The 2018 Black Hat Europe Attendee Survey

Europe's Cybersecurity Challenges

The struggle to implement GDPR and privacy regulations, concerns about corporate data leaks, and fears of a major critical infrastructure breach are keeping European IT security pros awake at night. Here's why.

TABLE OF CONTENTS

Figures

EXECUTIVE SUMMARY

Concerns about GDPR and individual privacy rights, risky user behavior, and threats to critical infrastructure are top of mind among information security professionals in Europe this year.

These are some of the key takeaways from this year's Black Hat Europe Attendee Survey, conducted in September 2018 among 132 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.

As with Black Hat's 2017 survey, about two-thirds (65%) of security professionals believe Europe is at risk of a major critical infrastructure breach affecting multiple nations within the next two years.

When it comes to specific attack vectors, security pros are most concerned about advanced and targeted attacks against their specific organizations. Survey participants are worried about skilled attackers who know just enough about their organization to conduct highly effective spearphishing and social engineering attacks. They also are concerned about end users who break policy or are ignorant of security risks. And most enterprises' defenses remain flawed; many respondents are worried about the difficulty of integrating tools to develop a cohesive security architecture.

As if these issues aren't enough, most respondents are struggling with growing regulatory pressure, particularly in the area of online privacy. This year's enactment of the Europe Union's General Data Protection Regulation (GDPR) has consumed significant time and resources among cybersecurity teams. Behind fighting phishing and social engineering, the second most time-consuming task in respondents' day-to-day work lives is compliance. Despite that, only about a third of organizations are very confident they are fully compliant with GDPR.

In Europe, as in other parts of the world, the security staffing shortage is creating significant challenges for IT organizations. In fact, the majority of respondents don't have the staff or budget they need to respond to the cyber threats they expect to face in the coming year.

The 2018 Black Hat Europe Attendee Survey provided a wide range of insights into the attitudes and concerns of cybersecurity leaders in the region, including:

- 65% of respondents believe a successful cyberattack on the critical infrastructure of multiple EU nations will occur in the next two years.
- Sophisticated and targeted attacks are the No. 1 cybersecurity concern for 52% of respondents.
- 42% of European security pros believe that the weakest link in their defenses are end users who violate security policy and are too easily fooled by social engineering attacks.
- Only a third of respondents are confident in their organization's state of GDPR compliance.
- Multifactor authentication and encryption were ranked as the top two most effective technologies.
- 20% of security professionals believe the security skills shortage is the main reason why enterprise security initiatives fail.

SYNOPSIS

RESEARCH

Survey Name The 2018 Black Hat Europe Attendee Survey

Survey Date September 2018

Region Europe

Number of Respondents 132 European IT and security professionals. The greatest possible margin of error for the total respondent base (N=132) is +/- 8.6 percentage points. UBM, Black Hat's parent company, 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 2018, 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 132 management and staff security professionals, predominantly at large companies, with 53% working at companies with 1,000 or more employees. Forty-seven percent of the respondents hold the CISSP security professional credential; 42% 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 Security Leaders Raise Concerns Over Targeted Cyberattacks

European security and IT professionals increasingly believe that the risks of targeted and sophisticated attacks are on the rise, particularly from nation-state actors.

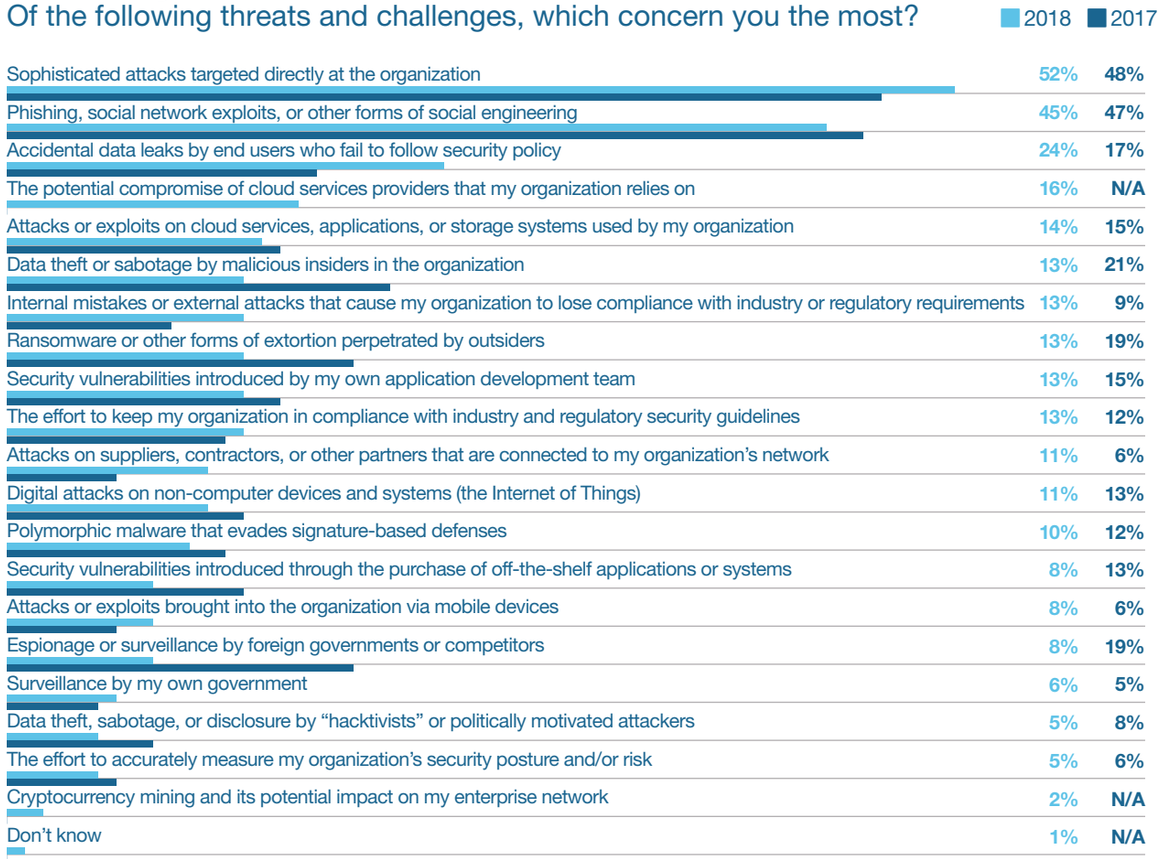
In this year's study, the No. 1 concern registered by cybersecurity professionals in the region was sophisticated attacks aimed directly at the organization. Approximately 52% of professionals voiced this as a top concern, which represented a four-point increase over last year's figures (**Figure 1**). And in open-ended responses, many respondents named advanced persistent threats, targeted attacks, and sophisticated social engineering of key employees as the top problems that keep them up at night.

Indeed, the sophisticated and knowledgeable attacker is the most feared among European cyber pros. The greatest fear is the attacker with inside knowledge of the organization, named by 43% of those surveyed (**Figure 2**). In second and third place came attackers with knowledge of zero-day

Figure 1

Security Professionals' Greatest Concerns

Of the following threats and challenges, which concern you the most?



