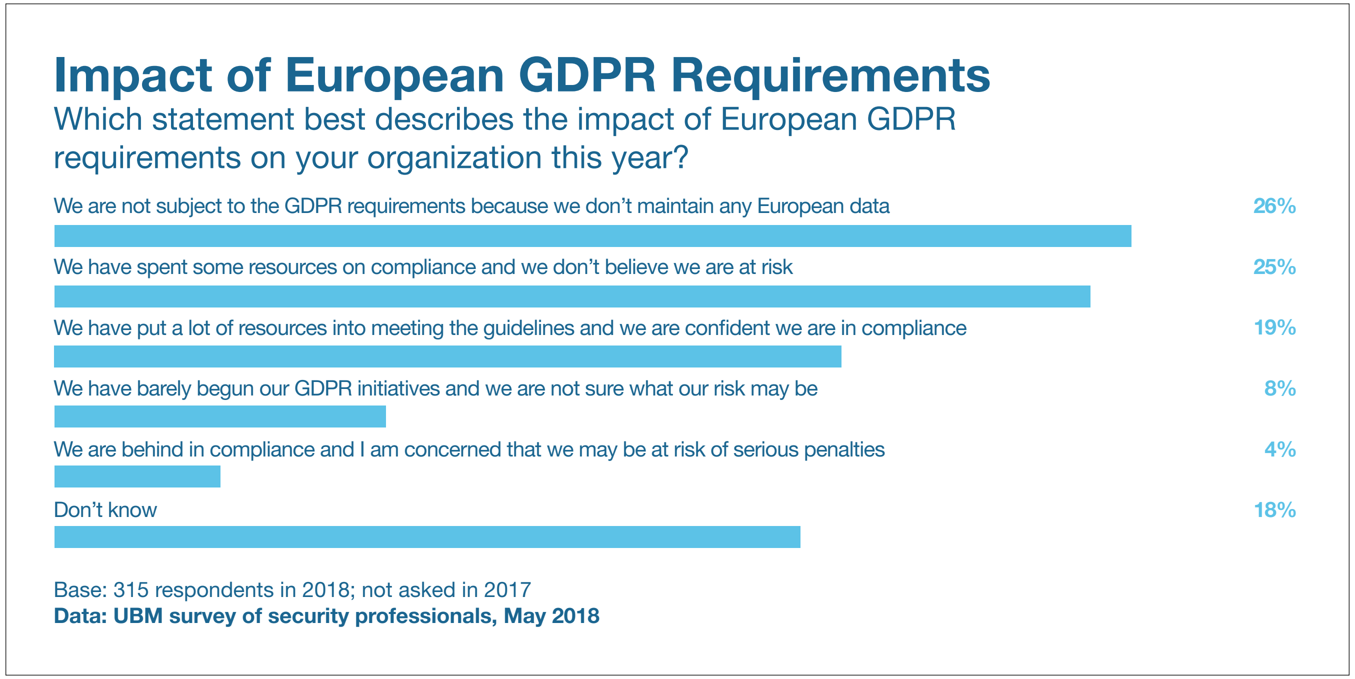
about the state of cybersecurity. In the survey, 315 well-credentialed security leaders — about three quarters (76%) based in the United States and most (62%) working in enterprises of 1,000 employees or more — offer insight not only on the technological challenges faced by the cybersecurity industry, but on the legal, commercial, and political challenges, and on the security and privacy of the individual in today's highly connected world.

While there are many new threats and challenges faced by security pros in the coming year, perhaps the newest and most important challenge is that of the individual's right to privacy — and the steps that enterprises and government must take to protect that privacy. From a regulatory perspective, that challenge is manifested in the European Union's General Data Protection Regulation (GDPR), which began enforcement action in May and requires enterprises to meet specific guidelines on the handling of personal data — and face enormous fines if they don't. From a practical perspective, the privacy issue is manifested in headlines about social networking giant Facebook, which stands accused of oversharing personal information with data brokers.

GDPR is very much on the minds — and task lists — of security professionals this year. The effort to achieve compliance now has become the single most time-consuming issue faced by survey respondents, ranking as a top time-consumer by 40% — more than targeted attacks and insider data leaks combined (**Figure 1**). And while 44% of respondents have already invested in GDPR compliance efforts and feel generally comfortable in their compliance, another 30% say they don't know if their organizations are in compliance, or they haven't started GDPR initiatives and are concerned. Furthermore, more than a quarter (26%) do not believe they are subject to GDPR — which seems unlikely, since most large enterprises do at least some business with European customers (**Figure 2**).

The issue of data misuse — illuminated by, but by no means limited to, recent revelations

Figure 2



Impact of European GDPR Requirements

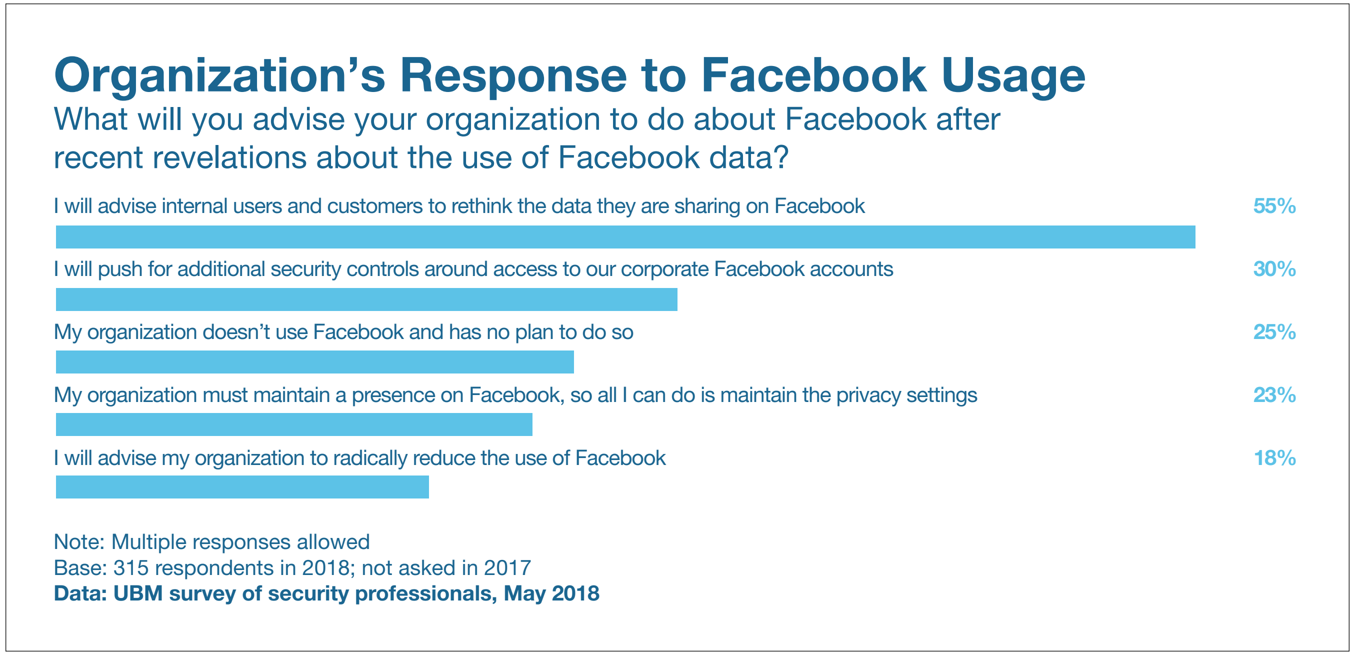
Which statement best describes the impact of European GDPR requirements on your organization this year?

Base: 315 respondents in 2018; not asked in 2017
Data: UBM survey of security professionals, May 2018

about Facebook's privacy practices — has also raised the consciousness of IT security professionals, both at their jobs and at home. A majority of our survey respondents (55%) say they plan to advise internal users and customers to rethink the data they are sharing on Facebook as a result of the allegations. Another 30% of respondents plan to push for additional security controls around access to their corporate Facebook accounts; 18% plan to advise their organizations to radically reduce the use of Facebook (**Figure 3**).

The news about Facebook's alleged misuse of private information has had an even greater impact on security professionals' personal approach to the social network. Forty-four percent of those surveyed said they plan to keep their accounts, but will minimize their Facebook usage. Seven percent said they are deleting their accounts; 14 percent said they didn't use Facebook in the first place because of security concerns. Only 25% said they plan to continue to use Facebook regularly, with appropriate privacy settings (**Figure 4**).

Figure 3


Organization's Response to Facebook Usage

What will you advise your organization to do about Facebook after recent revelations about the use of Facebook data?

Note: Multiple responses allowed
Base: 315 respondents in 2018; not asked in 2017
Data: UBM survey of security professionals, May 2018

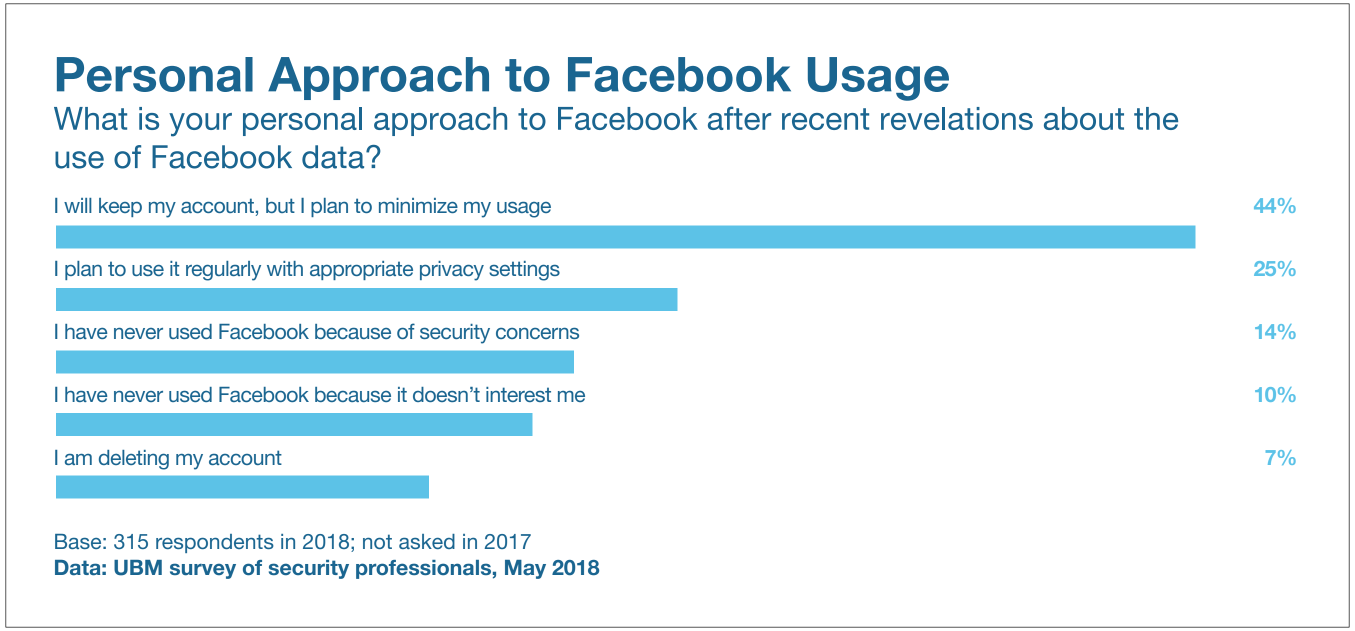
The recent issues with social networks, combined with never-ending reports of data breaches and compromise of personal information, has caused many security professionals to conclude that the protection of an individual's private information, no matter how carefully protected, is impossible. In the 2018 Black Hat Attendee Survey, only 26% of respondents said they believe it will be possible for individuals to protect their online identity and privacy in the future. This is a bleak outlook indeed when coming from those who understand the threat best, and in many cases, are professionally tasked with protecting that data (**Figure 5**).

