black hat® EUROPE 2017

www.blackhat.com

November 2017

Next

The 2017 Black Hat Europe Attendee Survey

The Cyberthreat in Europe

Information security leaders in Europe believe that a major breach of critical infrastructure is coming and that data breaches in their own organizations are imminent. Yet most are not ready.

TABLE OF CONTENTS

Figures

EXECUTIVE SUMMARY

Most information security professionals in Europe believe a cyber attack will breach critical infrastructure across multiple countries within the next two years. Many also believe that recent hacker activity emanating from Russia and China has made European enterprise data less secure than before. Significantly, few expect the EU's Directive on security of network and information systems (NIS Directive) will do much to improve security in 2018.

These are some of the key takeaways from a September 2017 survey of 127 IT and security professionals from more than 15 European countries. Among the survey respondents were chief executives, CISOs, CIOs, CTOs, auditors, and business executives from organizations in more than 20 sectors, including financial services, biotechnology, construction, healthcare, communication, and government.

The survey asked respondents about their biggest security worries and about their cyber-defense capabilities. Respondents offered feedback about the threats their organizations are facing, their budgets and staffing plans, the shortage of information security skills, and the impact of implementing the EU's General Data Protection Regulation (GDPR) requirements.

The survey results paint a bleak picture of the ability of European organizations to defend themselves and their critical infrastructure against modern cyber-attack threats. Information security professionals in Europe, like their counterparts in the United States, are under siege from multiple quarters. Cyber defenses are being stretched to the limit by a perfect storm of threats from organized cybercrime groups and nation-state-sponsored threat actors. Organizations are as concerned about critical infrastructure breaches as they are about attacks on their own IT systems and services. Security professionals in Europe feel they do not have the time, budget, or staff to meet the growing security challenges and the additional burdens imposed on them by regulations such as GDPR.

EXECUTIVE SUMMARY

The 2017 Black Hat Europe Survey provided a wide range of insights into the state of cybersecurity in the region, including:

- 77% of respondents believe a cyber attack will breach critical infrastructure across European countries within the next two years.
- 42% say cyber espionage by major nation-states such as Russia and China and attacks by rogue nations such as North Korea pose the biggest threat to EU critical infrastructure.
- Only 11% believe that implementing the NIS Directive will make EU critical infrastructure much more secure.
- Nearly two-thirds of the respondents believe it is likely their organizations will have to respond to a major security breach in the next 12 months.
- 39% say that GDPR requirements will have a major impact on current staff and IT budgets in the coming year.
- Nearly 6 in 10 of the respondents believe they do not have the budget to defend adequately against current and emerging threats.

SYNOPSIS

RESEARCH

Survey Name The 2017 Black Hat Europe Survey

Survey Date September 2017

Region Europe

Number of Respondents 127 IT and security professionals. The greatest possible margin of error for the total respondent base (N=127) is +/- 8.6 percentage points. 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 Europe conference.

Methodology In September 2017, Dark Reading and Black Hat conducted a survey of IT and security professionals from more than 15 European countries and the US. The online survey yielded data from 127 management and staff security professionals, predominantly at large companies, with 52% working at companies with 1,000 or more employees. Forty-six percent of the respondents hold the CISSP security professional credential; 39% are 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.

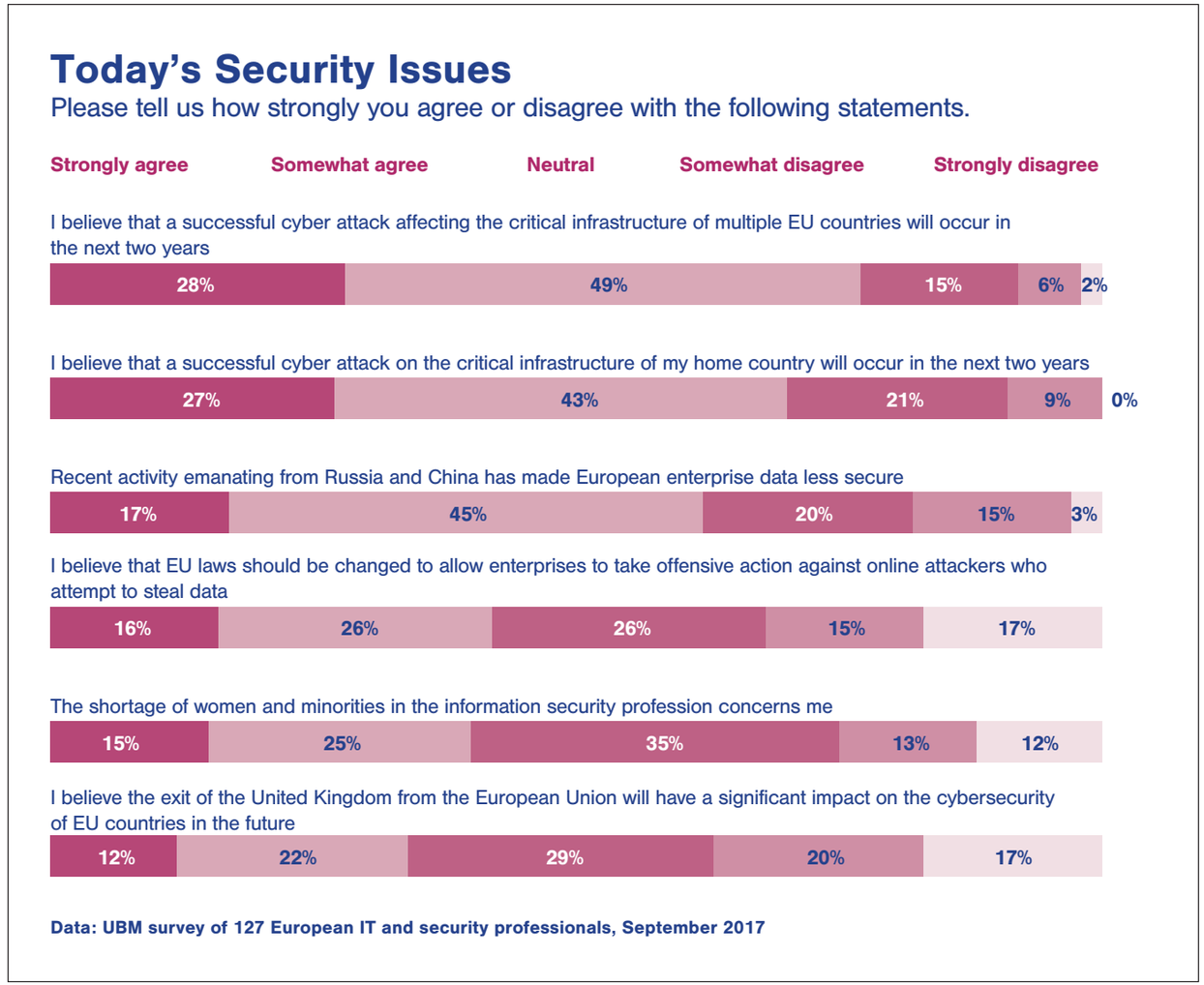
European Enterprises Highly Concerned about Critical Infrastructure Security

Most IT and security professionals we polled in our survey believe that a major cyber attack on European critical infrastructure is imminent. Seventy-seven percent believe somewhat strongly that such an attack will happen within the next two years — and that it will affect multiple countries in the region. In fact, respondents are even more worried about a multicountry breach than about a critical infrastructure breach limited to their own country. Fifteen percent are neutral on the topic, while just 8% disagree (**Figure 1**).

These sentiments are remarkably similar to those expressed by IT and security professionals in our 2017 Black Hat USA Attendee Survey in July and are a warning that critical infrastructure in Europe is as much at risk as it is in the United States.

In fact, limited cyber attacks on European infrastructure have already occurred. One example is the December 2015 cyber intrusions at three regional power distribution companies

Figure 1

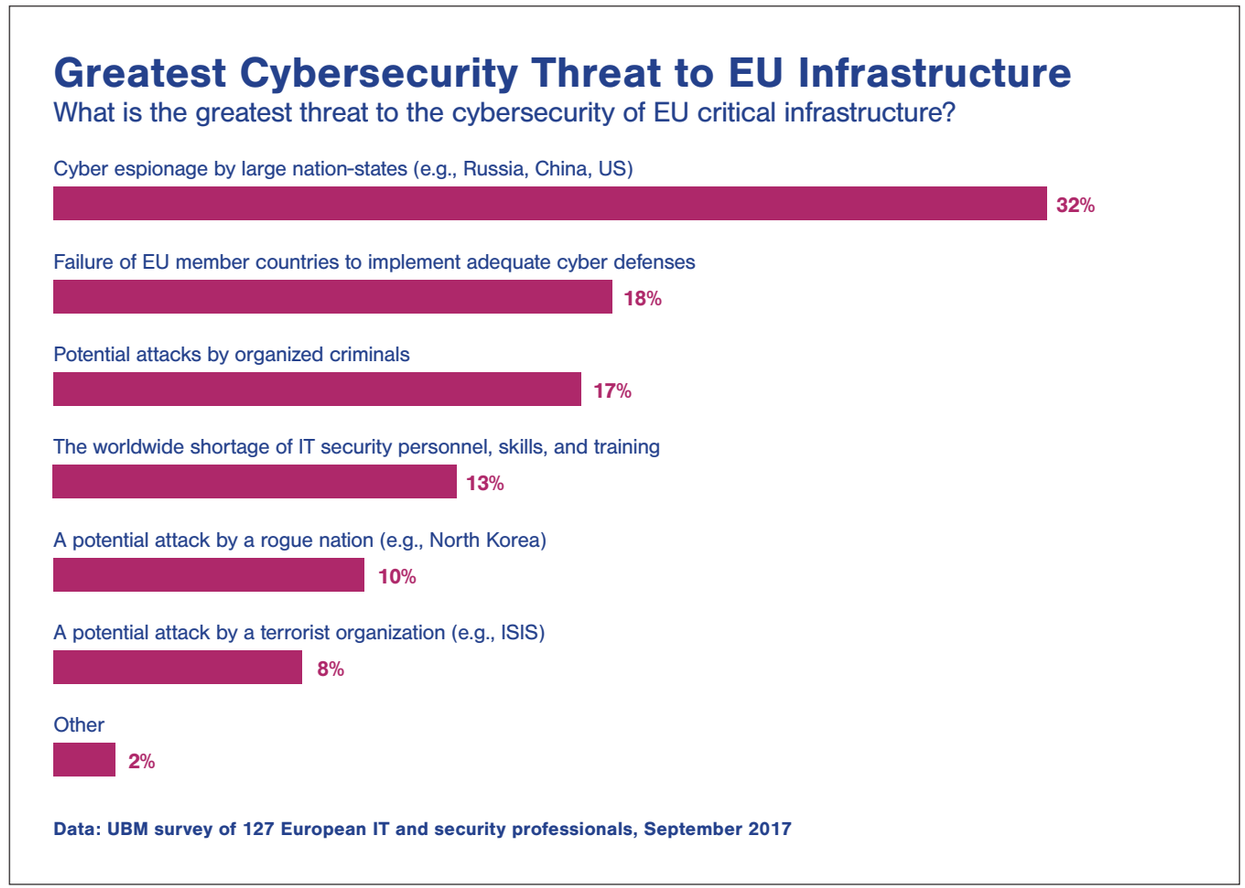


in Ukraine that caused unscheduled power outages for some 225,000 people. Another cyber attack on an electric transmission station a year later left nearly 20% of Ukraine's capital, Kiev, without power for about an hour. In late 2014, a steel mill in Germany became the victim of one of the first confirmed cases in Europe of a digital attack causing physical destruction of equipment.