Note: Maximum of three responses allowed
Base: 132 respondents in 2018 and 127 respondents in 2017
Data: UBM survey of European IT and security professionals, September 2018

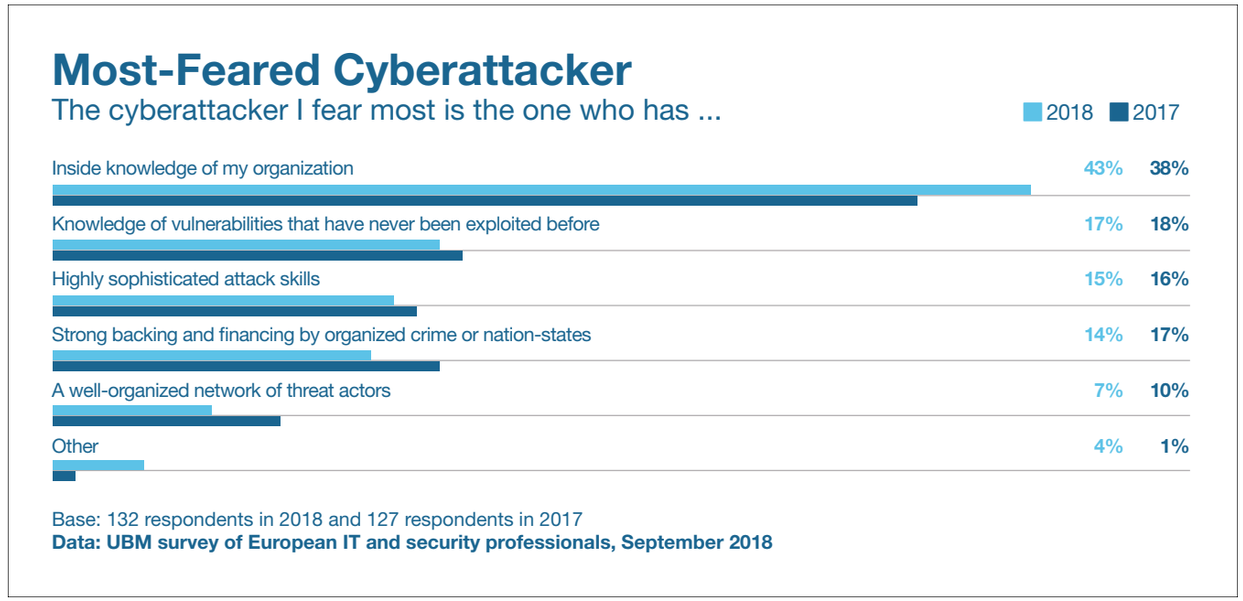
vulnerabilities (17%) and those with highly sophisticated attack skills (15%).

One of the greatest concerns among European security professionals is that these sophisticated, targeted attacks may extend to critical infrastructure. Approximately 65% of those surveyed said that they believe a successful cyberattack on critical infrastructure affecting multiple European Union nations will occur in the next two years (**Figure 3**).

"Vital infrastructure is way behind on the cyberthreats," said one respondent in an open-ended response to a survey question. "[Attackers] are often still hiding behind obfuscation techniques instead of [infrastructure] actually being secure."

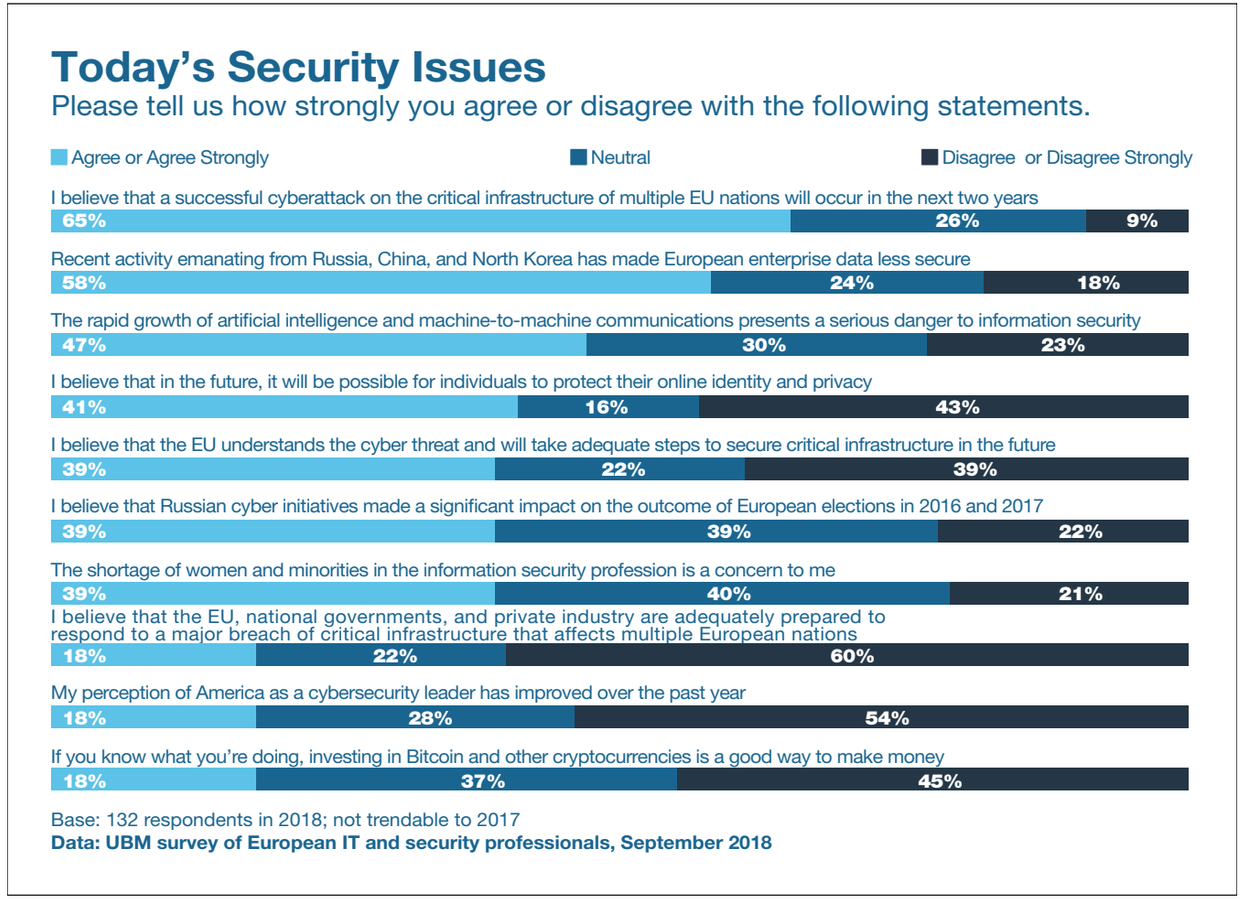
This level of concern, which has changed very little since the 2017 Black Hat Europe Attendee Survey, mirrors similar concerns voiced by North American security pros in the 2018 Black Hat USA Attendee survey, in which 69% of respondents said they believe US critical infrastructure will suffer a breach in the next two years. And in each case, security pros are doubtful that their regional governments are prepared to respond to such a breach. Only 15% of US respondents believe US government and private sector entities are ready for imminent critical infrastructure attacks; 18% of EU respondents believe their regional governments are sufficiently prepared. These responses are significant: They suggest that the overwhelming majority of cybersecurity professionals and leaders — the people who are most likely to understand the threat — lack confidence in their regional governments' ability to protect critical infrastructure.

Figure 2



According to a plurality of those surveyed (30%), the top threat to critical infrastructure is posed by large nation-states, such as Russia and China (**Figure 4**). And their concern extends to their own environments; more than half of survey participants believe recent activity from Russia, China, and North Korea has made European enterprise data less secure. Approximately 14% of respondents said that their most feared cyberattackers have

Figure 3



strong backing and financing by nation-states or organized crime organizations. Organized crime tied for the No. 2 threat to critical infrastructure, named by 17% of those surveyed. Another 17% cited concerns about the worldwide shortage of skilled security personnel, which they feel may affect the safety of critical infrastructure.

Will the situation improve? A majority of European security pros are doubtful, but there is some optimism: About 39% of respondents said that they believe that the EU understands the cyber threat and will take adequate steps to secure critical infrastructure in the future.

Given their assessment of the current attack surface — and fears of vulnerability to targeted exploits — it is not surprising that many security pros cited cyber warfare as a chief concern in their open-ended responses.

"We have reached the point where it is possible to cause mass destruction by cyber-attack," one respondent wrote. "This is a very worrying thing, as certain individual actors may cause large amounts of damage."

End Users: The Weakest Link

One of the reasons why European cybersecurity professionals lack confidence in their defenses is that online attackers continue to exploit what they believe to be enterprise security's weakest link: the end user.

"The weak part of the chain always will be the user," one survey respondent wrote. No

enterprise can ensure that 100% of users will be able to avoid some kind of critical cybersecurity mistake, he said.