A Political Struggle

While privacy may be the latest challenge for security professionals, another challenge is also fresh in their minds: politics. While GDPR is driving many of our U.S. respondents to consider how much data they handle from Europe, many are also contending with cyber threats from foreign governments — and frustration with their own government at home.

For today's information security departments, the threat of nation-state-sponsored attacks is very real. Seventy-one percent of respondents said that recent activity emanating from Russia, China, and North Korea has made U.S. enterprise data less secure. Fifty-two percent believe that Russian cyber initiatives made a significant impact on the outcome of the 2016 U.S. presidential election.

Figure 4


Personal Approach to Facebook Usage

What is your personal approach to Facebook after recent revelations about the use of Facebook data?

Base: 315 respondents in 2018; not asked in 2017

Data: UBM survey of security professionals, May 2018

In response to an open-ended question about what global or political issue concerns them most, many security pros cited nation-state sponsored threats, ranging from espionage to steal U.S. business data to all-out cyberwar. One respondent cited concern over the "lack of understanding by the general public as to the real result of nation-state hacking: loss of critical intellectual property, access to intelligence, and destabilization of both financial and critical infrastructure."

Compounding these concerns is a lack of confidence in the U.S. federal government's ability to manage the cybersecurity problem. In our survey, only 13% of respondents said they believe that Congress and the White House understand the cyber threat and will take adequate steps to secure critical infrastructure in the future. Only 16% say they approve of U.S. President Donald Trump's performance thus far. Interestingly, however, most information security professionals do not play party politics: just 12% identified themselves as Republicans, and 16% identified as Democrats. Ten percent are Libertarian, 26% are independents, and 36% preferred not to answer (**Figure 19**).

In the open-ended question about the chief global/political issue that worries them most, many respondents cited issues affecting the U.S. federal government, including election fraud, shortage of government cyber resources, and the recent decision to do away with the federal cyber adviser/czar position. About a dozen of the 179 responses to this optional, open-ended question cited President Trump as the primary concern.

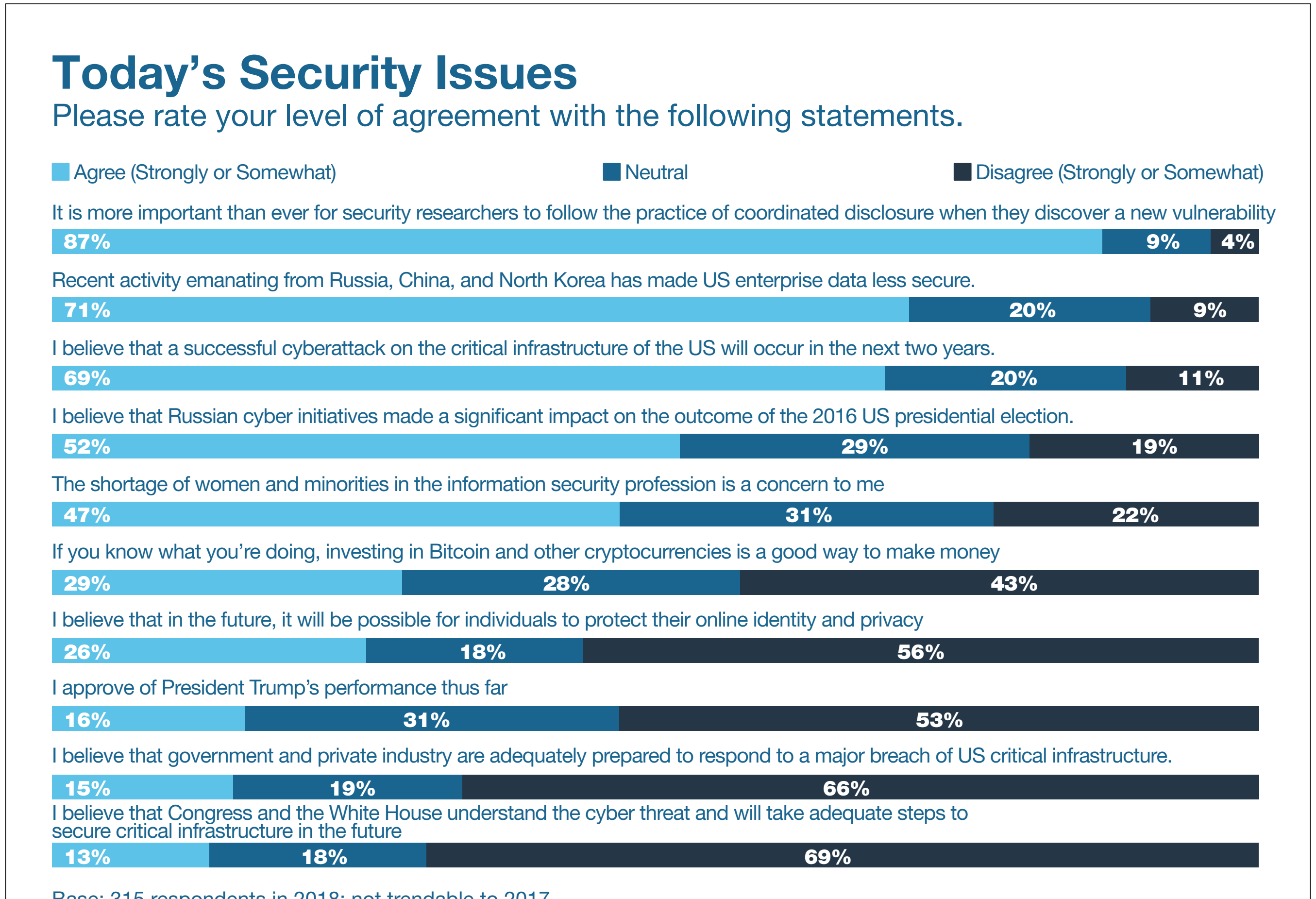
While not a political issue yet, many respondents also registered a great deal of interest and concern about the emergence of cryptocurrency, which has alternately been hailed as a boon to currency exchange and as a threat to currency trading. While they are perhaps among the most knowledgeable about cryptocurrency, our respondents were mixed in their attitudes toward Bitcoin trading: some 29% said investing in Bitcoin and other cryptocurrencies is a good idea for those who know what they're doing; 43% disagree.

The Critical Infrastructure Threat

Whether it comes from a large nation-state, a rogue nation, or a terrorist group, security professionals are fairly certain that an attack on U.S. critical infrastructure is coming. In fact, 69% or our survey respondents expect a successful cyberattack on U.S. critical infrastructure will take place within the next two years. This figure rose in this year's survey from 60% in 2017. Only 11 percent don't think it's going to happen. In the open-ended question asking which global/political issue worried respondents most, more than a dozen respondents wrote something related to cyberwar.

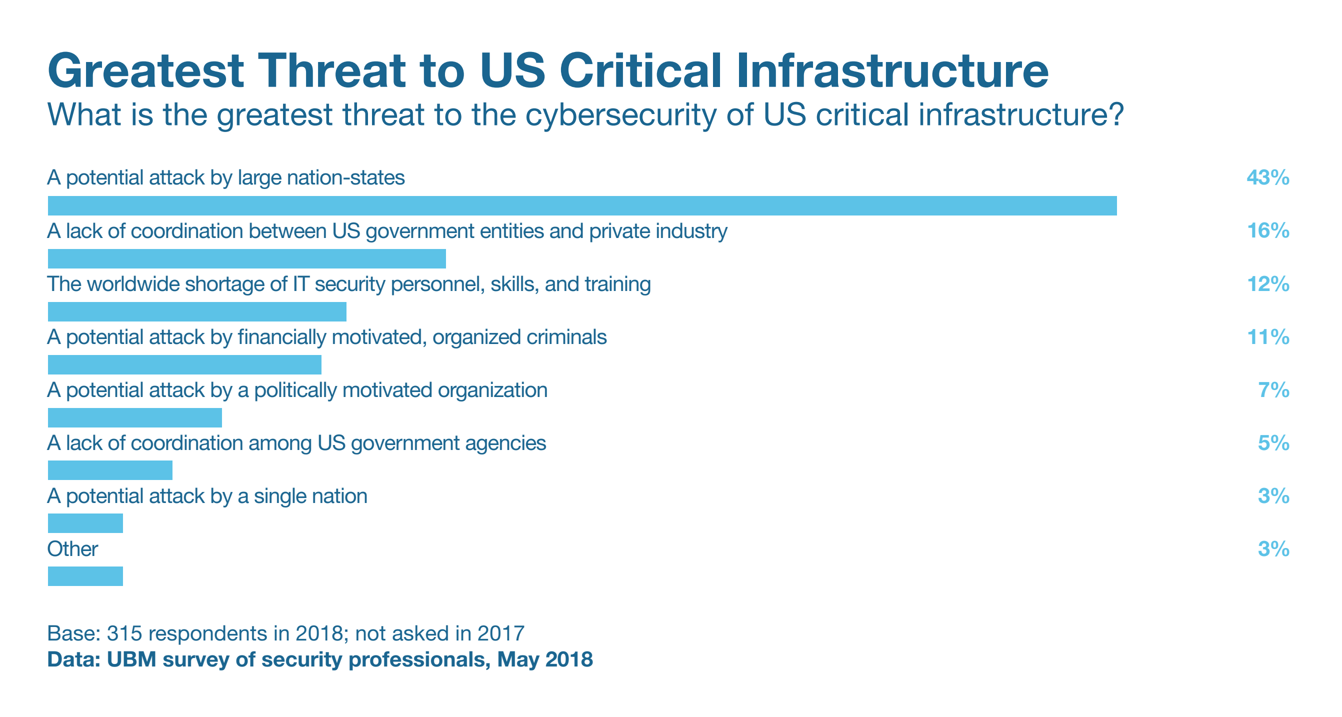
Of the various threats to U.S. critical infrastructure, 43% of security pros believe that the greatest is an attack by a large nation-state such as Russia or China. Interestingly, more respondents believe that an attack by a financially motivated cybercriminal organization is of greater concern than an attack by a politically motivated terrorist organization (7%) or a rogue nation-state such as North Korea (3%) (**Figure 6**).