There also is broad concern about cyber attacks between nation-states. European countries such as Germany are concerned about cyber spying by governments in Russia, China, and Iran, and Germany's domestic intelligence agency, BfV, has cautioned that cyber espionage by these nations poses a particular threat to its critical infrastructure. As in the US, the general elections in France in April 2017 were overshadowed by reports of Russian government sponsored groups allegedly using cyber attacks and misinformation campaigns to try and derail the campaign of candidate Emmanuel Macron.

These incidents, combined with widespread reporting about cyberthreats emanating from nation-state-sponsored hacking organizations, have clearly eroded confidence in critical infrastructure security among IT security professionals in Europe. In fact, 62% of our survey respondents fear that enterprise data in Europe has become less secure because of recent activities in Russia and China.

Figure 2

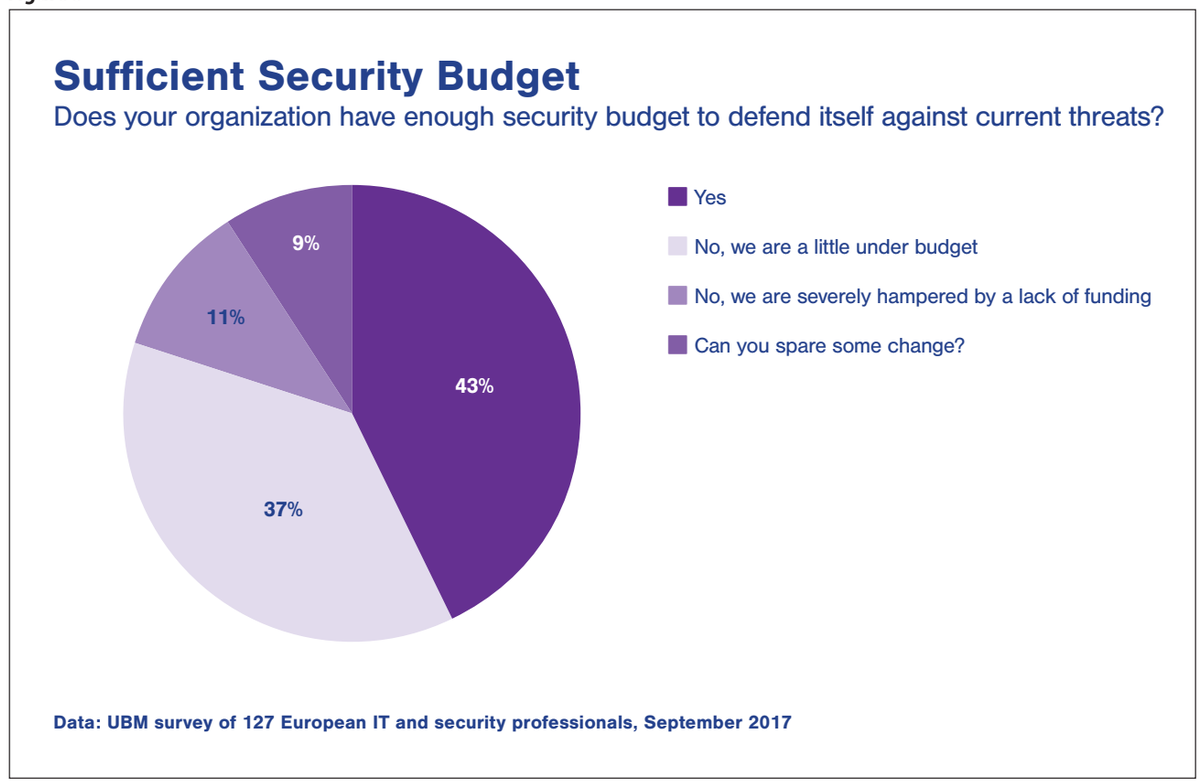


Roughly the same proportion of respondents in our 2017 Black Hat USA Attendee Survey expressed a similar sentiment — clearly, concerns over nation-state-sponsored activities are not restricted to specific geographies.

Forty-two percent of respondents in the European survey believe that EU law should be changed so enterprises can take offensive action against attackers who attempt to steal their data. These results suggest that IT professionals are frustrated over the ability of attackers to go unpunished while governments grapple over questions of attribution and proportional response.

While European IT security leaders are broadly concerned about an imminent breach, their opinions vary as to which is the greatest threat to critical infrastructure. Almost half (49%) cite a foreign power — terrorist organization, rogue nation, or large nation-state — as the primary threat. Seventeen percent point to attacks by organized criminals, and 13% believe the shortage of security skills poses the biggest threat. Many respondents are also concerned about European governments not paying enough attention to the problem.

Figure 3



Eighteen percent of the respondents see a failure by EU member nations to implement adequate security measures as the single biggest threat to critical infrastructure (**Figure 2**).

Can the implementation of the NIS Directive — the first EU-wide legislation on cybersecurity — help move the needle forward in 2018? Most of the IT security professionals in our survey don't think so. In fact, just 11% believe EU critical infrastructure will be more secure in 2018 because of NIS. Thirty-two percent, or about a third of the respondents,

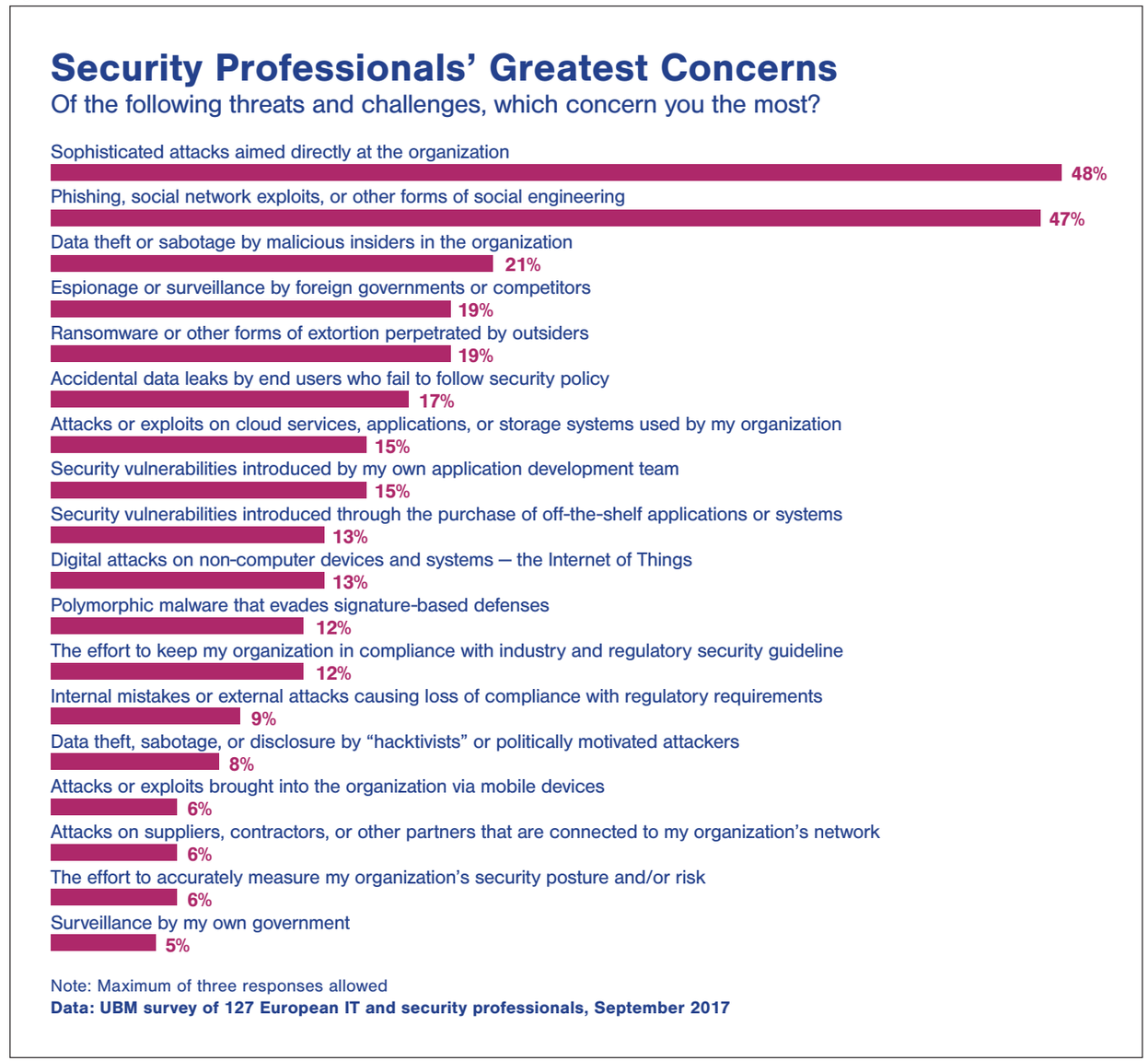
see NIS as contributing to an incremental improvement in critical infrastructure security, while 10% do not expect any change to result from it. Forty-five percent, a plurality of our respondents, say they don't know yet how NIS will affect cybersecurity.

Enterprise IT Security Also Threatened

While threats to critical infrastructure concern IT security leaders in Europe, worries over enterprise security are equally high. Just as with critical infrastructure, many IT security professionals in Europe appear resigned to the notion of a near-term breach in their own organizations. In fact, a troubling 65% of the respondents in the 2017 Black Hat Europe Survey believe that they will have to respond to a major security incident in the next 12 months. Only 27% feel confident enough in their defenses to believe that such an event will be unlikely in the coming year.

A few factors appear to be contributing to this sense of insecurity. Budget is a big one. The 2017 Black Hat Europe Survey shows that organizations in Europe are struggling with the same lack of security funding that US organiza-