That point of view was common among survey respondents. When asked which is the weakest link in IT security, 42% of survey participants cited end users who violate security policy and are too easily fooled by social engineering attacks (**Figure 5**). This figure increased 12 points over last year's survey and was cited more than twice as often as the second-weakest link: the lack of security planning that leads to a "firefighting" mentality.

The threat of phishing and social engineering is not only a top concern for European security professionals but also a chief time-consumer. According nearly one-third of survey respondents, the most time-consuming activity in today's cybersecurity department is fighting phishing, social network exploits, or other forms of social engineering. This response rated higher than compliance activities, risk measurement, and managing application vulnerabilities.

Some forms of phishing are of greater concern than others. For example, some respondents said that they are most concerned about attackers who are able to craft convincing spearphishing messages by gaining knowledge about their specific organizations.

One respondent said his biggest fear is "spearphishing attacks from 'potential clients' or adversaries pretending to be current business contacts or clients, where the adversary has enough information and skill to pretend they're a current business contact or client." This tactic is usually good enough to trick users into helping the bad guys exfiltrate data — or fool them into opening malware-infected documents that exploit zero-day vulnerabilities.

While end user-related vulnerabilities dominated the survey, there is growing sentiment

Figure 4

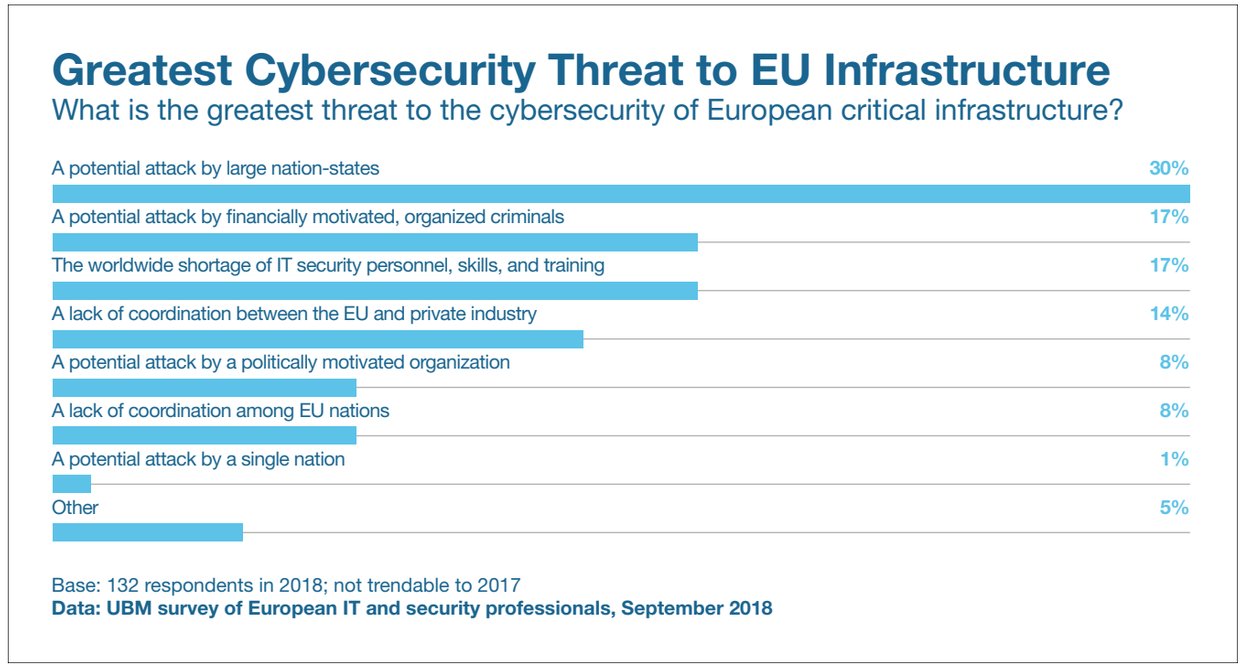
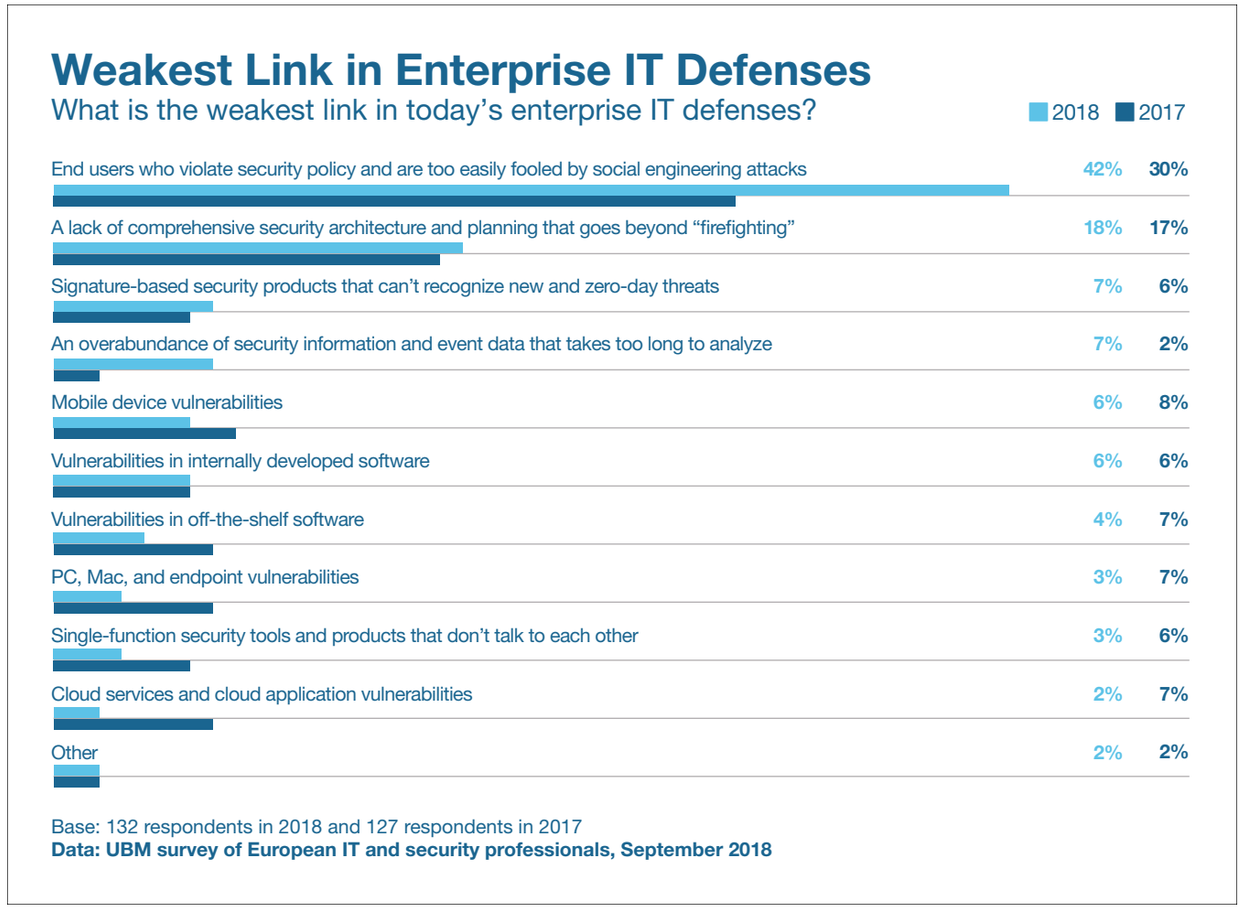


Figure 5



in Europe that IT security teams should spend more time developing a comprehensive strategy for defense and less time firefighting against the latest attack. This sentiment was reflected in many of the responses to open-ended questions about the chief challenges in enterprise security.

"There's too much focus on technological solutions and experts, not enough focus on getting organizations and individuals to adopt secure processes and behaviors," commented one respondent. "Prevention is better than detection and cure."