Figure 5



Base: 315 respondents in 2018; not trendable to 2017
Data: UBM survey of security professionals, May 2018

Figure 6



Base: 315 respondents in 2018; not asked in 2017
Data: UBM survey of security professionals, May 2018

While the certainty of knowledgeable, professional cybersecurity professionals about the likelihood of a critical infrastructure attack is a major concern, it is exacerbated by those professionals' lack of confidence in the United States' ability to respond to such an attack. In fact, only 15% of respondents said they believe that U.S. government and private industry are adequately prepared to respond to a major breach of critical infrastructure. When asked to name the greatest threat to critical infrastructure security, 16% cited a lack of coordination between federal government entities and private industry, making this the number two response. Five percent cited a lack of coordination among U.S. government agencies, which means that 21% of security pros believe that the greatest threat to U.S. critical infrastructure is a lack of preparedness and communication among the defenders.

"Our United States government has NO clue about technology, the Internet, and how our modern era's data and information moves," commented one respondent. "It's absolutely terrifying that these people make laws and guide our nation. They are obsolete."

The Threat to the Enterprise

While information security professionals may have added new privacy and political dimensions to their scope of concern, they haven't taken their eyes off their central role: protecting enterprise data. Unfortunately, as in past years, most security pros are still feeling vulnerable to attack.

When asked whether they believe their organizations will have to respond to a major security breach in the next 12 months, some 69% of respondents said they believe it is at least somewhat likely. The percentage of respondents who say they have "no doubt" that such a breach will occur has declined over the past two years — from 15% in 2016 to 9% in 2018 — but the percentage who say it is "highly likely" grew slightly, from 18% to 21%, in the last year.

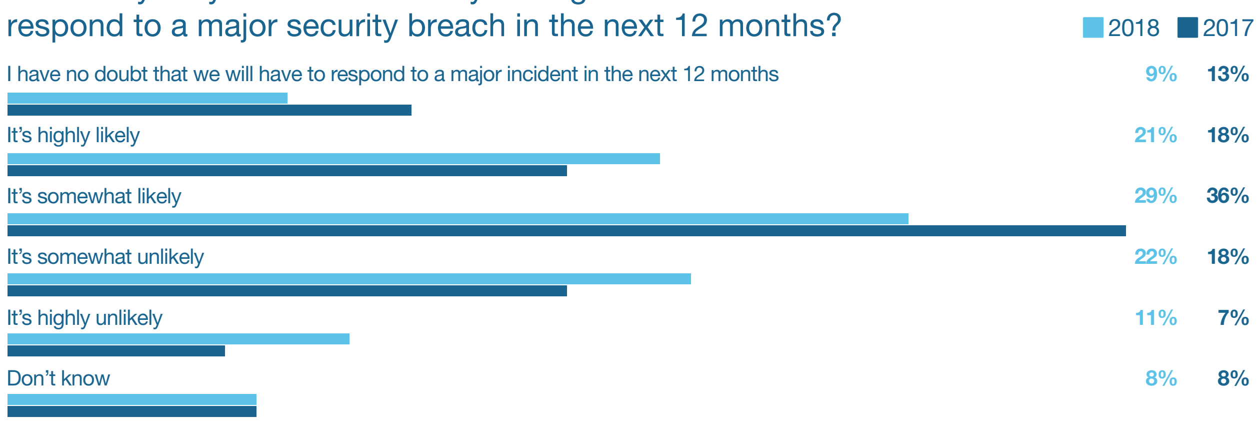
Previous Next

Table of Contents

Figure 7

Likelihood of a Major Security Breach in Next Year

How likely do you think it is that your organization will have to respond to a major security breach in the next 12 months?



Base: 315 respondents in 2018 and 580 respondents in 2017

Data: UBM survey of security professionals, May 2018

And while the degrees of concern may vary, the overall numbers have remained consistent over the past four years: more than two-thirds of security professionals expect to face a major breach in the coming months (**Figure 7**).

And, as in past years, the reasons for this concern center on a lack of resources. For the fourth straight year, approximately two-thirds of survey respondents said they do not have enough staff (65%) to defend their organizations against current threats (**Figure 14**). Fifty-three percent said they do not have enough budget — an improvement over the 63% of 2016, but still a majority (**Figure 15**). Sixty-six percent said they themselves do not have enough training to handle current threats and perform all of the job functions required of them (**Figure 8**).

This year's survey also revealed another issue in cyber defense: a lack of confidence in technology. For the first time, we asked security professionals to rate the effectiveness of a wide range of technologies available to enterprise security teams, from old-school solutions such as antivirus to emerging technologies such as orchestration and deception. In a list of 18 available technologies, however, only three were rated as "very effective" or "somewhat effective" by a majority of respondents: encryption, multifactor authentication tools, and firewalls. The other 15 technologies were rated "effective" by 47% of respondents or fewer. Passwords, perhaps the most universal of security technologies, were rated "effective" by only 19% of security pros, and "ineffective" by 37% (**Figure 13**).

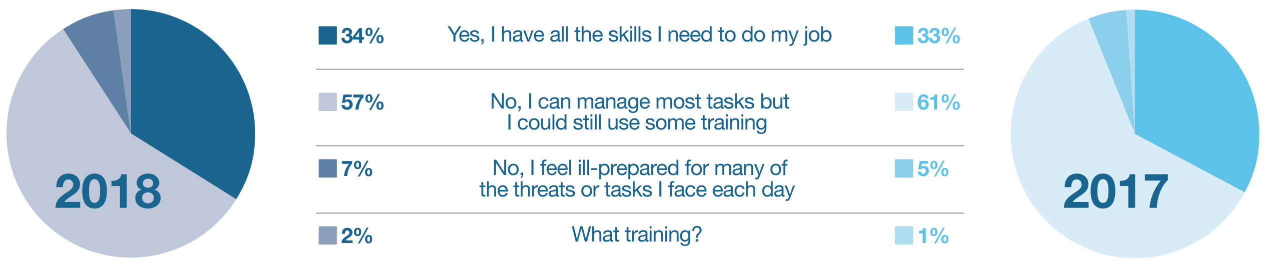
When it comes to what worries them most, security professionals registered many of the same top concerns as in past years: sophisticated, targeted attacks ranked at the top of the list (47%), followed by phishing and social engineering (40%). However, there were two new concerns that registered in the top five: potential compromises of cloud services (22%) and attacks or exploits targeted at cloud applications, storage systems, or services used by the organization (16%). Asked in an open-

Previous Next
Table of Contents

Figure 8

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: 315 respondents in 2018 and 580 respondents in 2017
Data: UBM survey of security professionals, May 2018

ended question about what keeps security pros awake at night, one respondent said "A major compromise of cloud resources — e.g. root account access — allowing control of high-level servers, compromising customer or enterprise-related data" (**Figure 9**).

Yet, while the shortcomings of current security technology and potential vulnerabilities in emerging cloud services are new aspects of security's current landscape, it is an old nemesis — staffing shortages — that continues to plague the data centers and minds of Black Hat Attendee Survey respondents. When asked to name the primary reason why enterprise security strategies fail, some 34% of respondents cited a shortage of qualified people and skills, making this the number one answer given. A lack of commitment and support from top management (23%) was the number two response; the numbers on both responses were up from a year ago (31% and 19%, respectively) (**Figure 10**).

"Diversity of thought, skill sets, and backgrounds is what is needed in order to build risk-based, comprehensive, and effective solutions," said one respondent to an open-ended question about what needs to be fixed in cybersecurity. "The team needs to be made up of more than just network engineers or previous SOC analysts or hackers. You need a team that understands security, understands the business, operations, the threat landscape, metrics, organizational behavior, etc. At the end of the day, people make the decisions."

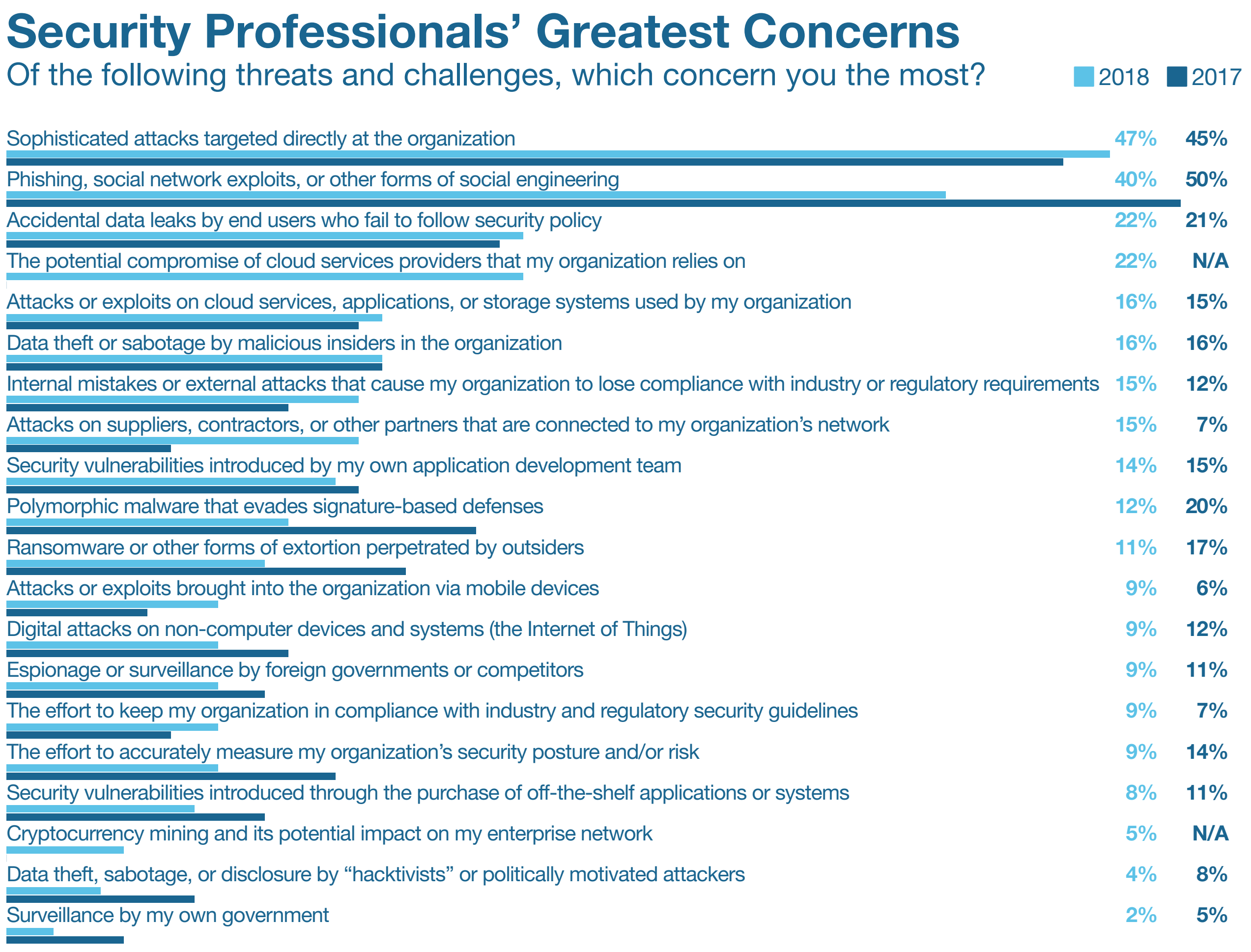
Yet, while the need for people represents the greatest hope for some survey respondents, it is human weaknesses that leads to the greatest concerns of others. Accidental data leaks ranked third among respondents' concerns in our survey (22%); end users who violate corporate security policy ranked as the weakest link in today's enterprise IT defenses (38%) (**Figure 11**). The attacker that security professionals fear most, as in past years, is the individual who has inside knowledge of the organization (**Figure 12**).