Figure 4



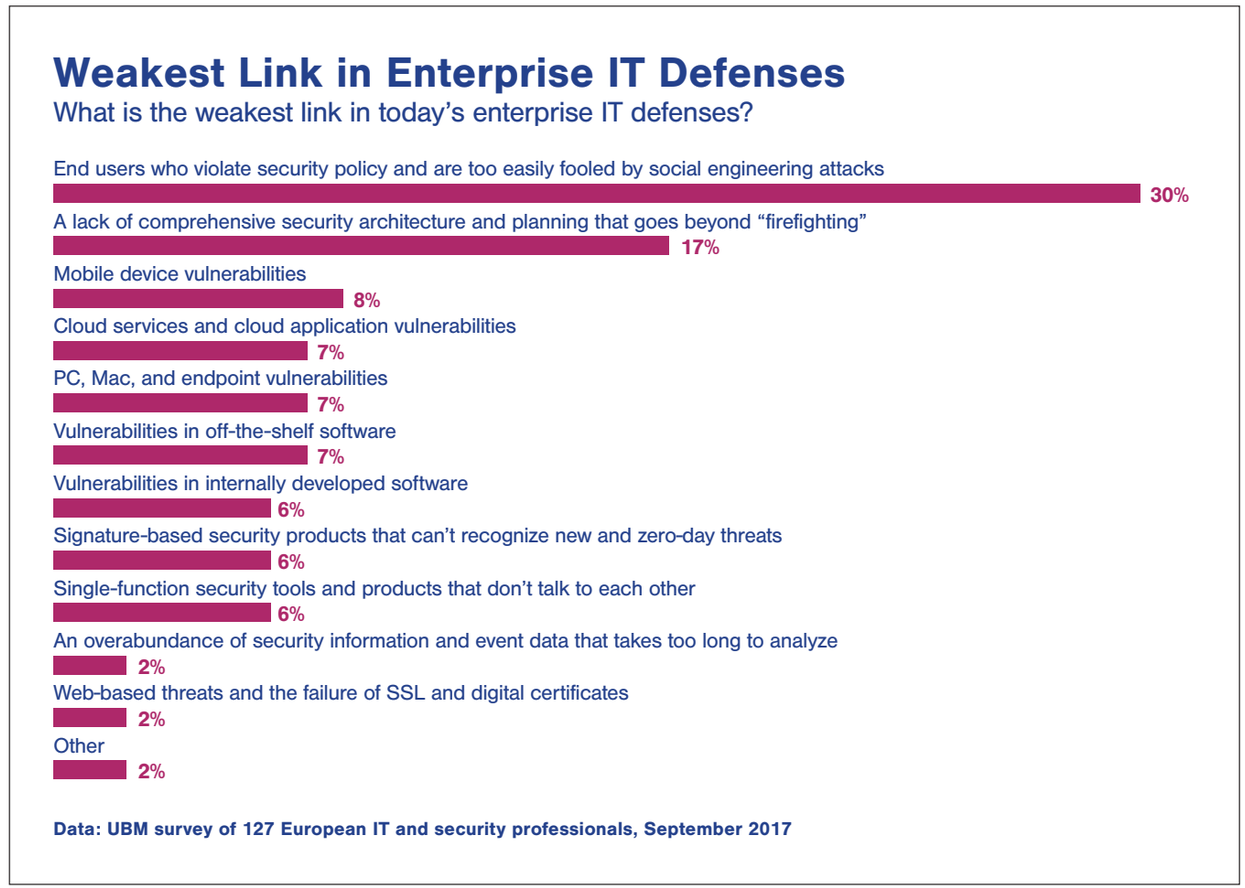
tions are experiencing. Fifty-seven percent of the respondents in our Europe 2017 survey say they do not have enough of a security budget to mount an adequate defense (**Figure 3**). In comparison, 58% of US IT security pros expressed the same sentiment in the 2017 Black Hat Attendee survey. Security staffing is another big issue. Sixty-two percent of the IT pros in the 2017 Black Hat Europe Survey say they do not have enough security staff to defend adequately against modern cyberthreats. In fact, just 38% say they are adequately staffed on the security front.

A constant barrage of reports about data breaches is likely affecting the pessimistic outlook among security professionals in our survey. In the United States, the Identity Theft Resource Center (ITRC) reported a total of 791 publicly disclosed data breaches in the first half of 2017 alone. Some of them, such as the recent intrusion at Equifax that compromised sensitive data belonging to a staggering 145.5 million people, have been impossible to overlook.

At this pace, the total number of US breaches this year will easily top the record-busting 1,093 incidents that ITRC reported for all of 2016. European organizations in general have reported substantially fewer data breaches than American entities, but many of the same factors that have caused major cyber breaches in the US are at play in Europe as well.

Security leaders in Europe reported many of

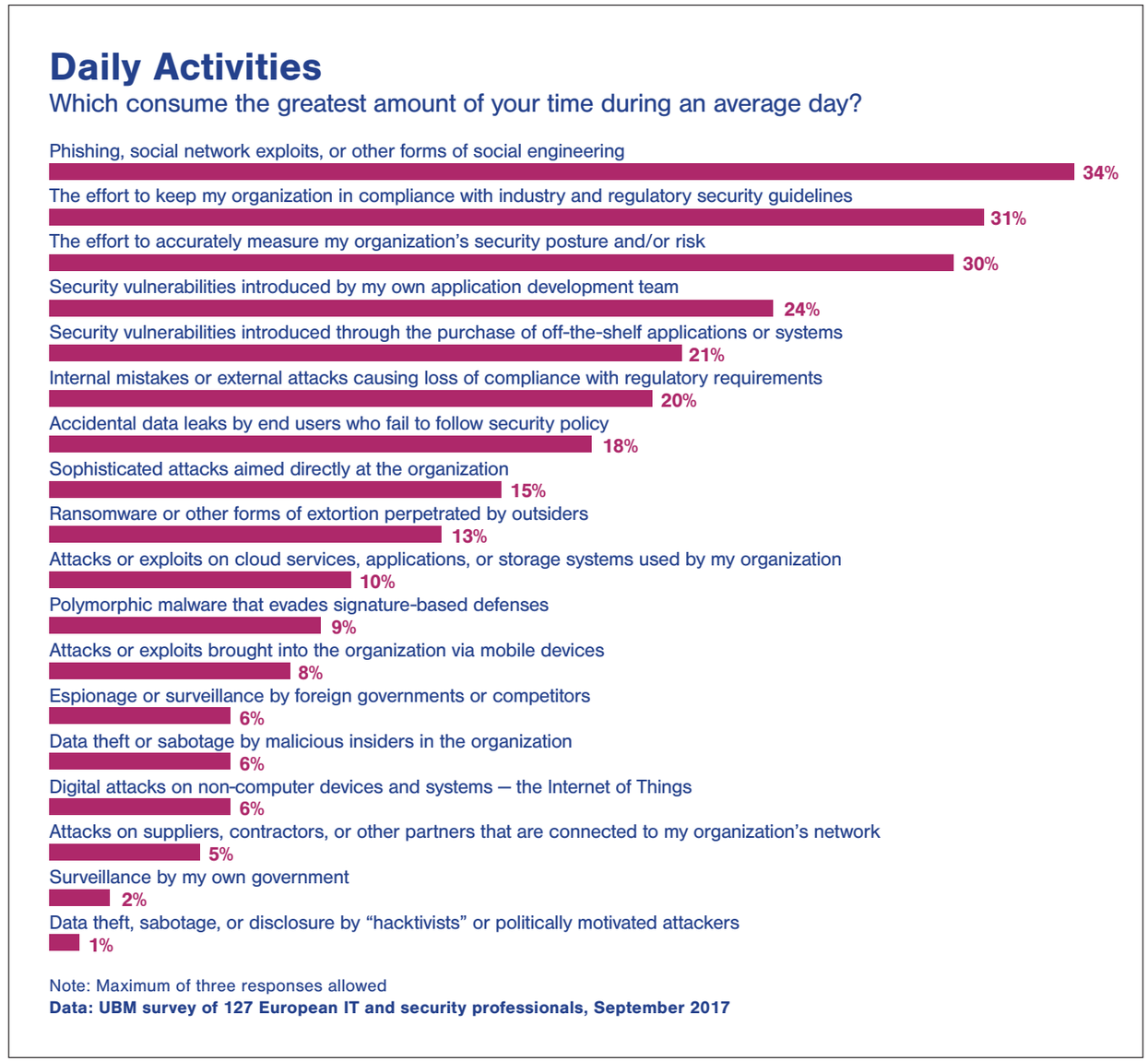
Figure 5



the same worries and priorities as their counterparts in the United States. When asked which threats cause the greatest concern, 48% cited sophisticated targeted attacks and 47% pointed to phishing and other social engineering attacks. The responses are remarkably similar to the US Black Hat Attendee Survey, and they're a clear indication that geography makes no difference when it comes to mounting defenses against potential intrusions and data breaches. Twenty-one percent expressed concern about data loss caused by insiders. Nineteen percent cited ransomware as a top concern, and an equal percentage cited concerns about espionage or surveillance by a foreign actor. Seventeen percent pointed to accidental leaks caused by end users who failed to abide with security polices (**Figure 4**).

Somewhat surprisingly, cloud and mobile security ranked relatively low in the overall list of top concerns among security. Only 15% of survey respondents perceive attacks on cloud services, applications, and storage systems as a top threat. An even smaller 6% feel that way about attacks and exploits being brought into their organizations via mobile devices. Even when

Figure 6



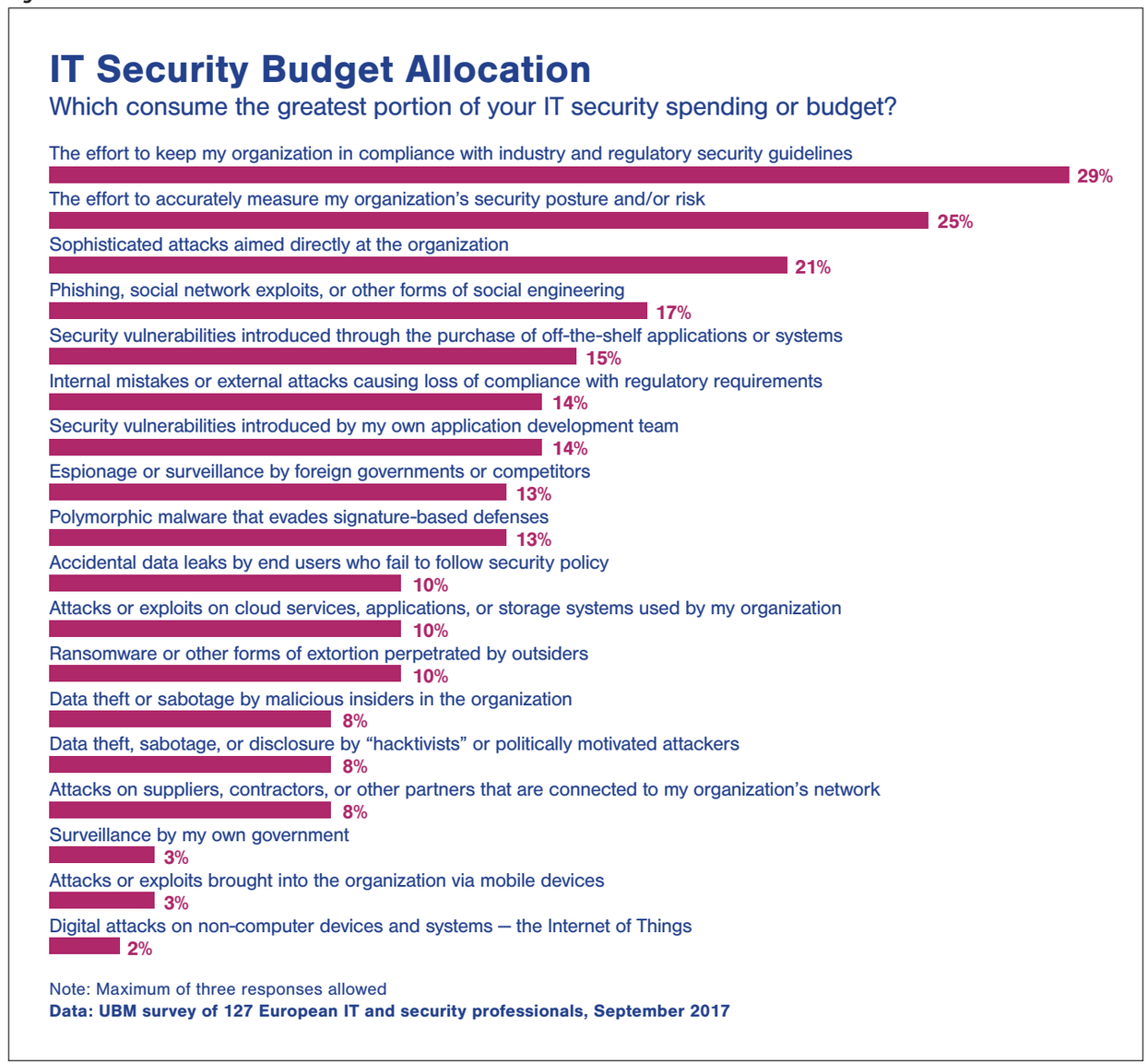
asked which threats would likely cause them the most concern in two years, only 19% and 18% cited cloud and mobile security, respectively. The responses suggest that many European organizations are confident they have a handle on cloud and mobile security issues.