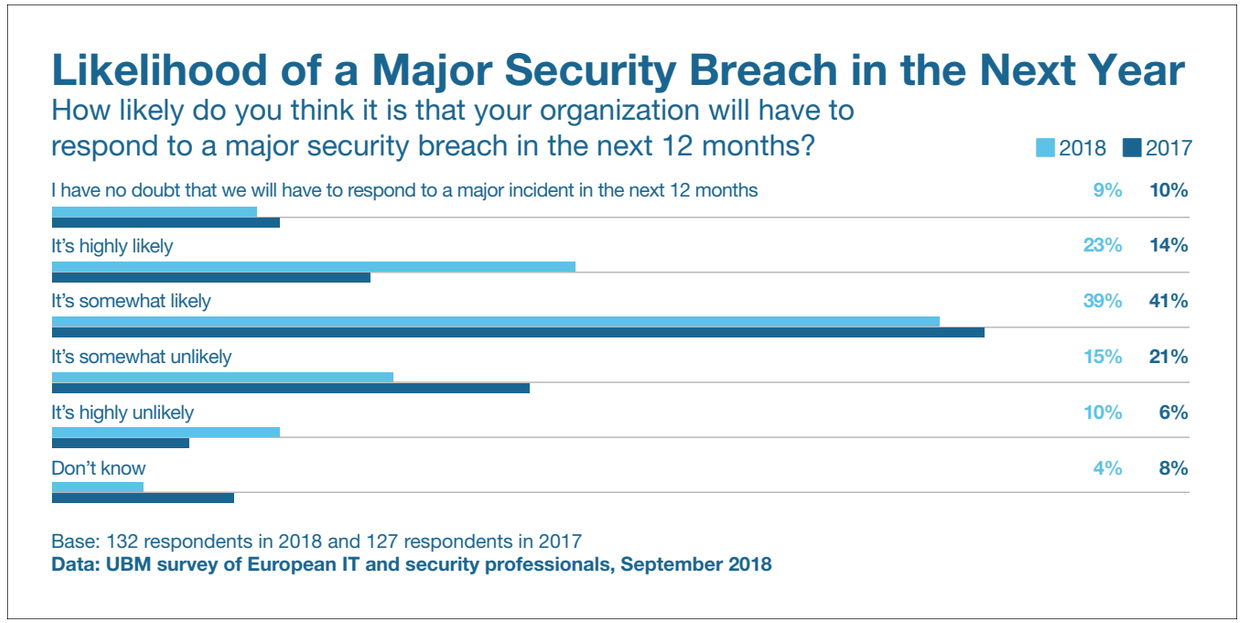
Enterprises need to build a stronger culture of security, respondents said. "Business is segmented, [which] leads to a mindset that security is the responsibility of someone else — and the security controls put in place to provide security are obstacles to be avoided rather than embraced," one respondent commented.

These fears and concerns result in a base of European security professionals who expect to face a major security breach in their organizations in the coming year. Only about a quarter of respondents think it unlikely that their organization will have to respond to a major breach in the next 12 months (**Figure 6**).

GDPR and Privacy: Adding to the Security Challenge

While respondents to the 2018 Black Hat Europe Attendee Survey registered high

Figure 6



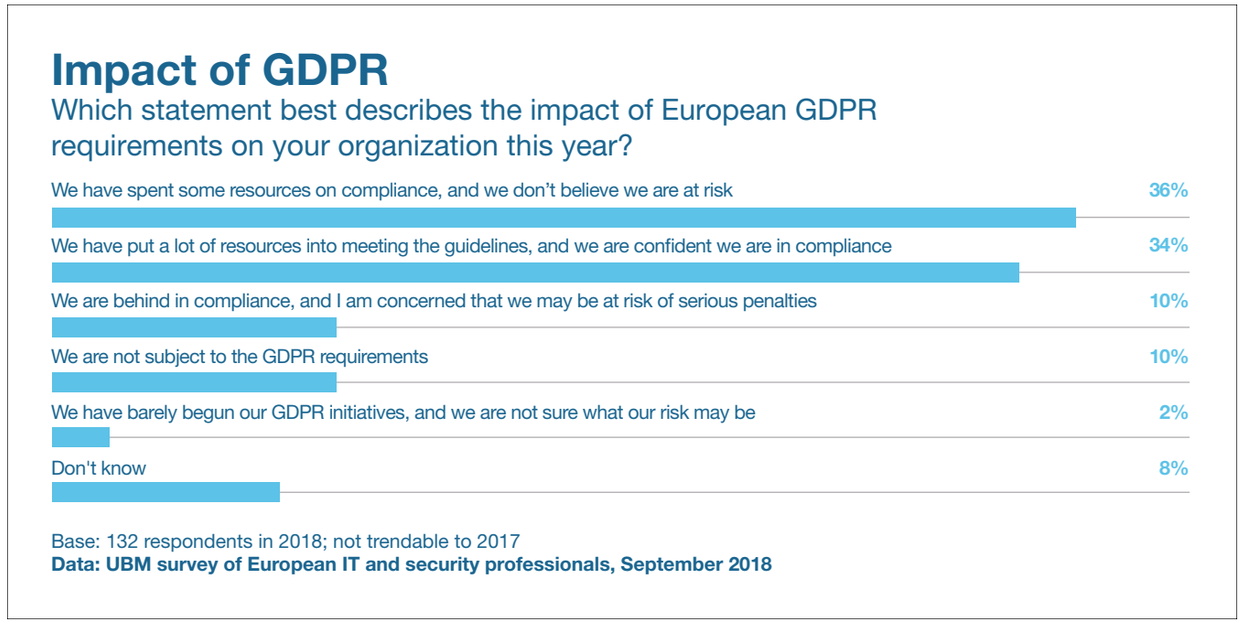
concern over online attacks and exploits, they are also increasingly concerned about privacy — particularly the implementation of the General Data Protection Regulation (GDPR). The EU officially commenced enforcement of GDPR in May, and European respondents to this year's survey report that GDPR compliance is at the top of their minds.

A solid 70% of those surveyed said their organizations have dedicated resources to GDPR initiatives. Yet only slightly more than a third say they're confident in their organization's state of GDPR compliance (**Figure 7**). Interestingly, while 85% of those surveyed think that GDPR will help at least a little bit to positively affect the protection of individuals' privacy, fewer than one in four think that impact will be substantial (**Figure 8**).

These responses highlight a growing skepticism among European security professionals with regard to the ability to protect user privacy. When asked about the greatest threats to privacy, respondents cited the collection and/or sale of personal information by enterprises and social media organizations that don't properly protect privacy, each of which was cited by 58% of respondents (**Figure 9**). In fact, commercial data collection of personal information and social media were cited by even more security pros than end user ignorance or even cyberattackers who target personal information. Only a minority of these security leaders say they believe that it will ever be possible for individuals to protect their online identity and privacy.

From a practical perspective, the privacy issue was manifested earlier this year in headlines about social networking giant Facebook, which stood accused of oversharing personal information with data brokers. Recently, Facebook also discovered a data compromise that may have affected as many as 50 million users. In light of these revelations, it's understandable that 70% of European security pros said they are advising internal users and customers to rethink the data they're sharing on social networks, and that 46% are pushing for addi-

Figure 7



tional security controls around social media access to corporate social media accounts (**Figure 10**).

Security Skills and Resources Still Running Short

With so many factors at play — including sophisticated attacks, careless users, and privacy concerns — many security practitioners are feeling overwhelmed and ready to call for help. Unfortunately, there isn't much help to be had: Many European security pros say they are contending with a detrimentally constrained pool of human resources.