"Insider threat is my biggest concern," said one respondent in answer to the open-ended question about what keeps security pros awake at night. "All security systems have authorized users who can bypass the security,

Previous Next

Table of Contents

Figure 9



Note: Maximum of three responses allowed
Base: 315 respondents in 2018 and 580 respondents in 2017
Data: UBM survey of security professionals, May 2018

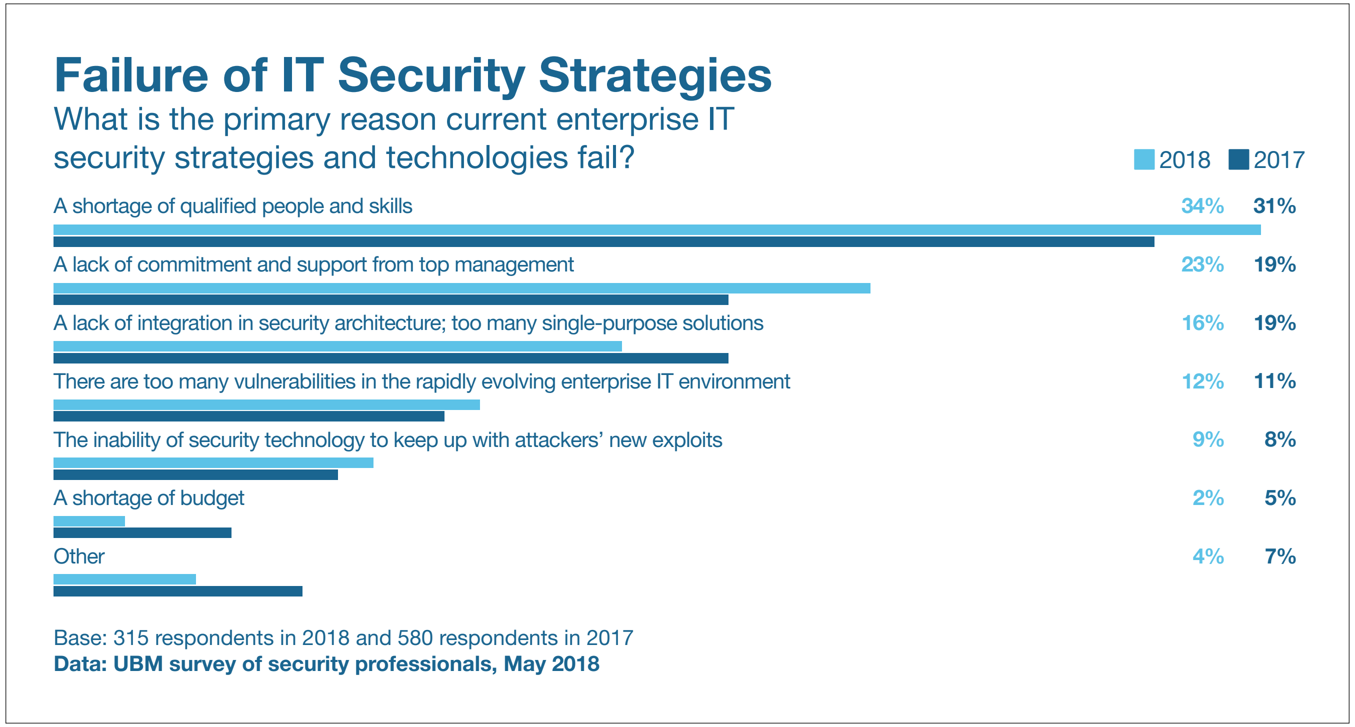
and if one of those people becomes a threat, there is very little that can be done to stop that person. While solutions exist, such as two-person controls, they are too expensive and impractical to implement everywhere."

Where Security Professionals Stand

We've discussed what concerns security professionals on an individual level, on a global level, and at an enterprise level. But what about their own personal interests and concerns? What are their passions and their goals? In the 2018 Black Hat Attendee Survey, we found out about some of those, too.

One issue security pros care about, nearly universally, is the issue of "coordinated disclosure," the set of rules that ethical hackers use when they do security research and test for vulnerabilities. The rules of coordinated disclosure state, for example, that a researcher should give the affected parties a chance to repair vulnerabilities to remediate a security flaw before disclosing it to the public. In recent years, however, many companies, governments, and other organizations have instituted "bug bounty" programs that pay researchers for vulnerabilities without necessarily requiring

Figure 10



Base: 315 respondents in 2018 and 580 respondents in 2017
Data: UBM survey of security professionals, May 2018

coordinated disclosure, potentially weakening the need for traditional rules and obligations.

In our survey, security pros indicated that the spirit of coordinated disclosure is alive and well among the community of ethical hackers. In fact, some 87% of respondents agreed with the statement "It is more important than ever for security researchers to follow the practice of coordinated disclosure when they discover a new vulnerability." Only 4% disagreed. When asked what they would do if they themselves discovered a new vulnerability, 82% of security pros said they would follow the practices of coordinated disclosure; only 12% said they would sell it to the highest bidder through forums or bug bounty programs (**Figure 16**). These results suggest that there remains a strong need for forums and conferences like the Black Hat events, which help researchers speak about new vulnerabilities only after they have completed the coordinated disclosure process.

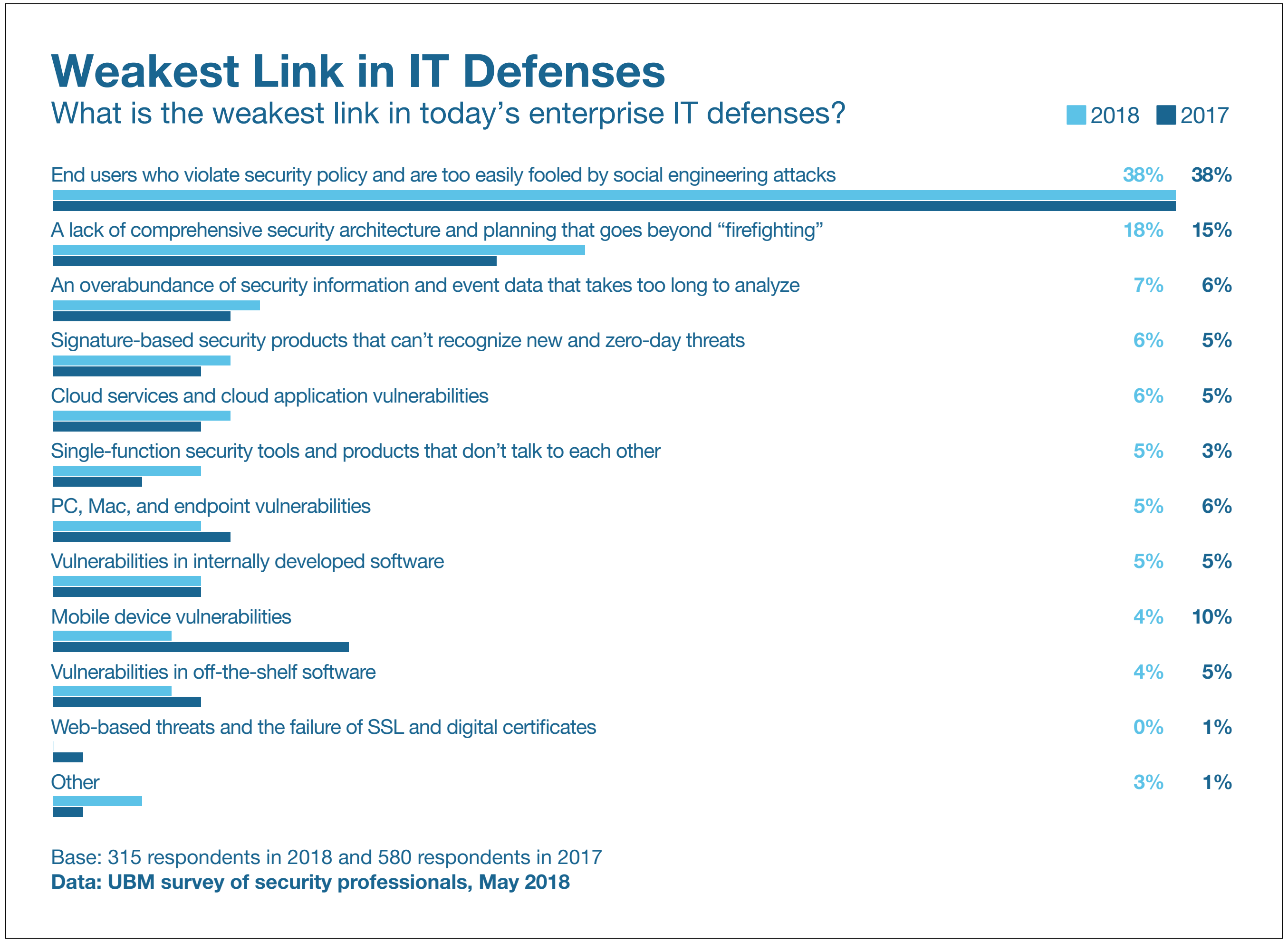
Do security professionals do security research themselves? More than two-thirds (68%) of Black Hat attendees said they do. Sixty-four percent said they do penetration testing. But when it comes to online activities that aren't relevant to their day jobs, or that might be less ethical, the percentages drop off significantly. For example, only 12% of respondents said they try to crack targeted systems or websites just to see if they can get in. Only 13% of respondents said they browse and communicate with others on the Dark Web; only 2% said they buy and sell items on the Dark Web (**Figure 17**).