The WannaCry outbreak in May and reports of a general rise in ransomware — Denmark's shipping giant Maersk suffered a $300 million hit — have clearly affected Europe's information security professionals. Thirty-six percent of the IT and security pros surveyed cited ransomware as the most serious cyberthreat to emerge in the last 12 months. A major data leak/dump resulting from a trusted third party was cited by 17% as the most serious threat to emerge in 2017.

Identifying Weaknesses

IT security professionals in Europe are divided over where the major weaknesses in their defenses exist. A plurality (30%) believes that end users who violate security policy and are too easily fooled by social engineering attacks are the weakest link. Recent breach statistics certainly support that concern. A startling

Figure 7



43% of the 1,935 breach incidents that Verizon investigated in 2016 involved social engineering.

But respondents are also concerned that IT security has become a tactical, firefighting mission, rather than a strategic imperative. Seventeen percent in the 2017 Black Hat Europe Survey said their biggest weakness stemmed from a lack of planning and from not having a security architecture that was strategic enough to deal with modern threats (**Figure 5**). Nineteen percent believe that the primary reason why their defense strategies fail is because their security architecture is not well integrated and is riddled with too many single-purpose technologies.

The shortage of skilled security professionals is also a key issue for many respondents. Thirty-nine percent believe that a lack of required skills is the primary reason why security strategies fail. This response reflects the concern over what can only be described as a crippling and deepening skills shortage in Europe — a shortage also felt around the world. According to research by (ISC)[2], a major association of security professionals, over the next few years European organizations are planning the fastest rate of cybersecurity hiring anywhere in the world. Yet the region is projected to be short as many as 350,000 security professionals by 2022.

Figure 8

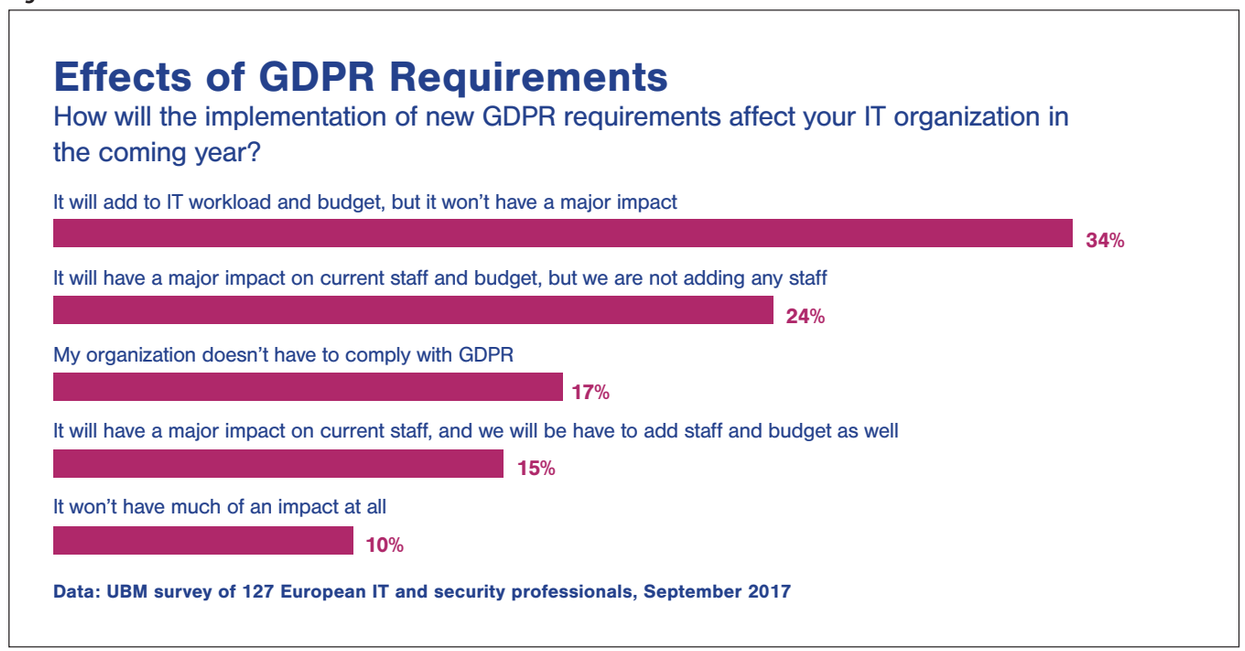
Interestingly, top executives in Europe seem a bit more engaged with cybersecurity matters than top execs in the US. Only 13% of the survey respondent cited a lack of commitment and support from top management as a reason why enterprise IT security strategies fail, compared to 19% who felt that way in the US. To some extent, top executives in Europe also seemed to be on the same page as IT and security executives with regard to their biggest security concerns. When asked about their top executives' concerns, 28% of respondents cited targeted attacks, and 23% said their top managers were concerned with phishing and social engineering attacks.

Even so, the same disconnect that exists in the US between IT security teams and corporate upper management is evident in Europe as well. Security pros are most worried about targeted attacks, phishing, and insider threats — but they actually end up spending most of their time and budget on compliance (such as GDPR) and risk measurement tasks, because those are a top priority for upper management.

When security pros were asked what consumes most of their time on an average day, two of the top three responses had little to do with their most pressing concerns. Thirty-one percent of the security pros said the effort to keep their organization in compliance with industry and regulatory guidelines consumes most of their time, while 30% cited the task of measuring their organization's security posture and risk. Defense against sophisticated, targeted attacks ranked eighth among the tasks that receive the most time and attention, while insider threats came in at 14th (**Figure 6**).

Not surprisingly, security budgets and spending mirror many of the same priorities as time and manpower. Compliance, for instance, ranked only a distant 12th on the priority list among security pros. But when asked how their security budgets are actually spent, 29% of Black Hat survey respondents said the largest portion of it went toward compliance-related tasks; 25% said it went toward measuring organizational security posture and risk. Measures for dealing with targeted attacks and phishing/social engineering threats ranked only third and fourth in the budget priority list (**Figure 7**).

Figure 9



As in the United States, top management at European companies tends to hold the IT security budget purse strings and steers security spending toward its own priorities. For the moment, those priorities are heavily compliance-focused and not well aligned with the issues that security pros identify as their most pressing concerns. The gap between management and IT security pros in Europe suggests

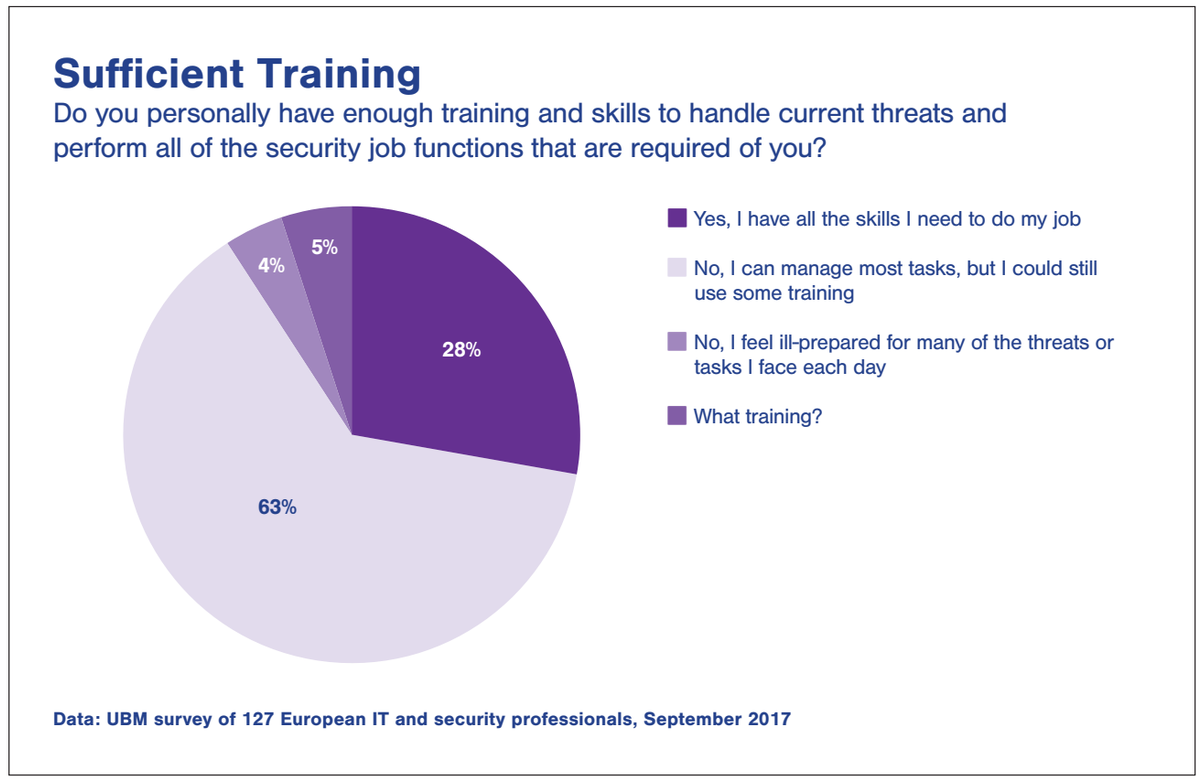
the same kind of communication failure that is evident among companies in the US.

Interestingly, the survey responses show that security professionals also are very concerned about threats emanating from inside their organization. Thirty-eight percent of survey takers said the cyber attacker they feared the most was any individual with inside knowledge. Individuals with knowledge of zero-day vulnerabilities (18%) and those backed by organized crime groups and nation-states ranked second and third, respectively, among the types of cyber attackers that security pros fear the most (**Figure 8**).

Staffing Outlook

The acute shortage of security skills in Europe is being exacerbated by GDPR requirements at many organizations. Thirty-nine percent of organizations that must comply with GDPR say implementing the requirements will have a major impact on their current IT staff. Fifteen percent plan on adding staff and budget because of GDPR. Another 34% believe that implementing GDPR will add to the IT workload and budget but won't otherwise have a major impact (**Figure 9**).

Figure 10



Security skills have become a valuable commodity among European organizations and will almost certainly become more so as the skills gap worsens. More than 50% of the survey respondents already have annual salaries that range between €50,000 and €99,999 ($59,000 and $117,000). Still, few respondents are taking their skills to market. When asked about plans to seek a new IT position in the near future, only 17% said they are actively looking for one.