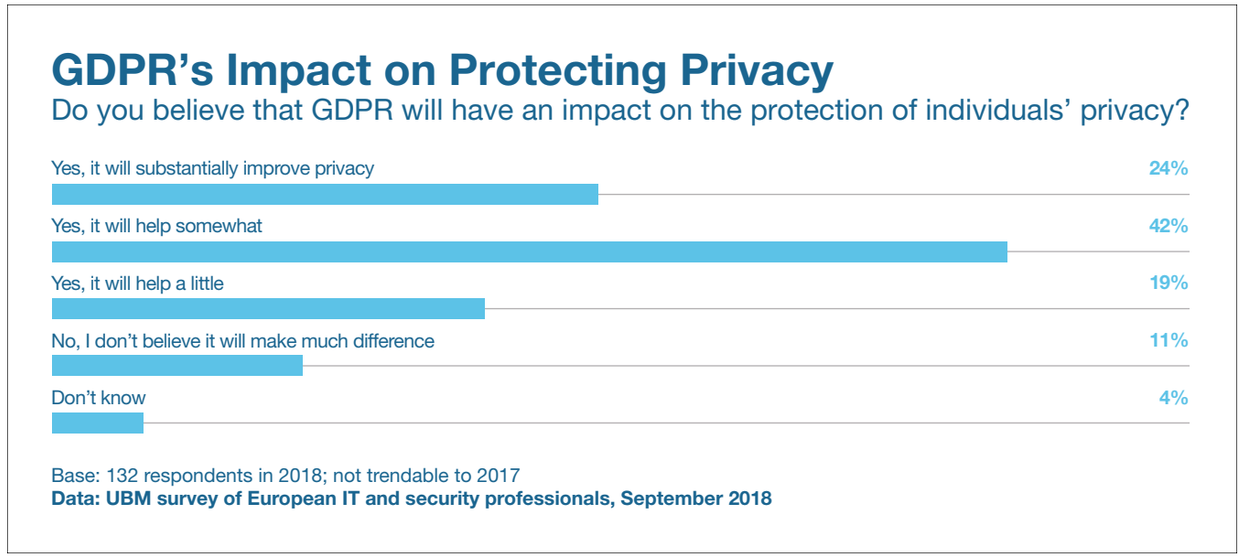
Our survey found that fewer than half of respondents report that they have enough security budget to help them defend against today's threats (**Figure 11**). Similarly, just under half of organizations report having enough staff to defend against current threats (**Figure 12**). The numbers indicate that the hiring situation has improved slightly over the past year, but the open-ended answers offered some sobering comments about the security skills shortage.

"No company is staffed appropriately for security," one respondent said. "In my group, we have one security practitioner for each 107 software developers. That's an impossible ratio. Imagine 107 people creating dirty rooms and one person responsible for cleaning each room — mission impossible. We need education, tooling, [and] technology to begin influencing software engineers to write more secure code."

Many security experts believe the skills shortage is contributing to the growing frequency of data breaches. In fact, one in five respondents said that the security skills shortage was the No. 1 reason why enterprise security initiatives fail (**Figure 13**). However, some respondents used the open-ended questions to suggest changes in recruiting strategy.

"When recruiting, we aren't taking every résumé seriously, and actually sitting down with most of the people," one respondent

Figure 8



wrote. "Most people don't necessarily have the qualifications to work in the industry but do already possess the skill set to work in a cyber environment."

What's Working — and What's Not

From a technology perspective, European security professionals are moving away from traditional wisdom about perimeter defense and moving on to other strategies such as identity-based security. When asked about the most effective security tools, firewalls and antivirus defenses are being supplanted at the top of the list by other technologies.

This year, the most highly rated technology was multifactor authentication, which was rated as effective by 88% of respondents (**Figure 14**). This was closely followed by encryption in the No. 2 spot (87%). Firewalls were No. 3, with a 75% effectiveness rating, indicating that they still occupy an important spot in the pantheon of security tools. Antivirus, on the other hand, came in 10th place behind other technologies such as security information and event management, threat intelligence, and application security tools. Passwords were scored as the least effective security technology, rated by only about 41% of respondents as an effective security tool.

Our survey respondents also are concerned that security technologies are difficult to integrate. For the first time this year, the No. 1 answer for why current enterprise IT security strategies and technologies fail is a lack of integration in security architectures, with too many point products in place.

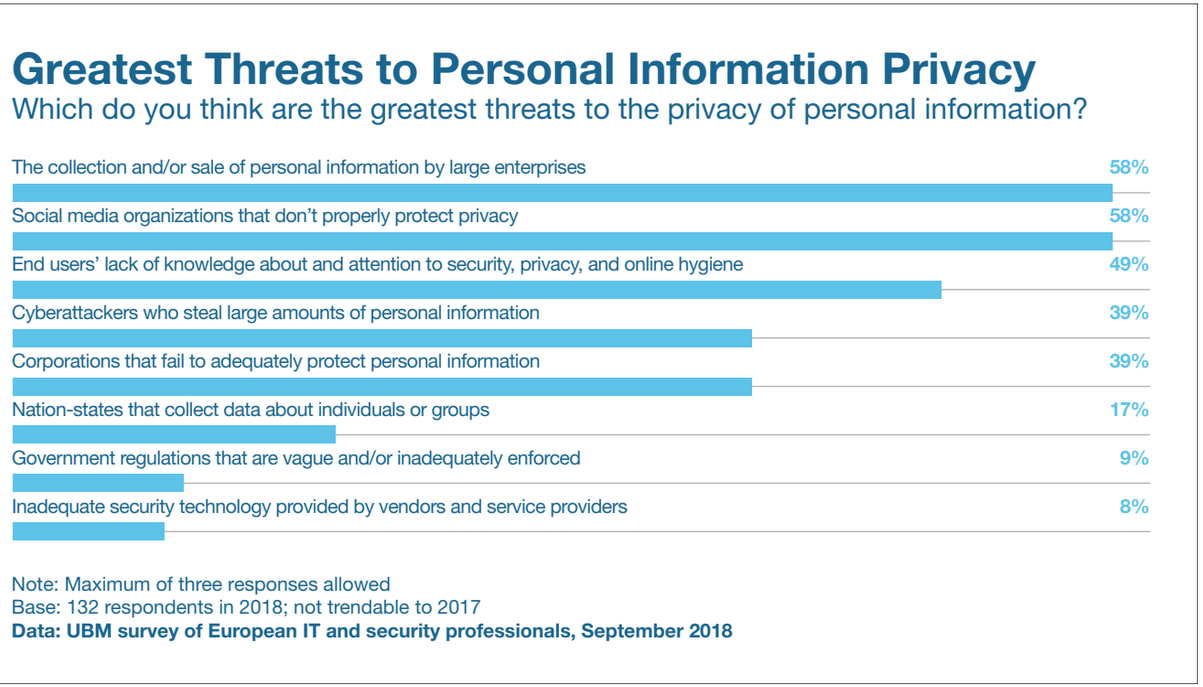
Conclusion

One response to an open-ended question shows European security professionals' current state of mind about the state of IT security — both in the enterprise and in the broader industry.

"We've built on sand, and continue to build on it by sticking plasters on things," the respondent said. "And vendor behavior is now worse than I have even seen. Short support cycles, product support being dumped, the real world ignored for the shiny new."

In many ways, the survey indicates that European security professionals recognize an industry need to get back to basics — both with technology and with practices. This means doing as much as possible to eliminate complexity from security architectures, while doubling-down on high-value activities that can address the root cause of problems such as targeted attacks and phishing. Clearly, these steps can't be taken without better funding and an effort to recruit, train, and retain quality security teams.