Interestingly, while the world of cryptocurrency trading and mining seems of great interest to today's security professionals, very few of them seem to be directly involved. In our survey, just 15% of respondents said they do cryptocurrency buying and selling; only 29% agreed with the statement, "If you know what you're doing, investing in Bitcoin and other currencies is a good way to make

Previous Next

Table of Contents

Figure 11



money.” And while cryptocurrency mining has been reputed to be a growing trend among the security-savvy, only 12% of survey respondents say they are doing it. Are security pros worried that cryptocurrency miners might try to tap their own enterprise systems to gain additional processing power? Only 5% of respondents rated this as a top concern.

On a career level, most security professionals seem happy with their positions. When asked whether they are actively looking for employment right now, only 11% responded positively, down a point from 2017. Even the percentage of respondents who said they are updating their resumes is down, going from 20% in 2017 to 17% this year. Twenty-eight percent said, “I really love my job and my employer, and it would take a LOT to get me to move” (**Figure 18**).

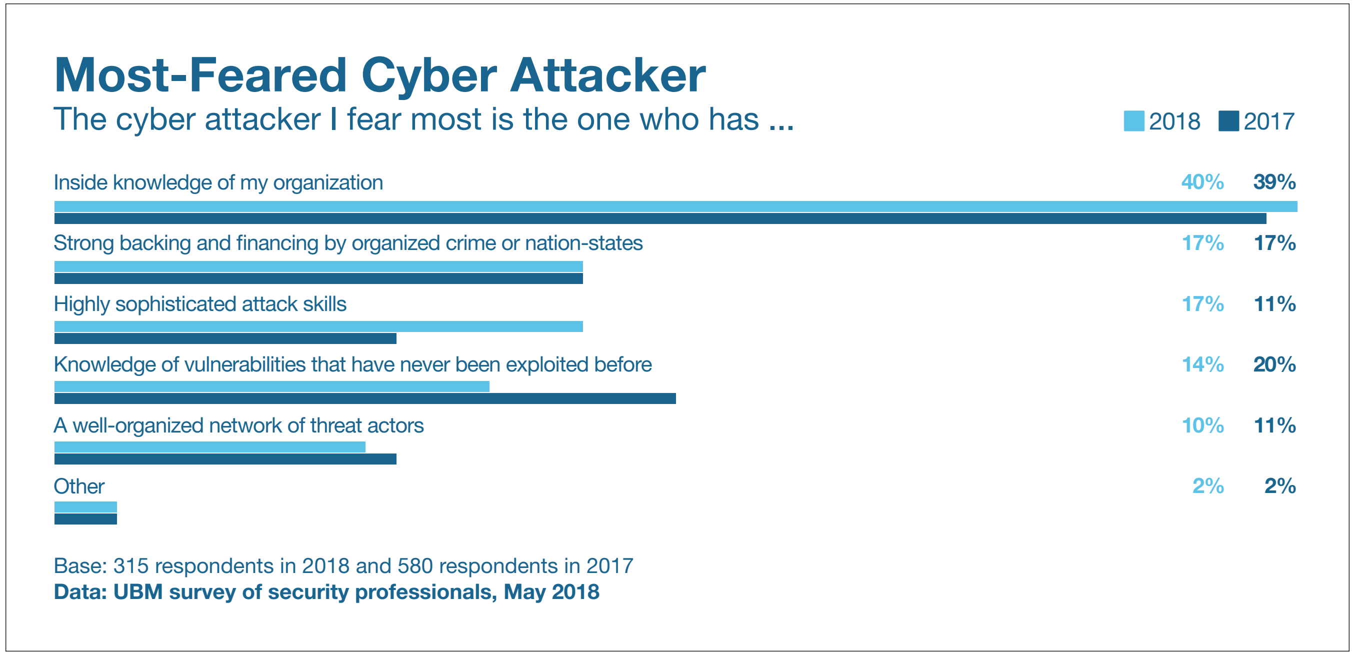
One reason why information security pros are happy is the money they make. According to our survey, some 30% of respondents make $150,000 or more annually; 6% make $250,000 or more. Some 69% of security professionals make a six-figure salary — no small feat in an economy where wages in other industries have grown very slowly (**Figure 20**).

Still, many of today’s security professionals would like to see their colleagues — particularly women and minorities — finding better employment opportunities. Recent studies indicate that women make up less than 15% of the cybersecurity workforce; minorities account for about 26%. In our survey, 47% of respondents said that the shortage of women and minorities in the information security profession is a concern to them.

Conclusion

The security environment of 2018 is more complex than the environment described in the first Black Hat Attendee Survey conducted four years ago. In addition to dealing with a shortage of internal resources and an increasingly sophisticated level of attacks, today's IT security professionals find themselves wrestling with a growing number of global, political, personal, and business issues, many of which they are called upon to manage on behalf of their organizations. For today's security leaders, it is becoming critical to not only pay attention to the threats and issues inside their own organizations, but to issues that affect global commerce and communications — and society as well.

Figure 12

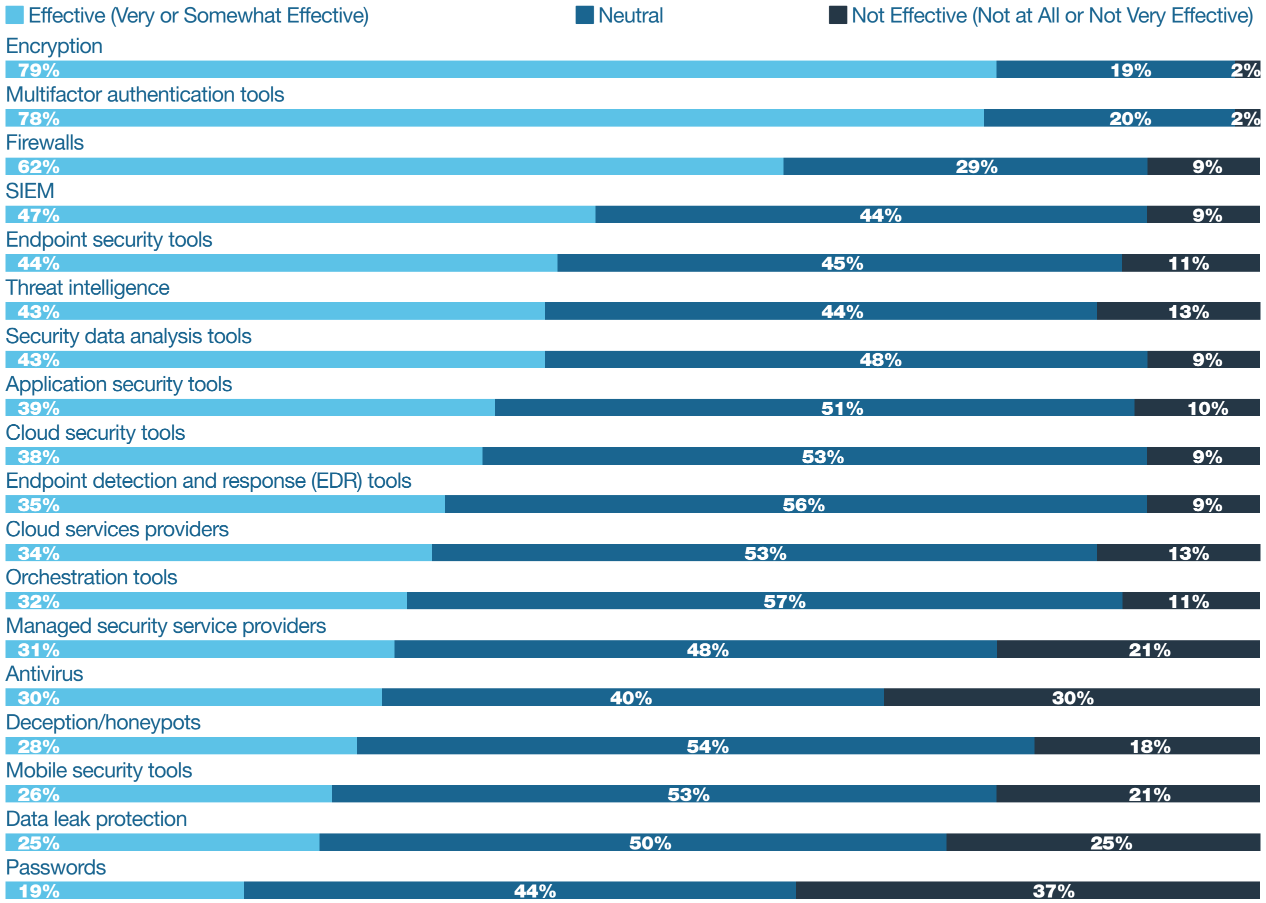


Base: 315 respondents in 2018 and 580 respondents in 2017
Data: UBM survey of security professionals, May 2018

Figure 13

Effectiveness of Technologies in Protecting Data

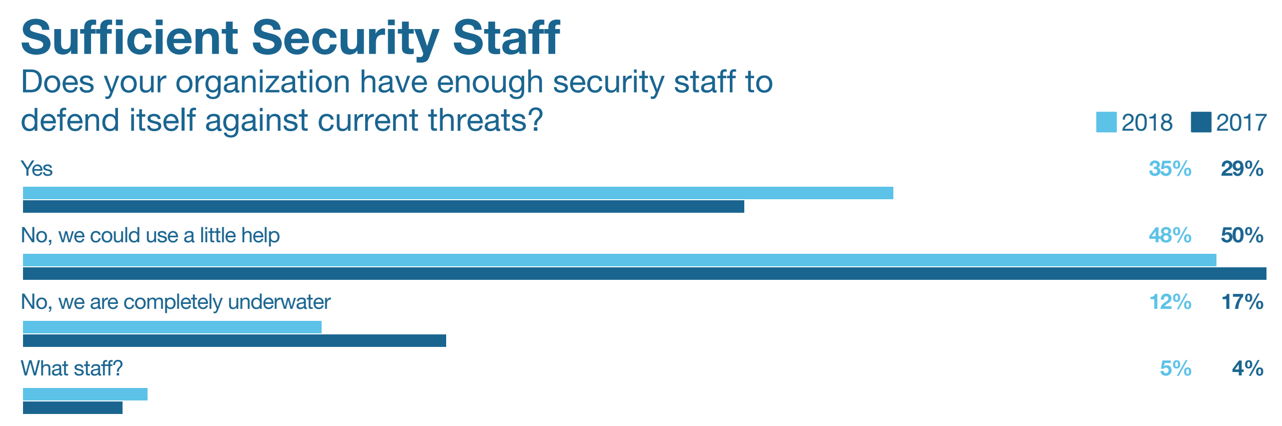
Please rate the effectiveness of the following technologies in protecting enterprise data.