Many of the security professionals in the

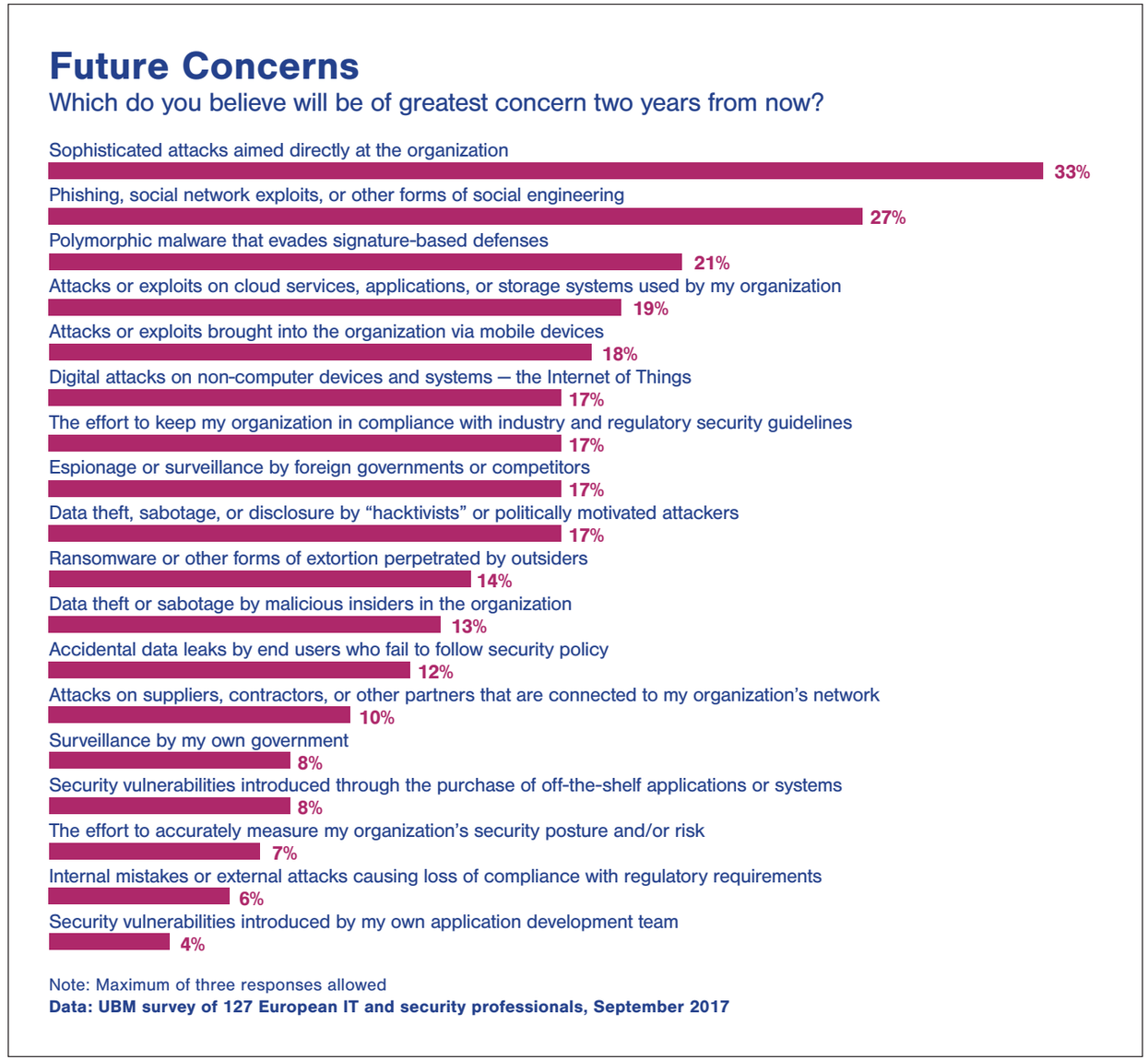
Black Hat survey have professional certifications. Forty-six percent reported having a CISSP certification, and 39% were certified ethical hackers (CEH). Other commonly reported certifications included CISM (24%), MCSE (24%), and CompTIA Security (20%). The survey allowed respondents to check all certifications they have, so it is very likely that many of the respondents have multiple qualifications.

Despite having myriad certifications, 63% of the respondents to the 2017 Black Hat Europe Survey believed they could use more training. When asked if they thought they had enough training and skills to handle current threats and perform job functions, only 28% of security pros surveyed believed they did (**Figure 10**). The responses are a clear warning that a majority of the professionals tasked with defending enterprises against modern threats do not have the skills and are not being adequately trained for the task.

Future Issues

Interestingly, despite the constantly evolving nature of the threat landscape, many respondents to the Black Hat survey expect targeted attacks (33%) and phishing/social engineering

Figure 11



(27%) to remain their top threats two years from now. But they expect other priorities to shift. Polymorphic malware, for instance, currently ranks 11th in terms of the proportion of respondents who view it as a threat. In two years, they expect it will be one of their top three security concerns, perhaps a reflection of the growing ability of new malware to evade signature-based detection tools. More security pros also expect to be dealing with cloud (19%) and mobile security concerns (18%) in two years (**Figure 11**).

One of the most striking differences between IT security pros in the US and Europe is the perception of the security threat around devices that are not computers or smartphones — the Internet of Things. Thirty-four percent of the respondents to the 2017 Black Hat USA Attendee Survey expect digital attacks on IoT devices to be their biggest security threat in two years, an increase from the 28% who ranked IoT as a top concern today. Concerns fueled by the Mirai botnet-enabled attacks of 2016 and reports of widespread vulnerabilities in many Internet-connected devices have made IoT security a hot topic in the United States. In complete contrast, only 17% of IT professionals in the Europe survey said that IoT security will be a top concern in two years, up slightly from the 13% who see it as a major threat currently. While US IT pros expect IoT security to be their top priority in two years, their counterparts in Europe believe IoT will be the sixth-most pressing issue in two years.

Conclusion

Europe's leading IT and security professional are highly concerned about the security of critical infrastructure and their ability to defend their own enterprises against modern cyberthreats. Most believe that a major critical infrastructure breach is likely in the next two years, and that a breach of their own organizations will happen even sooner. Many also believe that implementation of the NIS Directive will do little immediately to bolster European cybersecurity. The data in this report is an urgent call to planners in government and industry to adequately fund cybersecurity initiatives and ensure that regulatory mandates and compliance efforts are properly aligned with security imperatives.

APPENDIX

Figure 12

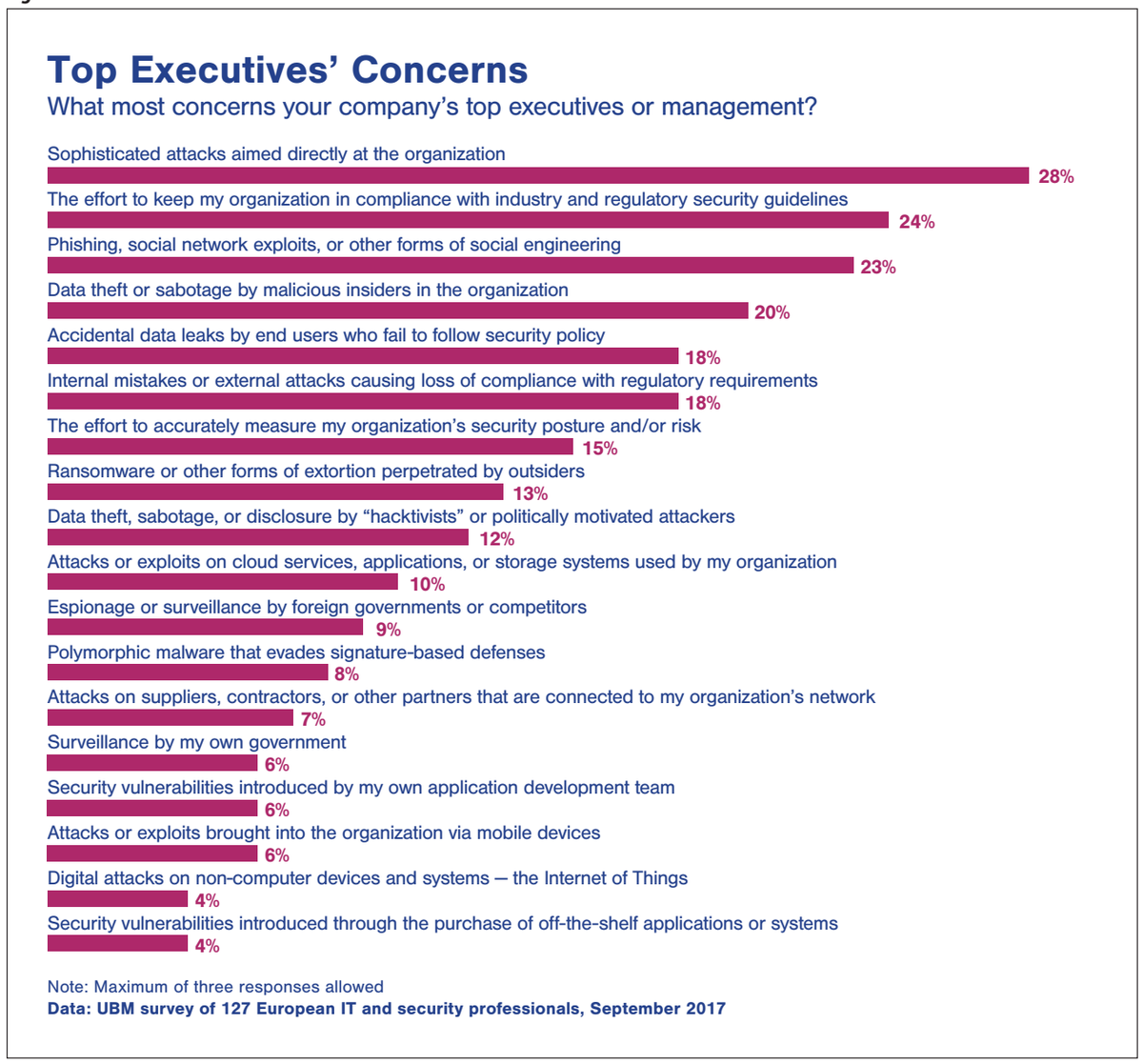
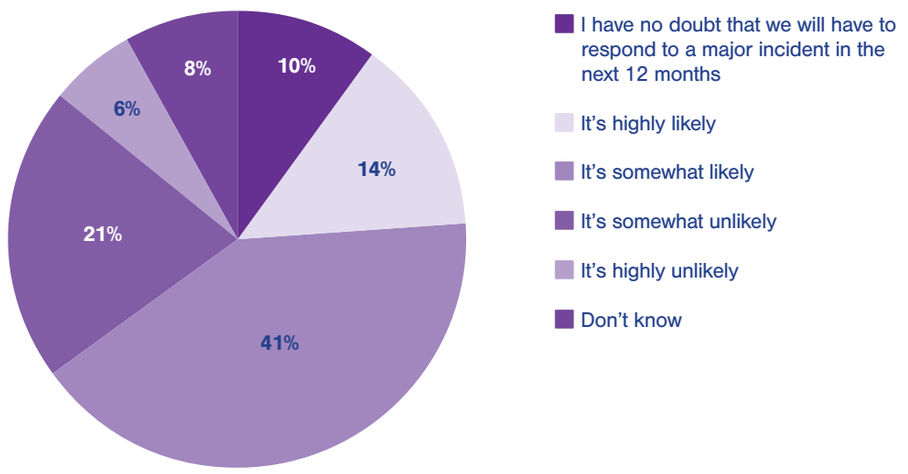


Figure 13

Likelihood of Major Security Breach in the 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?