Figure 9



APPENDIX

Figure 10

Figure 11

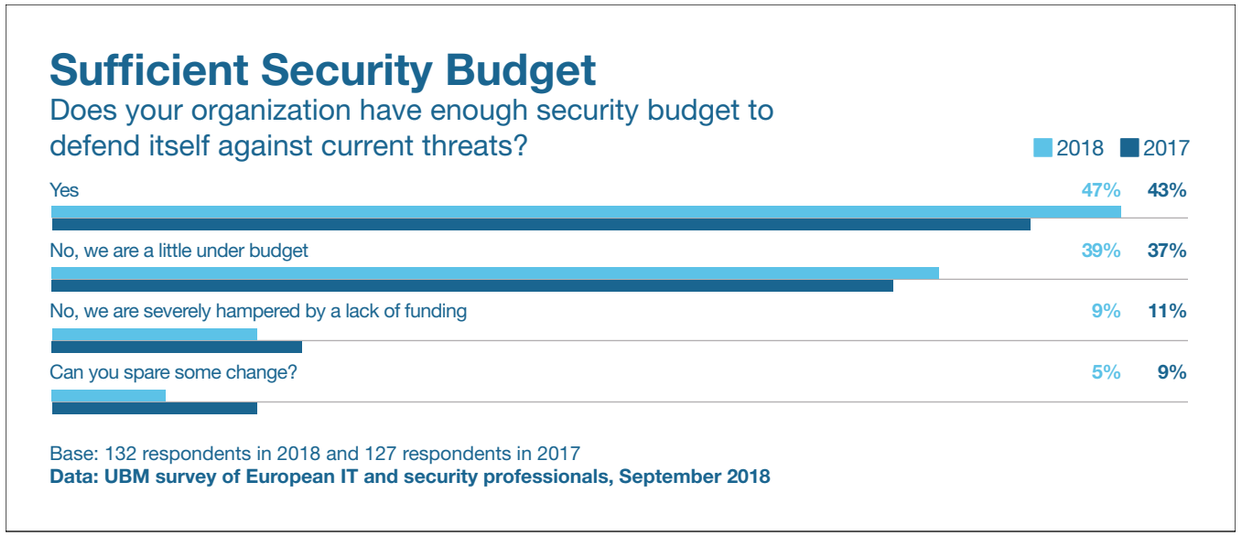

Sufficient Security Budget
Does your organization have enough security budget to defend itself against current threats?
2018
2017
Yes
47%
43%
No, we are a little under budget
39%
37%
No, we are severely hampered by a lack of funding
9%
11%
Can you spare some change?
5%
9%
Base: 132 respondents in 2018 and 127 respondents in 2017
Data: UBM survey of European IT and security professionals, September 2018

Figure 12

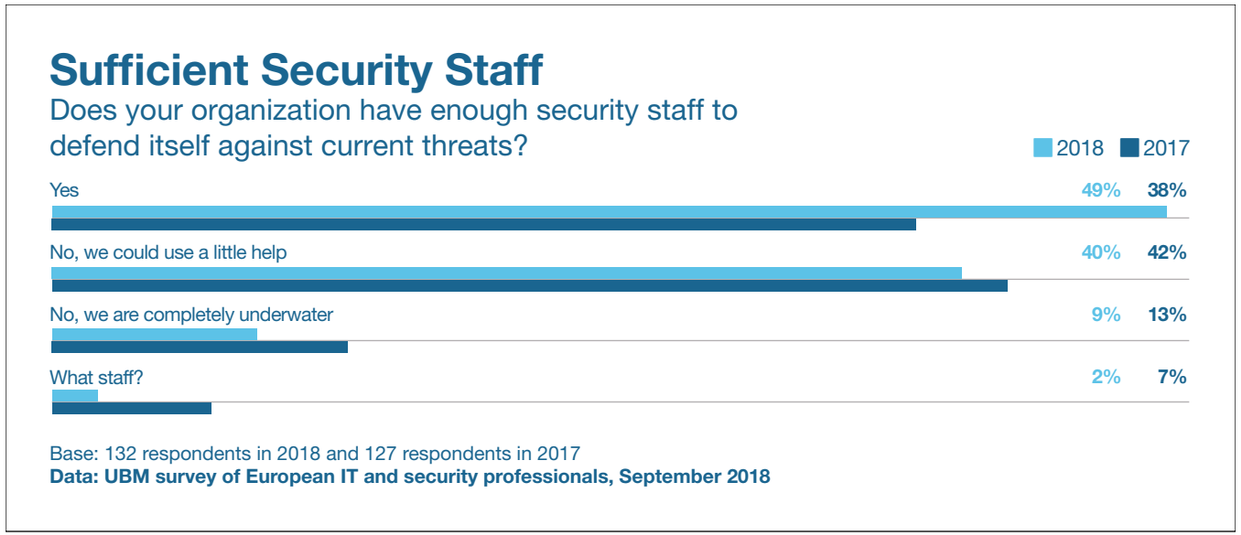

Sufficient Security Staff
Does your organization have enough security staff to defend itself against current threats?
2018
2017
Yes
49%
38%
No, we could use a little help
40%
42%
No, we are completely underwater
9%
13%
What staff?
2%
7%
Base: 132 respondents in 2018 and 127 respondents in 2017
Data: UBM survey of European IT and security professionals, September 2018

Figure 13

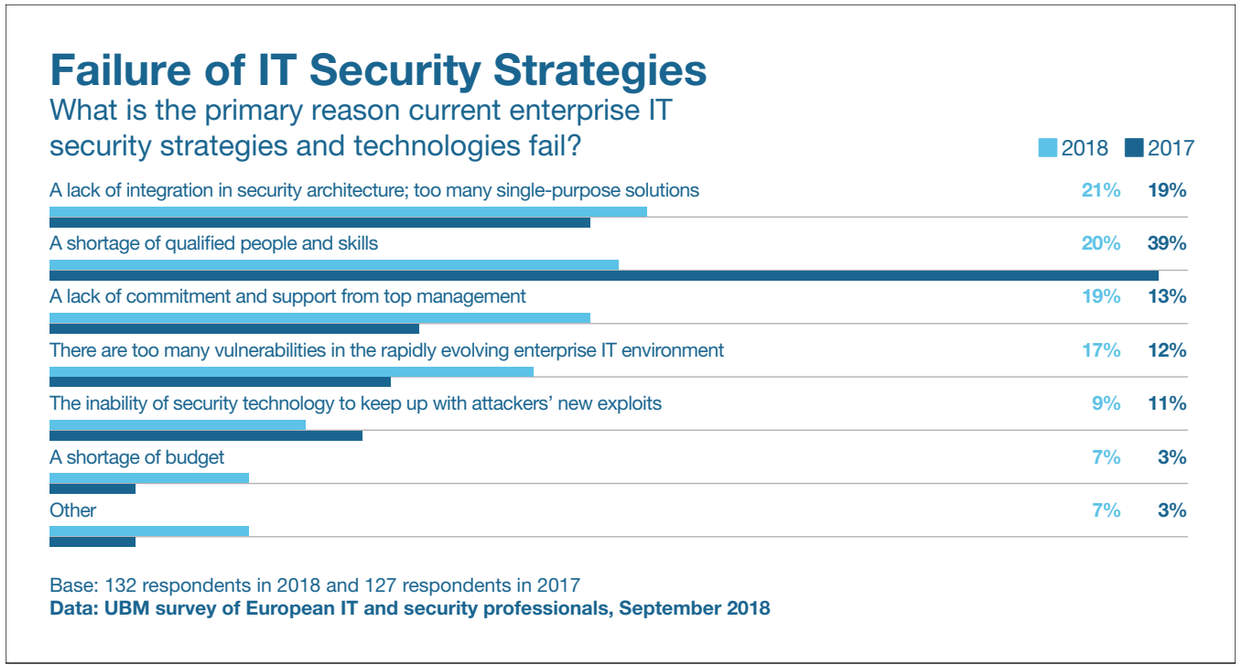

Failure of IT Security Strategies
What is the primary reason current enterprise IT security strategies and technologies fail?
2018
2017
A lack of integration in security architecture; too many single-purpose solutions
21%
19%
A shortage of qualified people and skills
20%
39%
A lack of commitment and support from top management
19%
13%
There are too many vulnerabilities in the rapidly evolving enterprise IT environment
17%
12%
The inability of security technology to keep up with attackers' new exploits
9%
11%
A shortage of budget
7%
3%
Other
7%
3%
Base: 132 respondents in 2018 and 127 respondents in 2017
Data: UBM survey of European IT and security professionals, September 2018