Base: 315 respondents in 2018; not asked in 2017

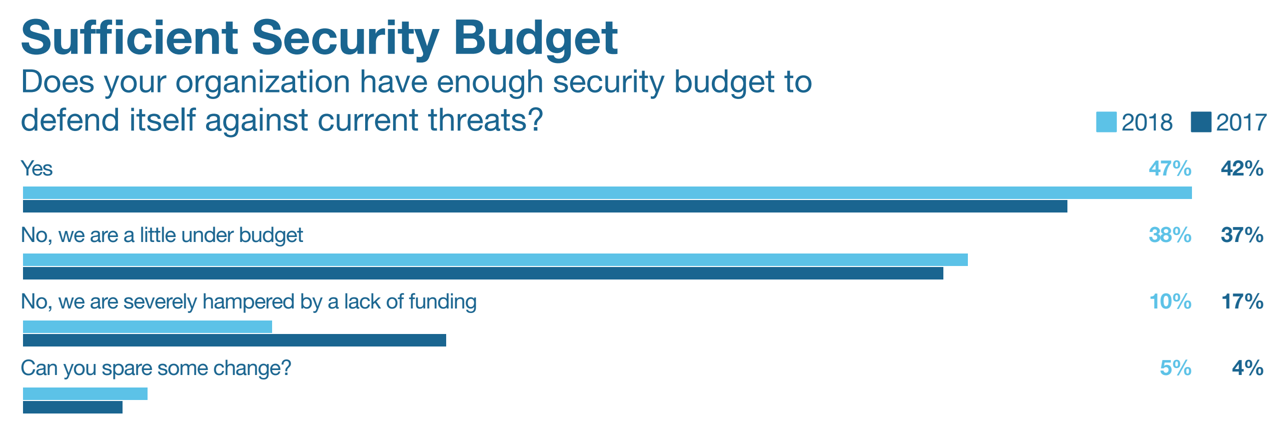
Data: UBM survey of security professionals, May 2018

Figure 14



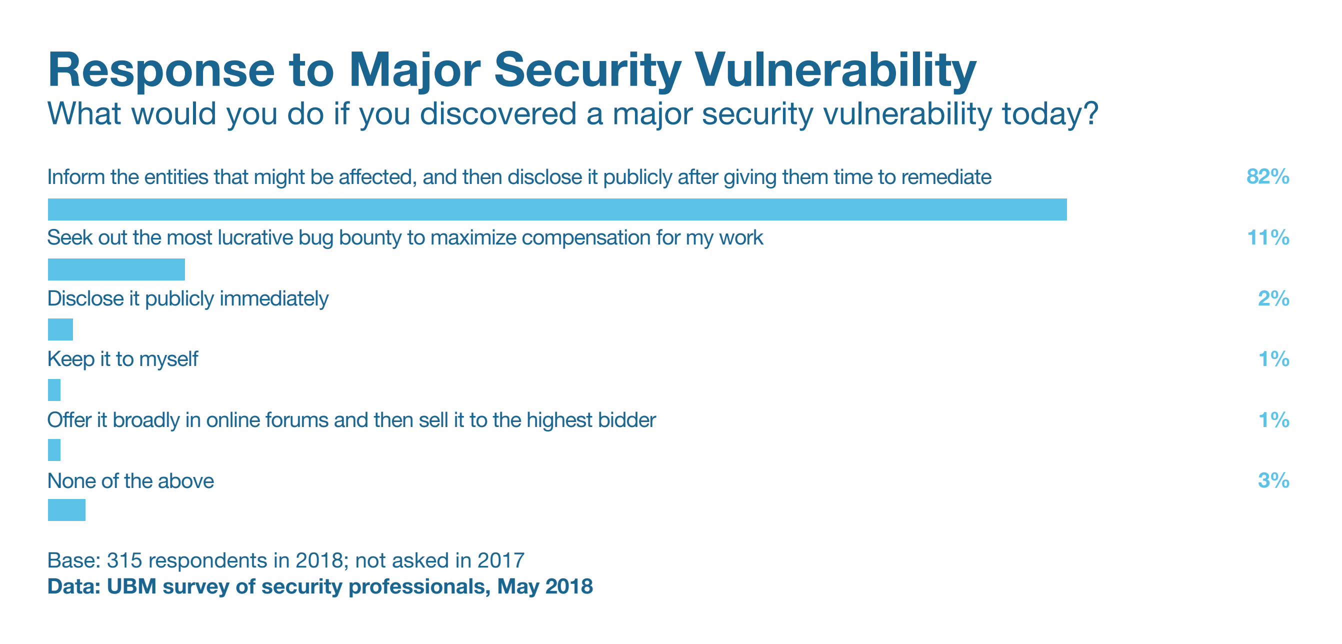
Base: 315 respondents in 2018 and 580 respondents in 2017
Data: UBM survey of security professionals, May 2018

Figure 15



Base: 315 respondents in 2018 and 580 respondents in 2017
Data: UBM survey of security professionals, May 2018

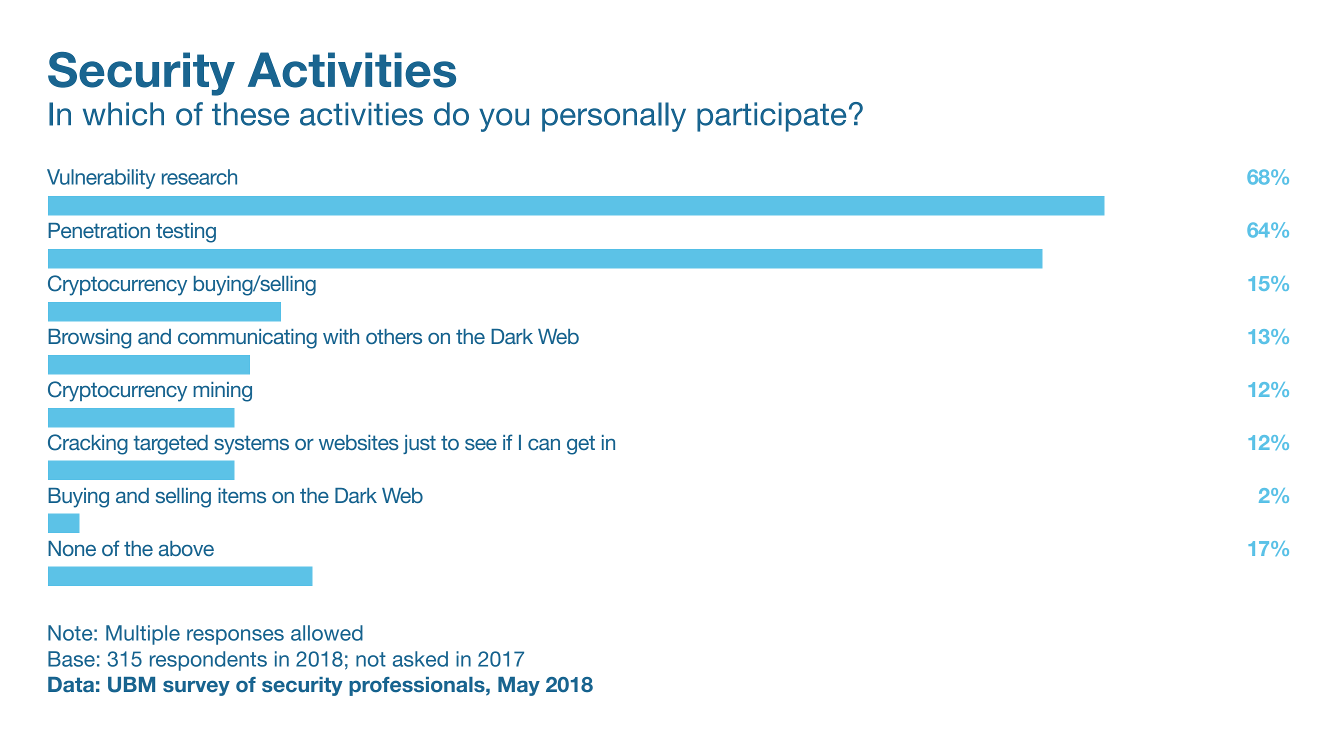
Figure 16



Base: 315 respondents in 2018; not asked in 2017

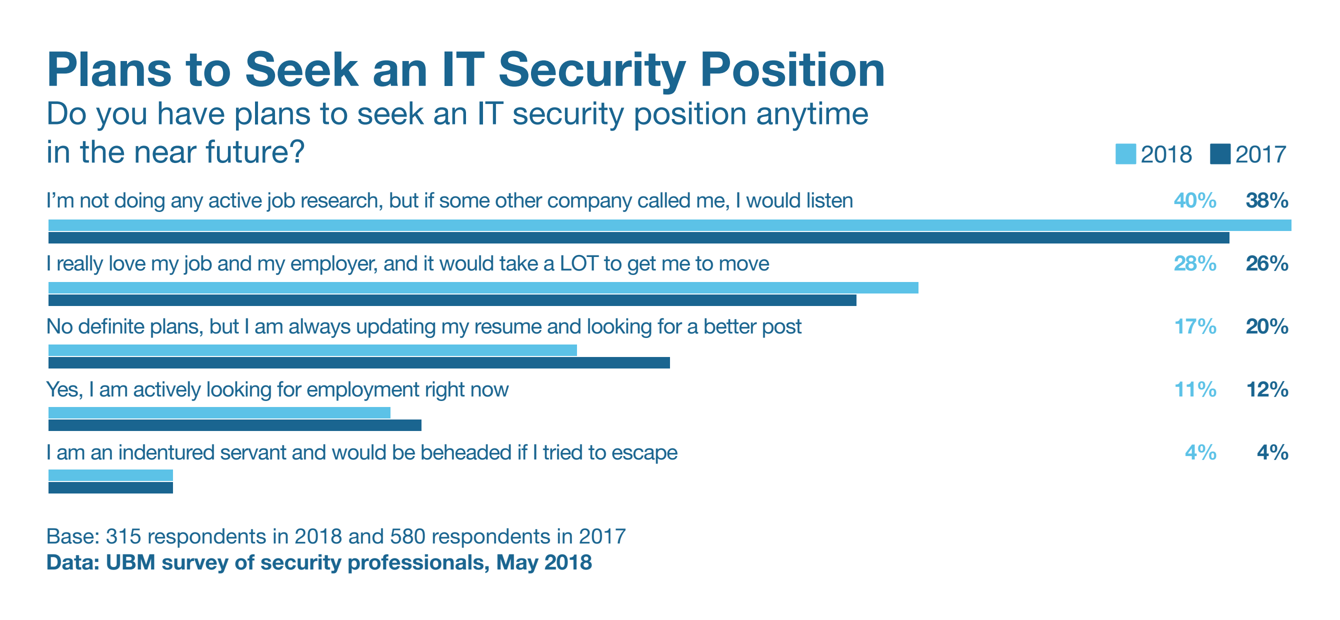
Data: UBM survey of security professionals, May 2018