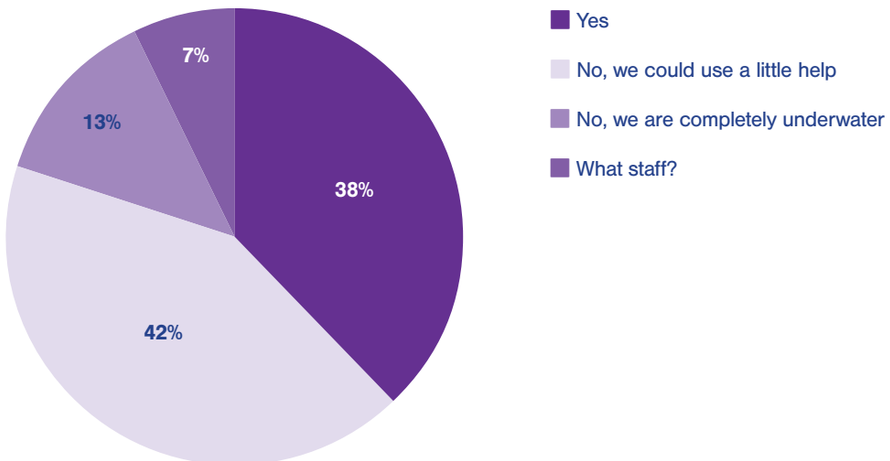


Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 14

Sufficient Security Staff

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



Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 15

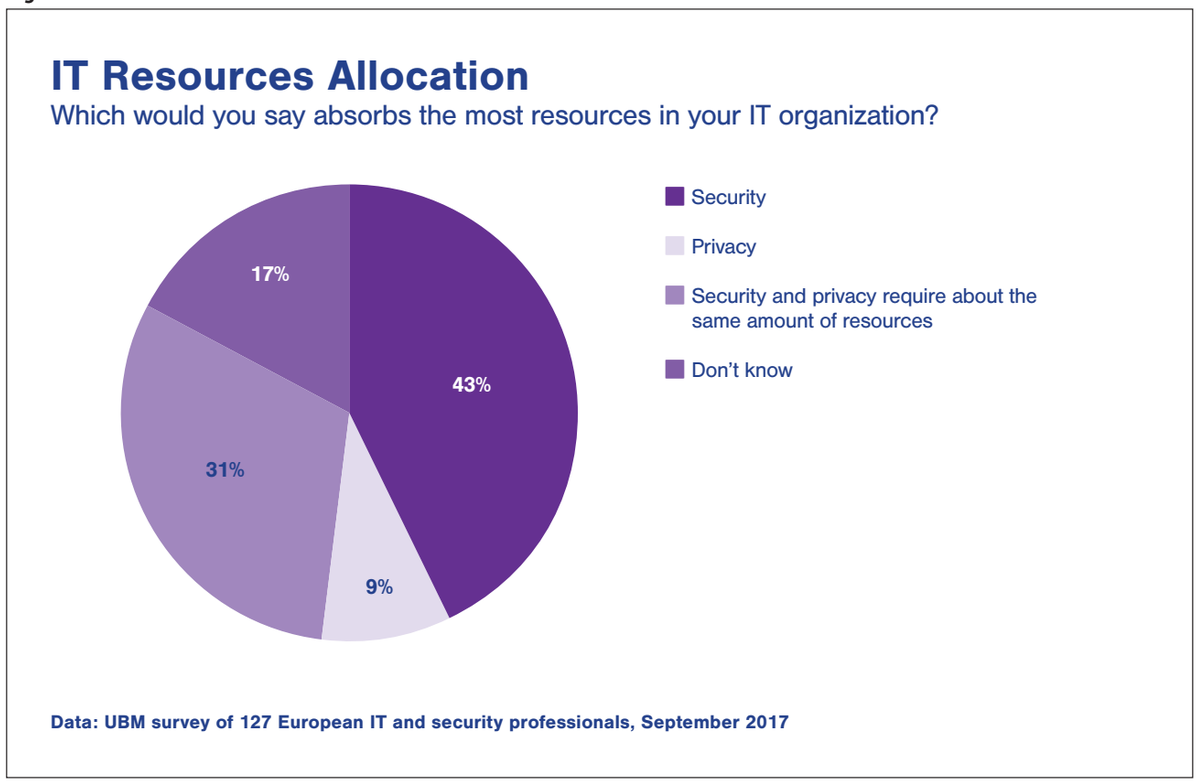
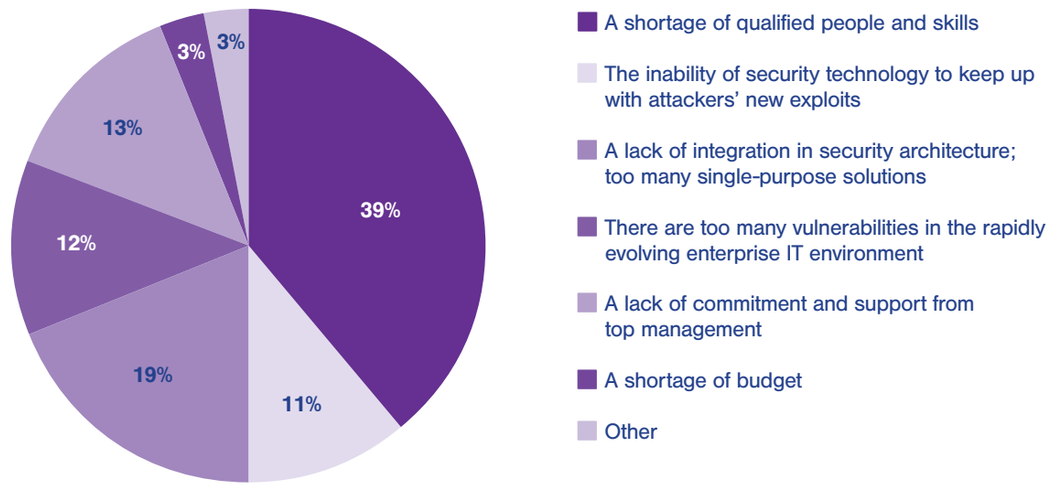

IT Resources Allocation
Which would you say absorbs the most resources in your IT organization?
17%
43%
31%
9%
Security
Privacy
Security and privacy require about the same amount of resources
Don't know
Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 16

Primary Factor in Security Strategies' Failure

What is the primary reason current enterprise IT security strategies and technologies fail?



Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 17

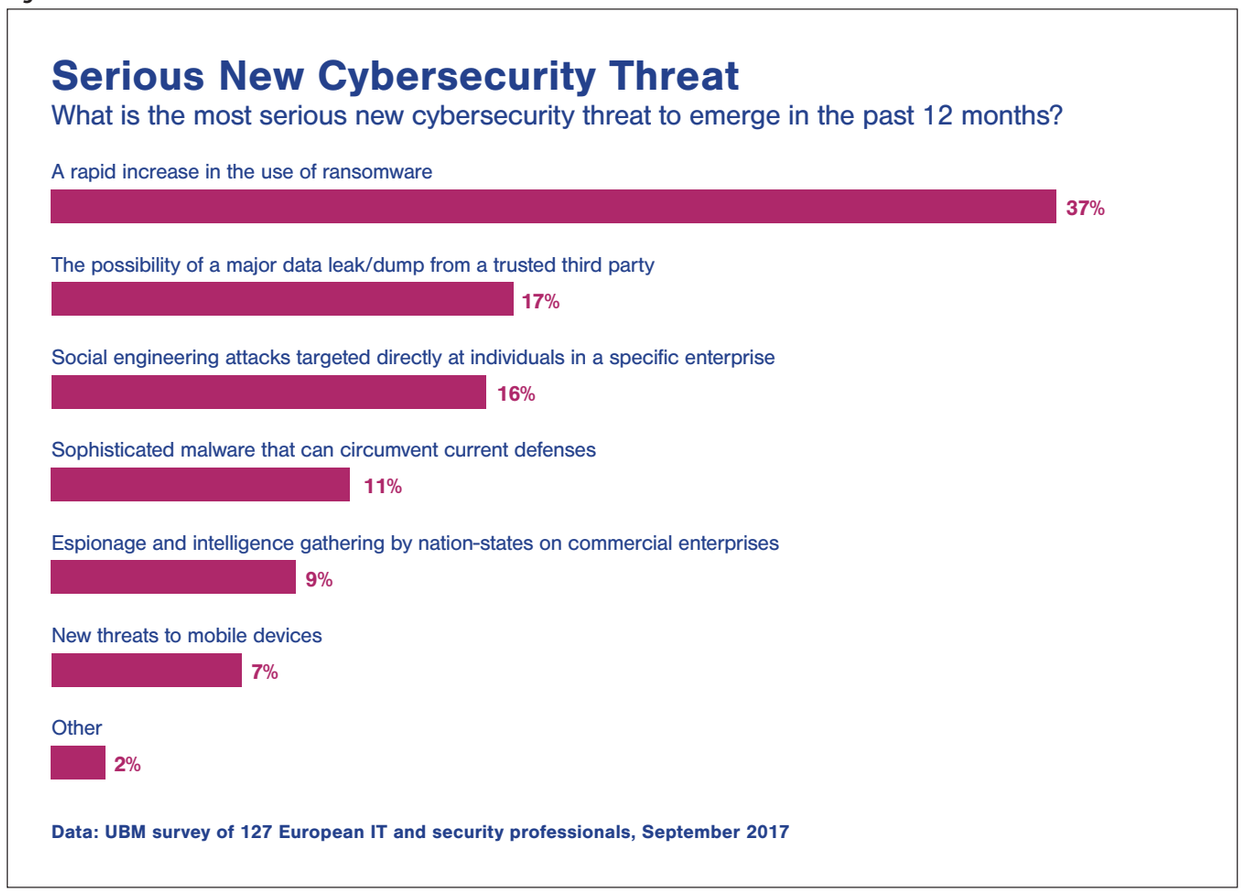
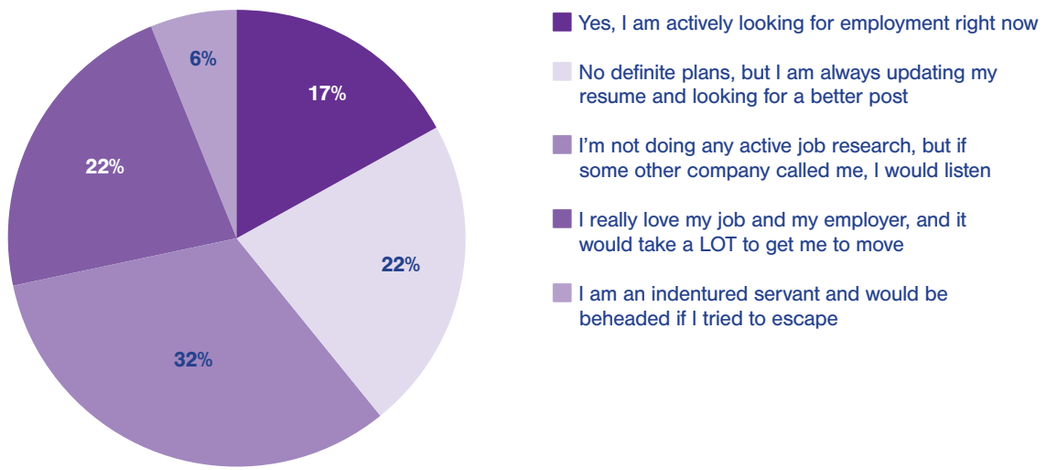

Serious New Cybersecurity Threat
What is the most serious new cybersecurity threat to emerge in the past 12 months?
A rapid increase in the use of ransomware
37%
The possibility of a major data leak/dump from a trusted third party
17%
Social engineering attacks targeted directly at individuals in a specific enterprise
16%
Sophisticated malware that can circumvent current defenses
11%
Espionage and intelligence gathering by nation-states on commercial enterprises
9%
New threats to mobile devices
7%
Other
2%
Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 18

Plans to Seek an IT Security Job

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

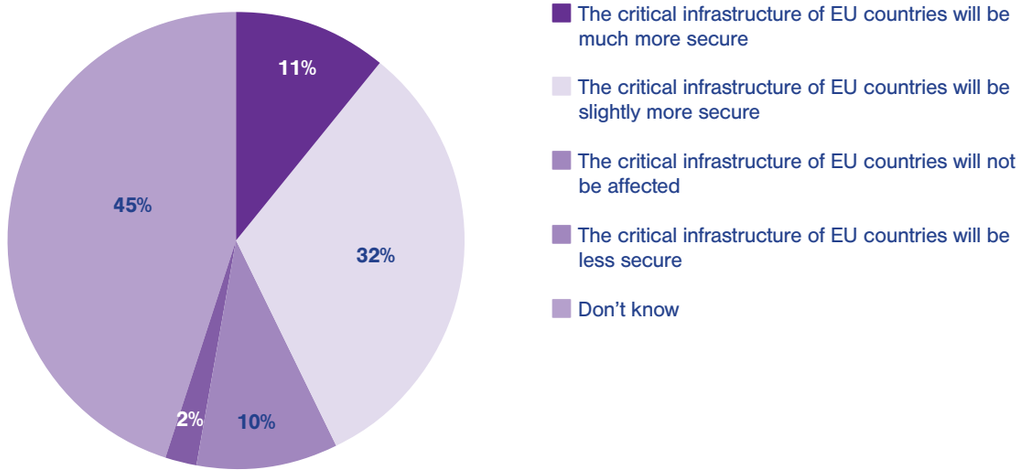


Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 19

Impact of the NIS Directive in 2018

What will be the impact of the implementation of the NIS Directive in 2018?



Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 20

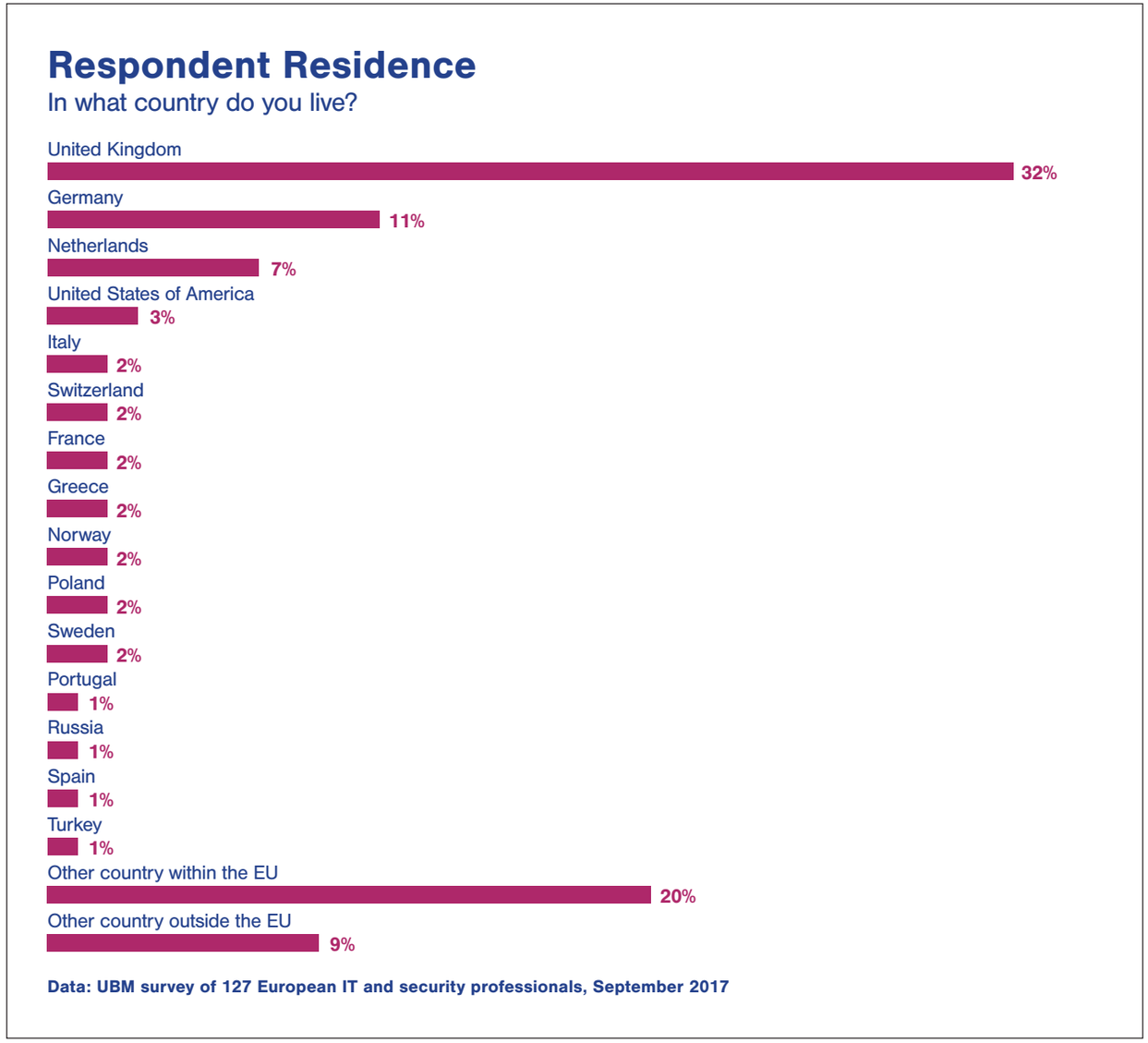

Respondent Residence
In what country do you live?
United Kingdom
32%
Germany
11%
Netherlands
7%
United States of America
3%
Italy
2%
Switzerland
2%
France
2%
Greece
2%
Norway
2%
Poland
2%
Sweden
2%
Portugal
1%
Russia
1%
Spain
1%
Turkey
1%
Other country within the EU
20%
Other country outside the EU
9%
Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 21

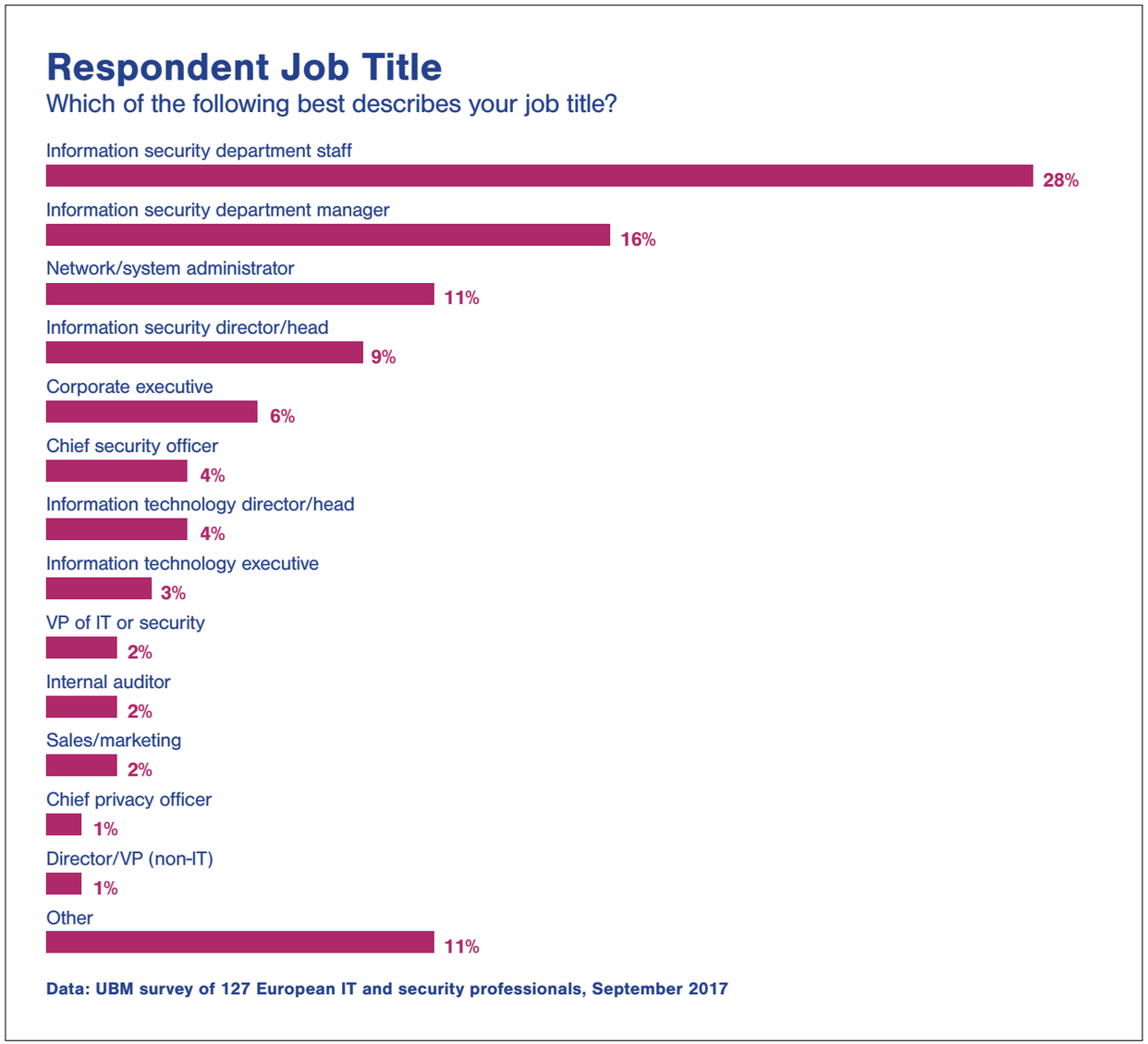

Respondent Job Title
Which of the following best describes your job title?
Information security department staff
28%
Information security department manager
16%
Network/system administrator
11%
Information security director/head
9%
Corporate executive
6%
Chief security officer
4%
Information technology director/head
4%
Information technology executive
3%
VP of IT or security
2%
Internal auditor
2%
Sales/marketing
2%
Chief privacy officer
1%
Director/VP (non-IT)
1%
Other
11%
Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 22