Figure 14

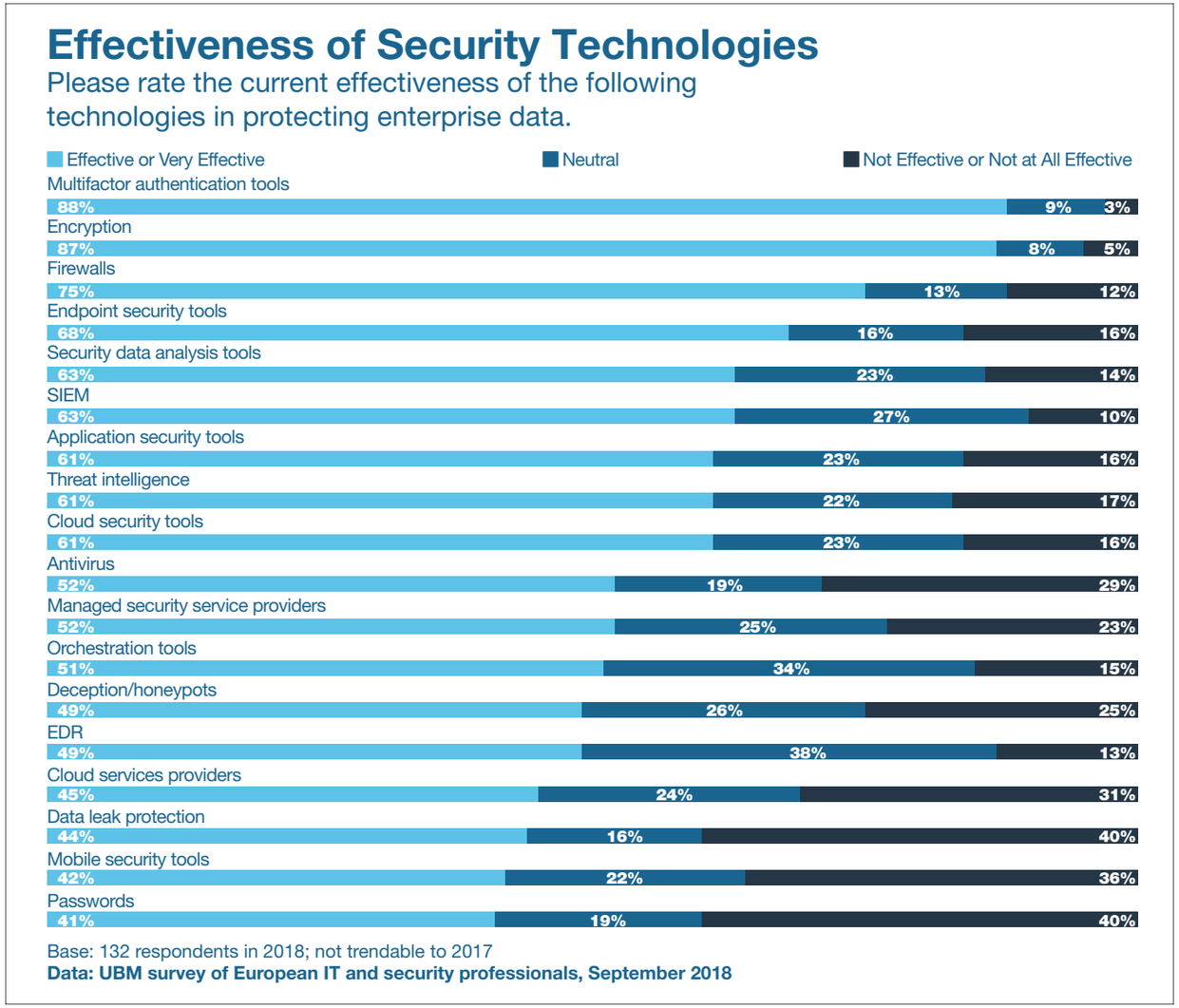

Effectiveness of Security Technologies
Please rate the current effectiveness of the following technologies in protecting enterprise data.
Effective or Very Effective
Neutral
Not Effective or Not at All Effective
Multifactor authentication tools
88%
9%
3%
Encryption
87%
8%
5%
Firewalls
75%
13%
12%
Endpoint security tools
68%
16%
16%
Security data analysis tools
63%
23%
14%
SIEM
63%
27%
10%
Application security tools
61%
23%
16%
Threat intelligence
61%
22%
17%
Cloud security tools
61%
23%
16%
Antivirus
52%
19%
29%
Managed security service providers
52%
25%
23%
Orchestration tools
51%
34%
15%
Deception/honeypots
49%
26%
25%
EDR
49%
38%
13%
Cloud services providers
45%
24%
31%
Data leak protection
44%
16%
40%
Mobile security tools
42%
22%
36%
Passwords
41%
19%
40%
Base: 132 respondents in 2018; not trendable to 2017
Data: UBM survey of European IT and security professionals, September 2018