Figure 17



Note: Multiple responses allowed
Base: 315 respondents in 2018; not asked in 2017
Data: UBM survey of security professionals, May 2018

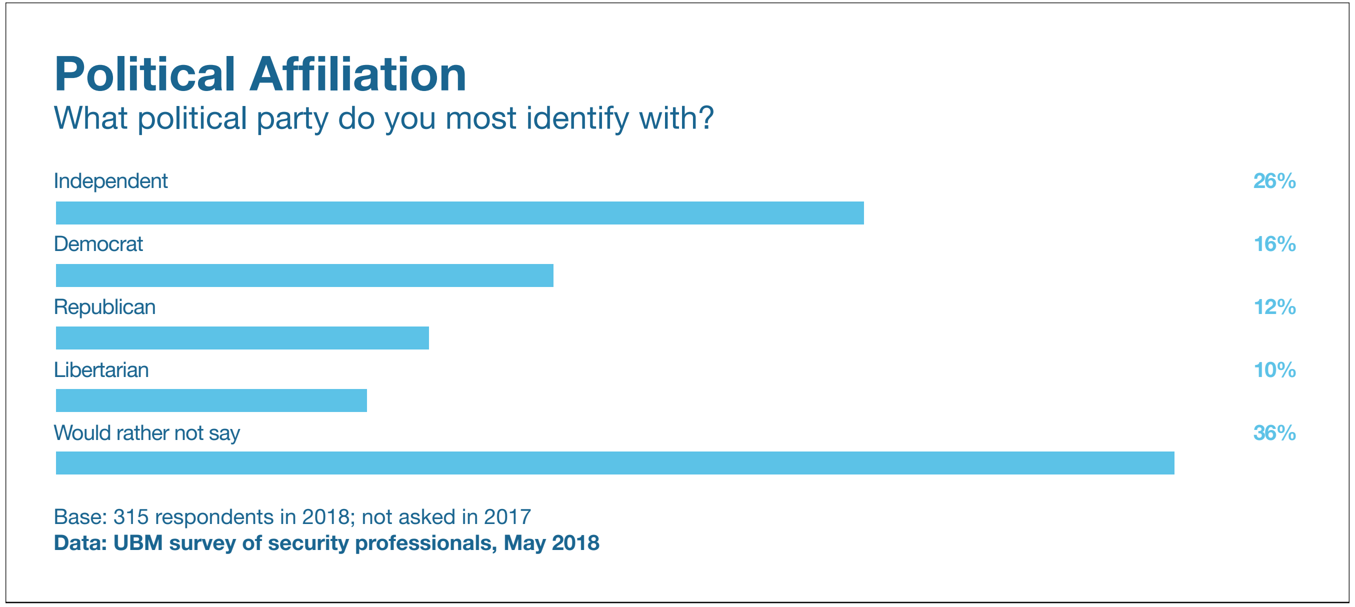
Figure 18



Base: 315 respondents in 2018 and 580 respondents in 2017

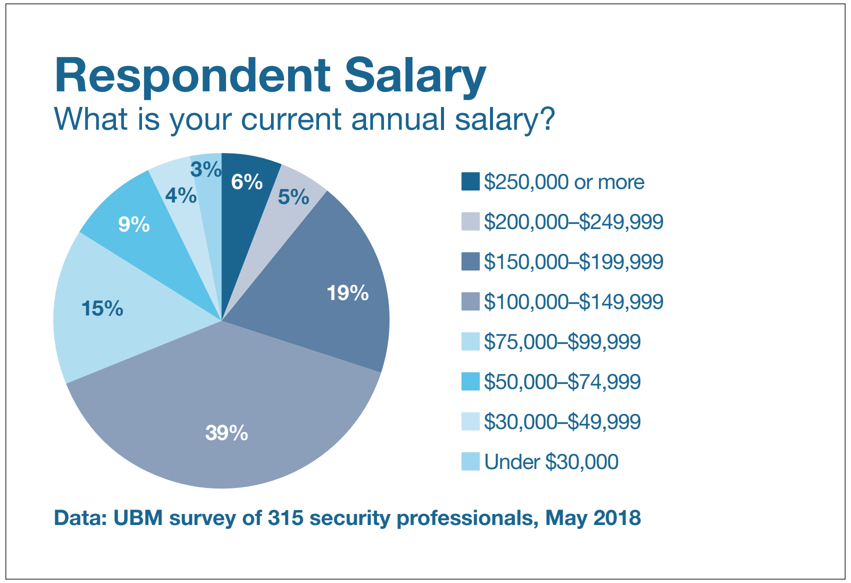
Data: UBM survey of security professionals, May 2018

Figure 19



Base: 315 respondents in 2018; not asked in 2017
Data: UBM survey of security professionals, May 2018

Figure 20

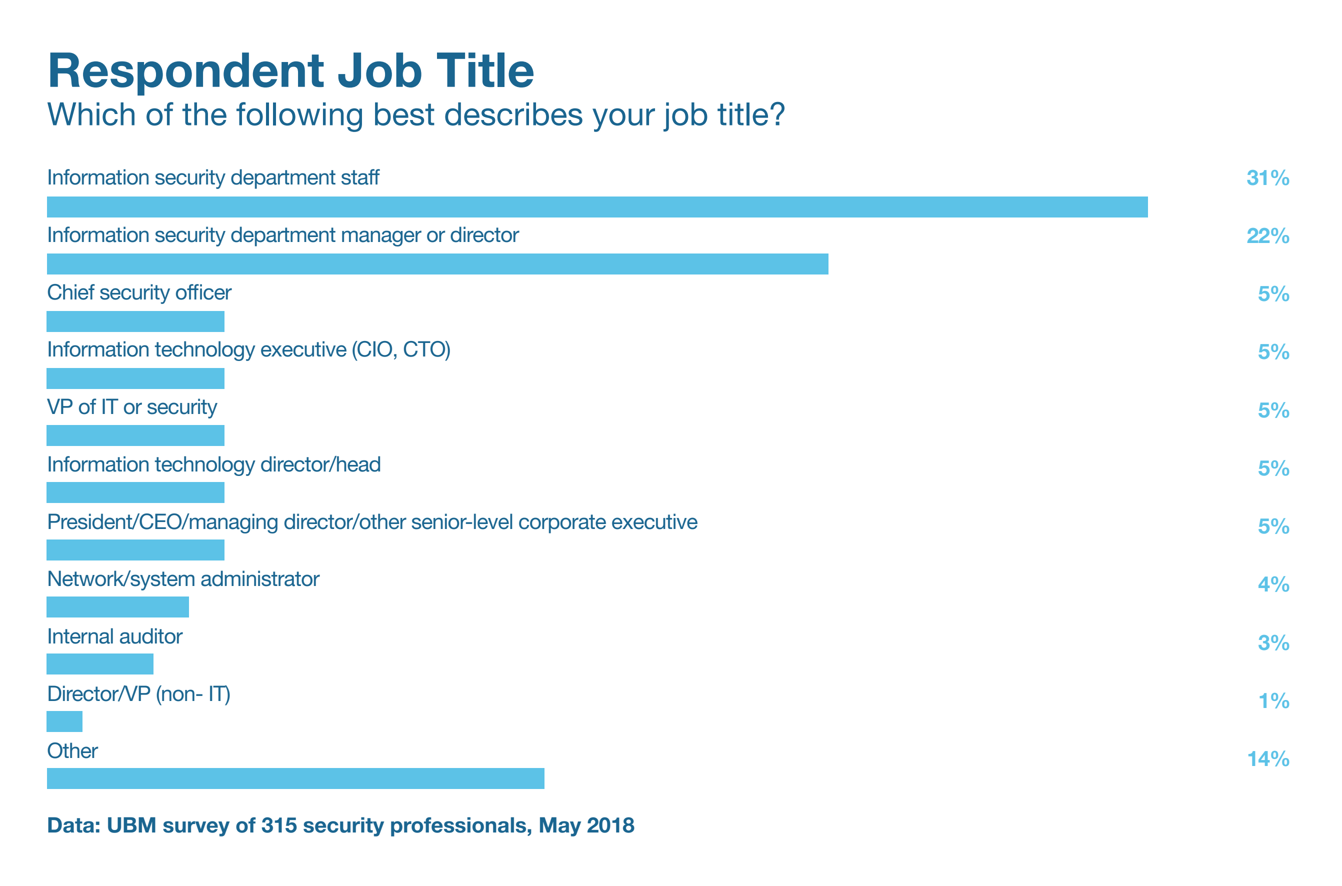


Respondent Salary

What is your current annual salary?