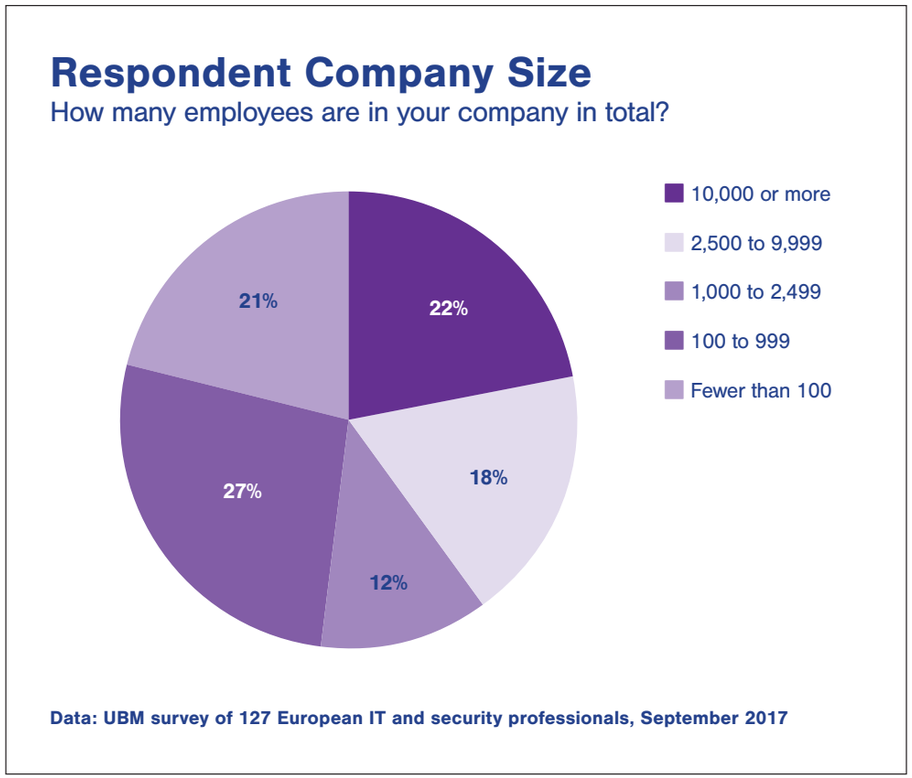
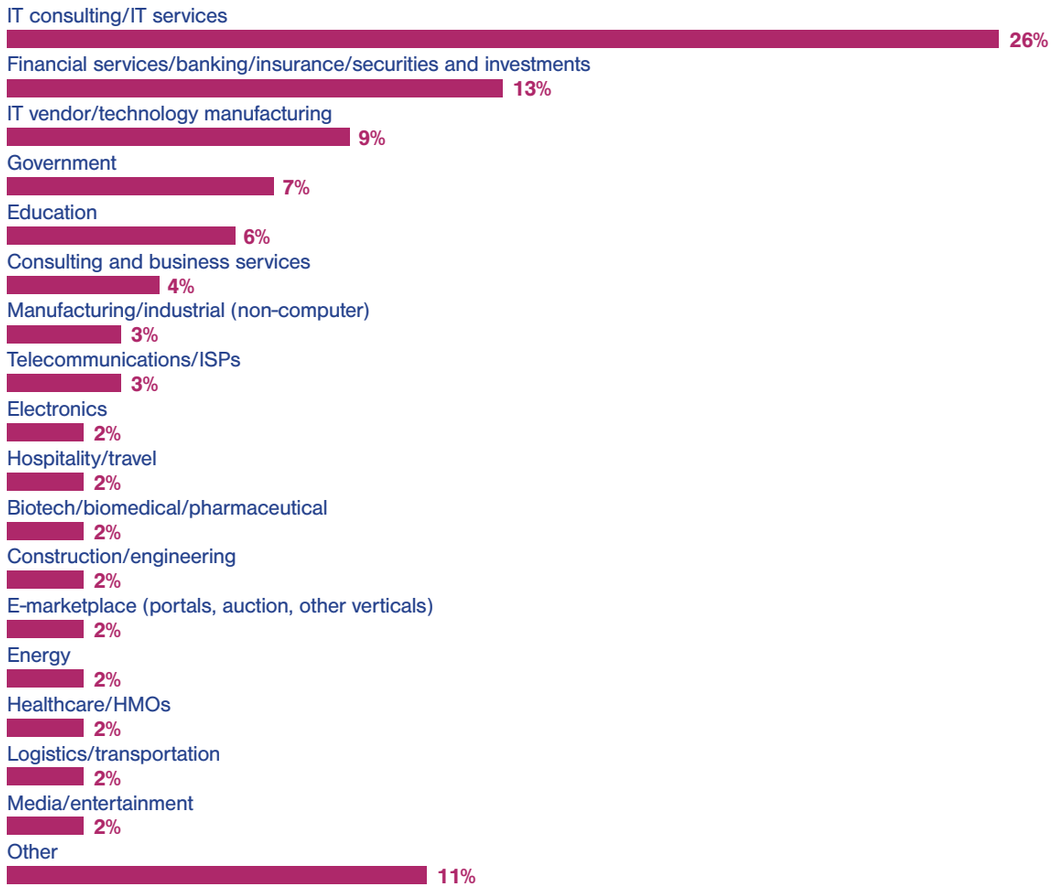

Respondent Company Size
How many employees are in your company in total?
22%
18%
12%
27%
21%
10,000 or more
2,500 to 9,999
1,000 to 2,499
100 to 999
Fewer than 100
Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 23

Respondent Industry

What is your organization's primary industry?



Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 24

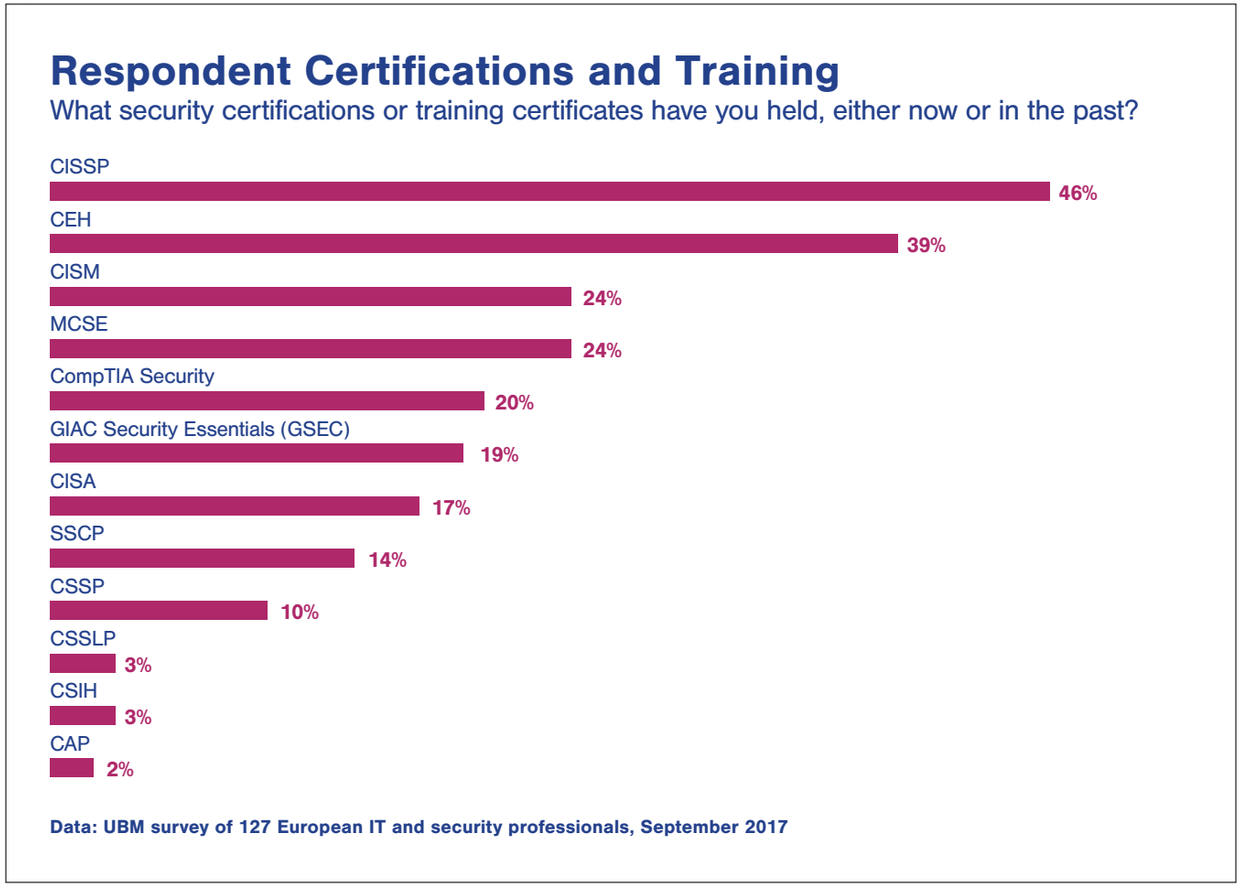
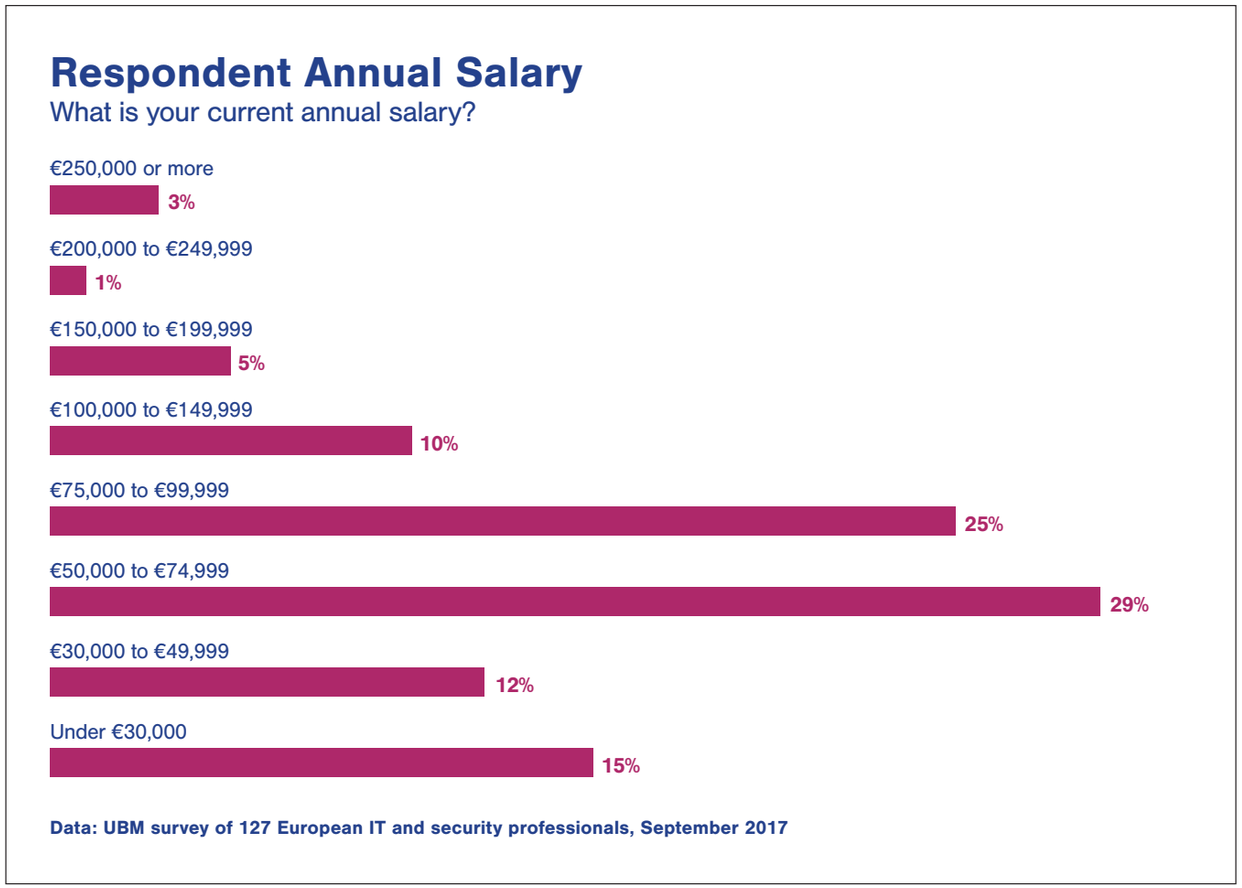

Respondent Certifications and Training
What security certifications or training certificates have you held, either now or in the past?
CISSP
46%
CEH
39%
CISM
24%
MCSE
24%
CompTIA Security
20%
GIAC Security Essentials (GSEC)
19%
CISA
17%
SSCP
14%
CSSP
10%
CSSLP
3%
CSIH
3%
CAP
2%
Data: UBM survey of 127 European IT and security professionals, September 2017

Figure 25


Respondent Annual Salary
What is your current annual salary?
€250,000 or more
3%
€200,000 to €249,999
1%
€150,000 to €199,999
5%
€100,000 to €149,999
10%
€75,000 to €99,999
25%
€50,000 to €74,999
29%
€30,000 to €49,999
12%
Under €30,000
15%
Data: UBM survey of 127 European IT and security professionals, September 2017