Data: UBM survey of 315 security professionals, May 2018

Figure 21

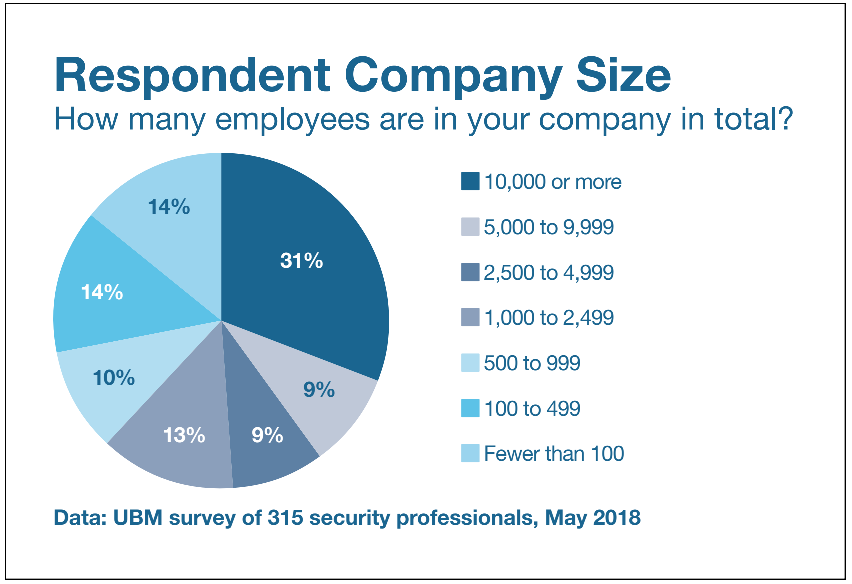


Data: UBM survey of 315 security professionals, May 2018

Previous Next

Table of Contents

Figure 22



Respondent Company Size

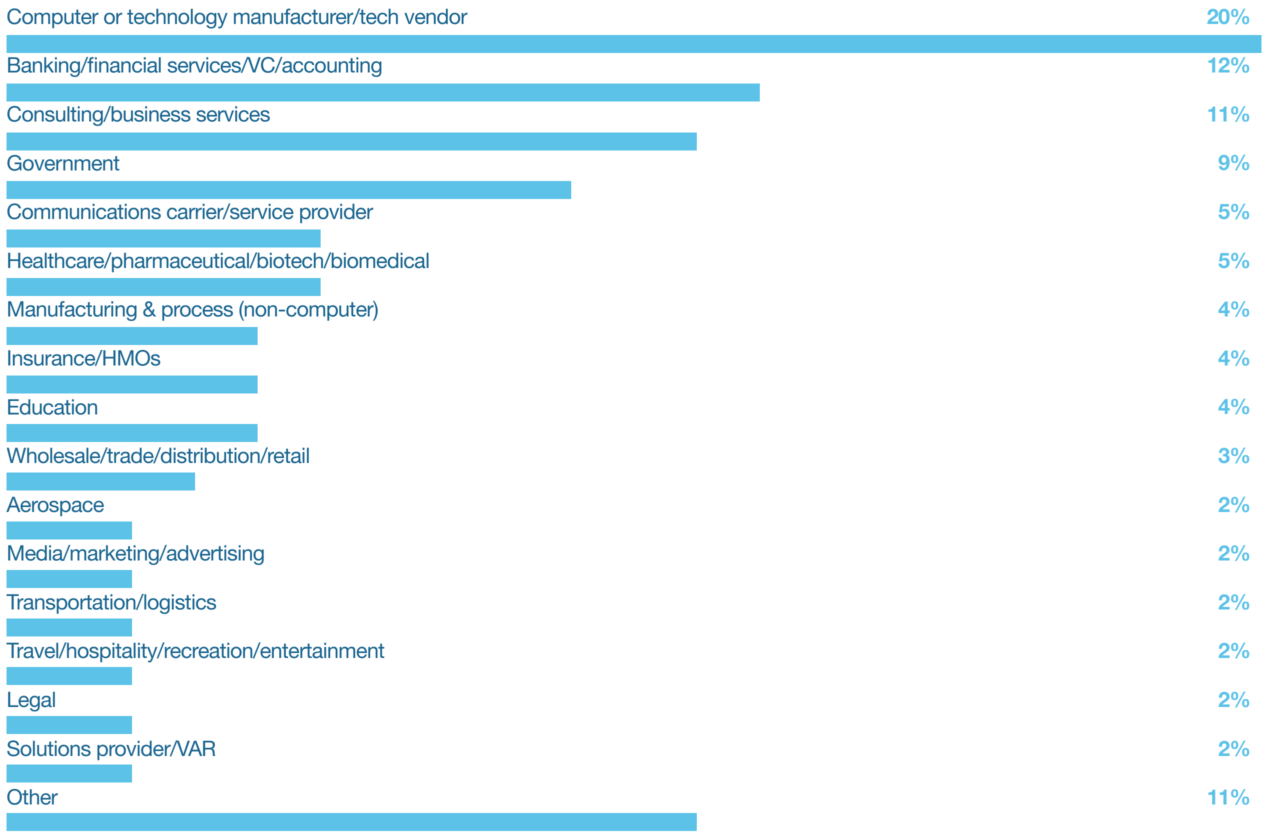
How many employees are in your company in total?

Data: UBM survey of 315 security professionals, May 2018

Figure 23

Respondent Industry

What is your organization’s primary industry?



Data: UBM survey of 315 security professionals, May 2018

Figure 24

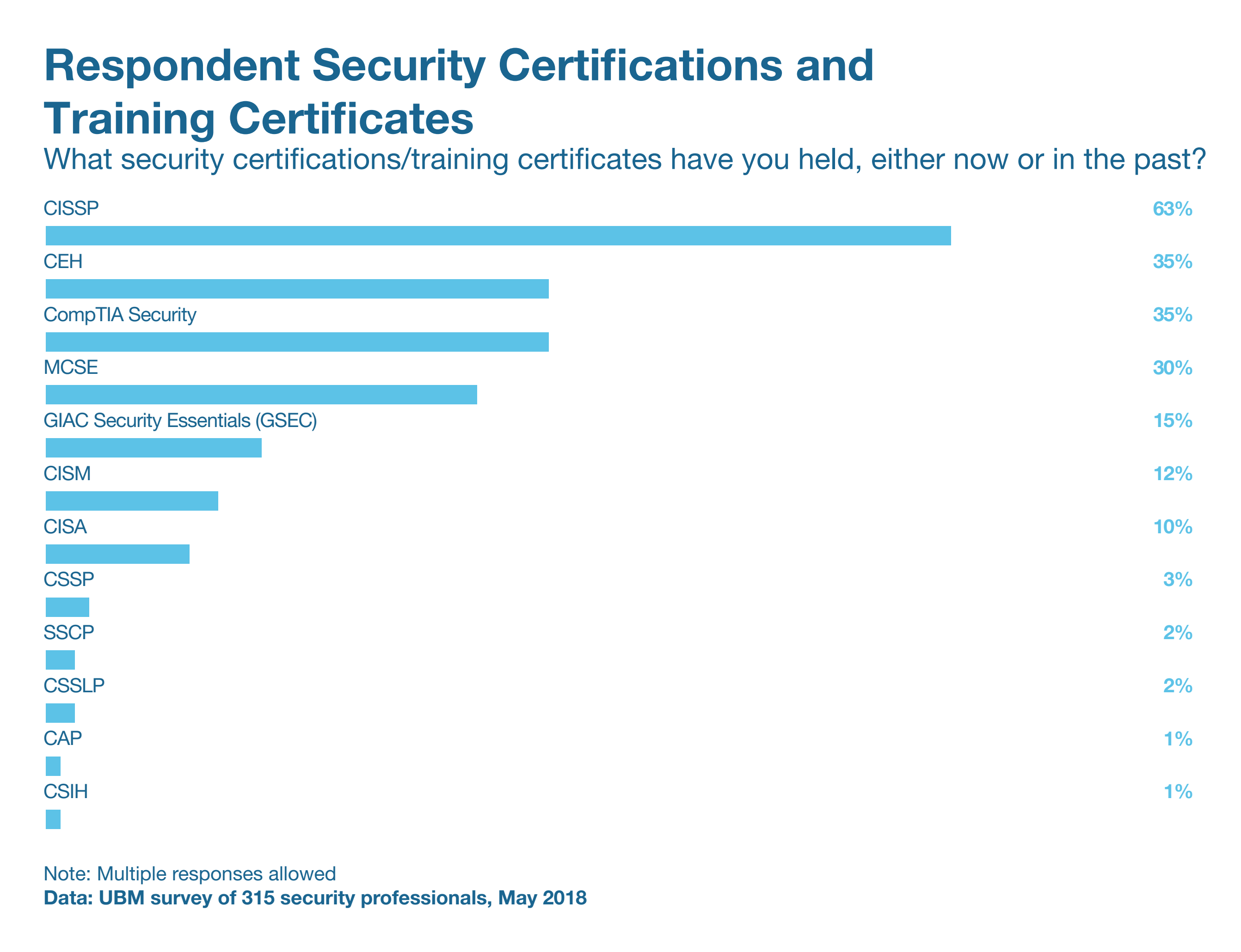
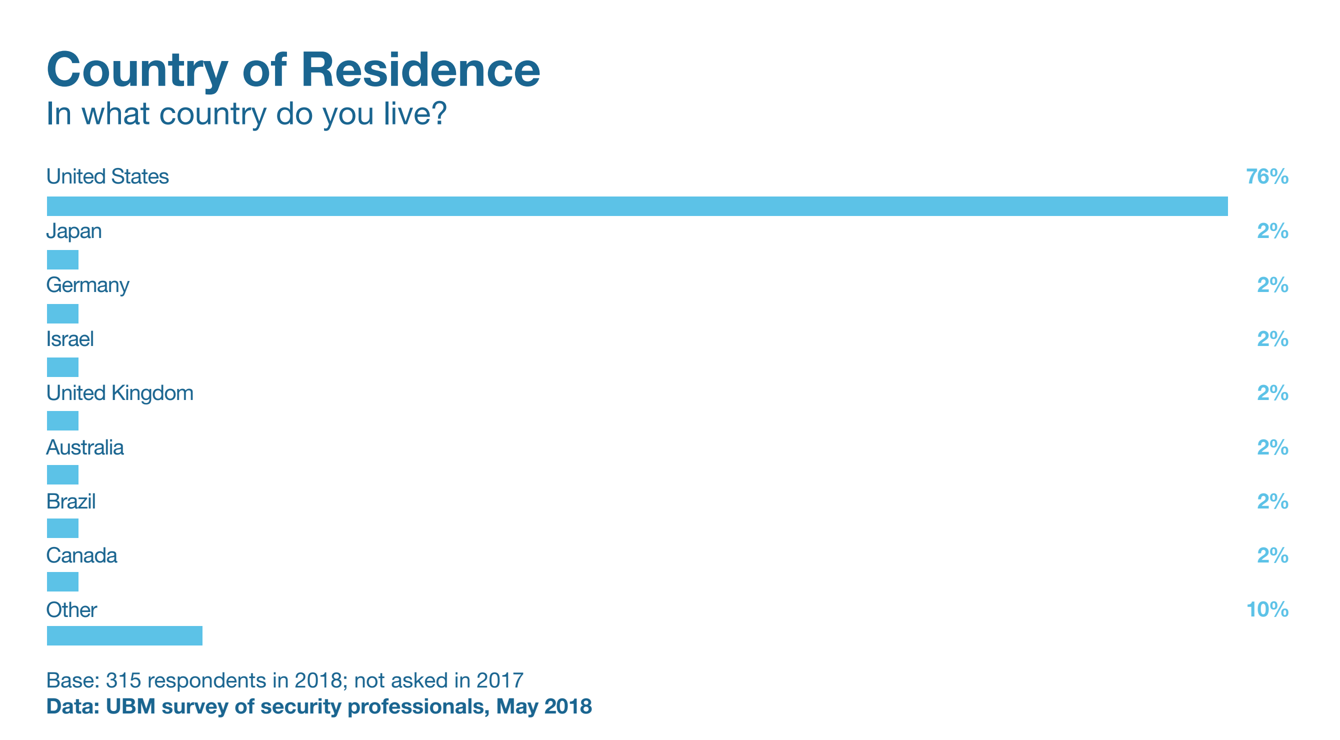

Respondent Security Certifications and Training Certificates
What security certifications/training certificates have you held, either now or in the past?
CISSP 63%
CEH 35%
CompTIA Security 35%
MCSE 30%
GIAC Security Essentials (GSEC) 15%
CISM 12%
CISA 10%
CSSP 3%
SSCP 2%
CSSLP 2%
CAP 1%
CSIH 1%
Note: Multiple responses allowed
Data: UBM survey of 315 security professionals, May 2018

Figure 25


Country of Residence
In what country do you live?
United States 76%
Japan 2%
Germany 2%
Israel 2%
United Kingdom 2%
Australia 2%
Brazil 2%
Canada 2%
Other 10%
Base: 315 respondents in 2018; not asked in 2017
Data: UBM survey of security professionals, May 2018