Figure 15

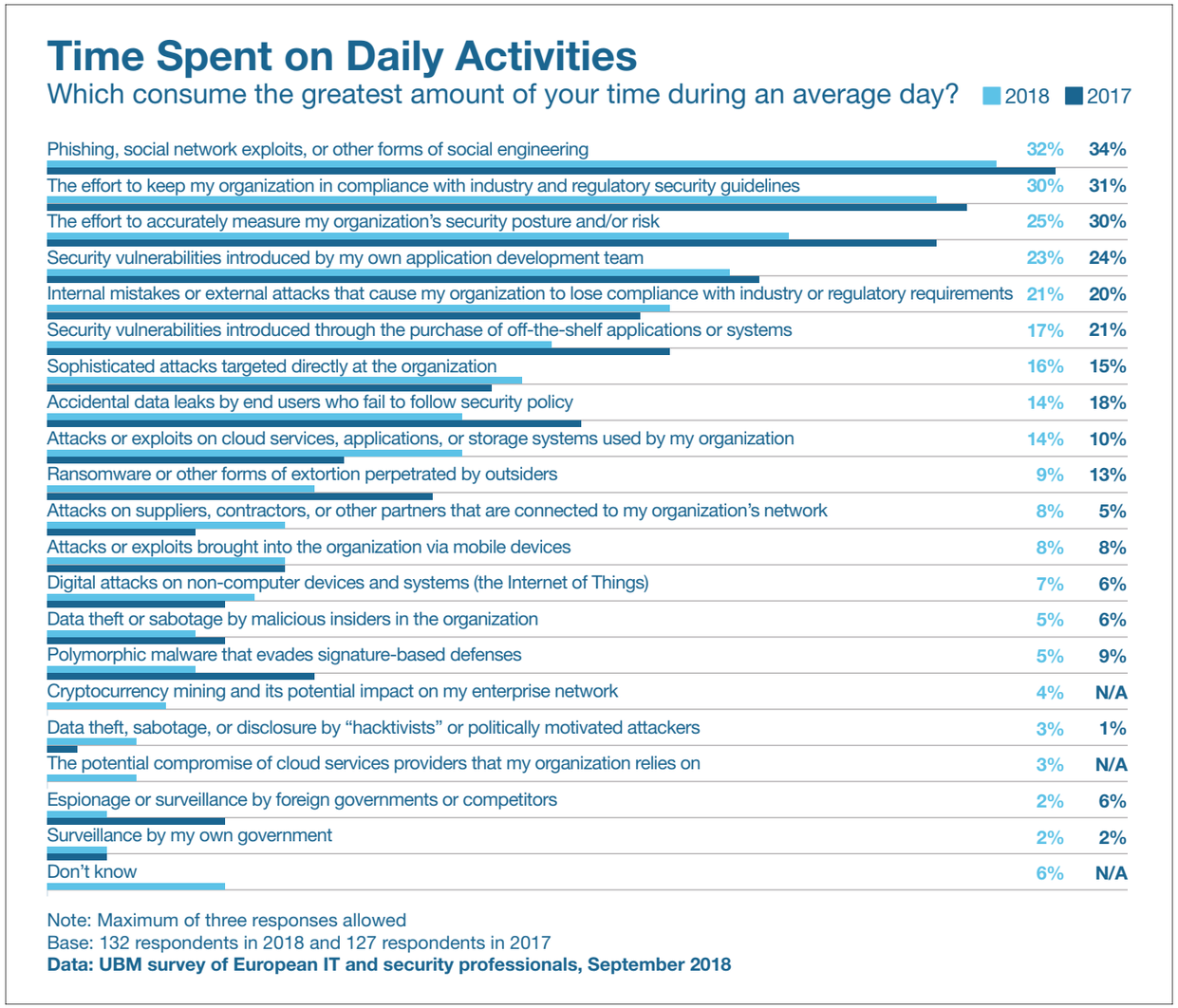

Time Spent on Daily Activities
Which consume the greatest amount of your time during an average day?
2018
2017
Phishing, social network exploits, or other forms of social engineering 32% 34%
The effort to keep my organization in compliance with industry and regulatory security guidelines 30% 31%
The effort to accurately measure my organization's security posture and/or risk 25% 30%
Security vulnerabilities introduced by my own application development team 23% 24%
Internal mistakes or external attacks that cause my organization to lose compliance with industry or regulatory requirements 21% 20%
Security vulnerabilities introduced through the purchase of off-the-shelf applications or systems 17% 21%
Sophisticated attacks targeted directly at the organization 16% 15%
Accidental data leaks by end users who fail to follow security policy 14% 18%
Attacks or exploits on cloud services, applications, or storage systems used by my organization 14% 10%
Ransomware or other forms of extortion perpetrated by outsiders 9% 13%
Attacks on suppliers, contractors, or other partners that are connected to my organization's network 8% 5%
Attacks or exploits brought into the organization via mobile devices 8% 8%
Digital attacks on non-computer devices and systems (the Internet of Things) 7% 6%
Data theft or sabotage by malicious insiders in the organization 5% 6%
Polymorphic malware that evades signature-based defenses 5% 9%
Cryptocurrency mining and its potential impact on my enterprise network 4% N/A
Data theft, sabotage, or disclosure by "hacktivists" or politically motivated attackers 3% 1%
The potential compromise of cloud services providers that my organization relies on 3% N/A
Espionage or surveillance by foreign governments or competitors 2% 6%
Surveillance by my own government 2% 2%
Don't know 6% N/A
Note: Maximum of three responses allowed
Base: 132 respondents in 2018 and 127 respondents in 2017
Data: UBM survey of European IT and security professionals, September 2018

Figure 16

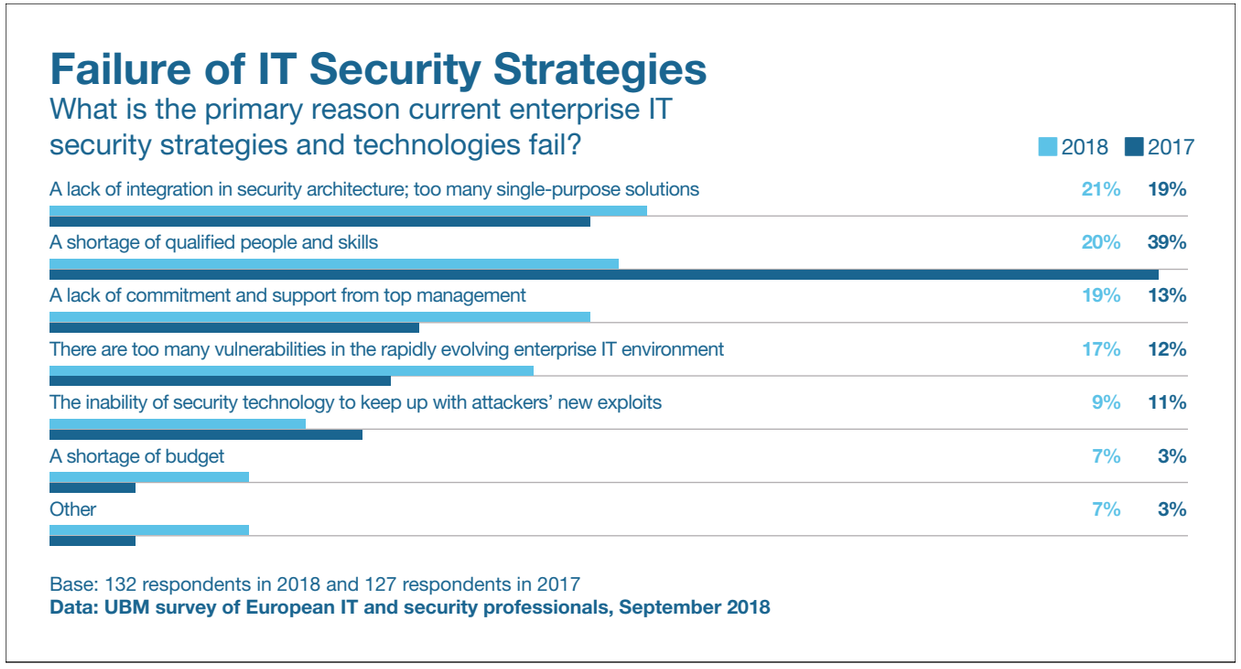

Failure of IT Security Strategies
What is the primary reason current enterprise IT security strategies and technologies fail?
2018
2017
A lack of integration in security architecture; too many single-purpose solutions
21%
19%
A shortage of qualified people and skills
20%
39%
A lack of commitment and support from top management
19%
13%
There are too many vulnerabilities in the rapidly evolving enterprise IT environment
17%
12%
The inability of security technology to keep up with attackers' new exploits
9%
11%
A shortage of budget
7%
3%
Other
7%
3%
Base: 132 respondents in 2018 and 127 respondents in 2017
Data: UBM survey of European IT and security professionals, September 2018

Figure 17

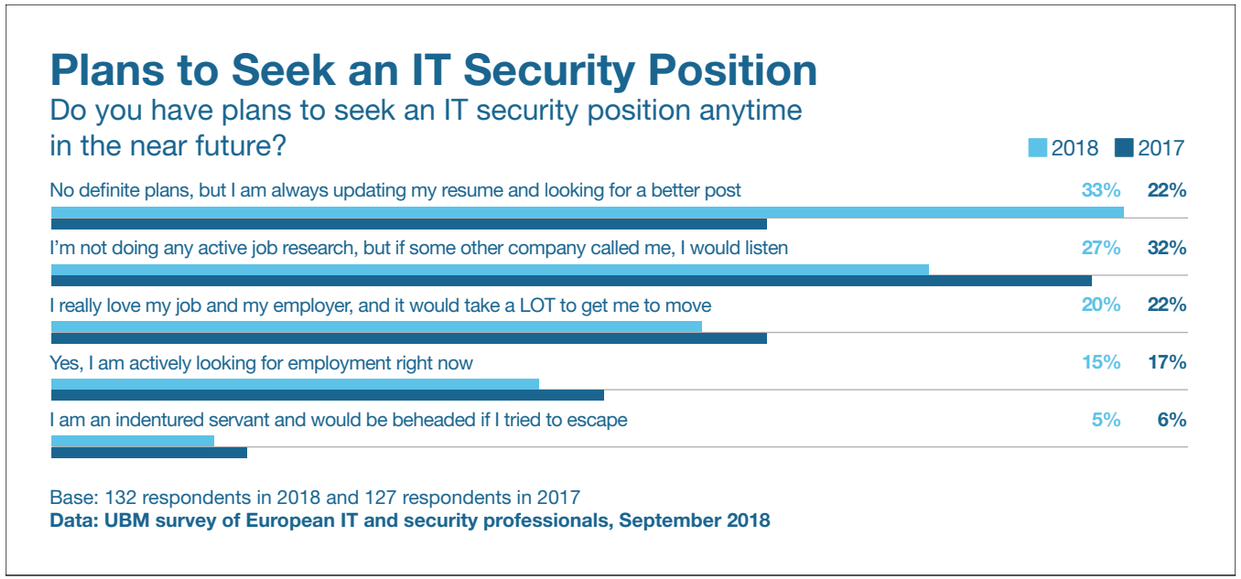

Plans to Seek an IT Security Position
Do you have plans to seek an IT security position anytime in the near future?
2018
2017
No definite plans, but I am always updating my resume and looking for a better post
33%
22%
I'm not doing any active job research, but if some other company called me, I would listen
27%
32%
I really love my job and my employer, and it would take a LOT to get me to move
20%
22%
Yes, I am actively looking for employment right now
15%
17%
I am an indentured servant and would be beheaded if I tried to escape
5%
6%
Base: 132 respondents in 2018 and 127 respondents in 2017
Data: UBM survey of European IT and security professionals, September 2018

Figure 18

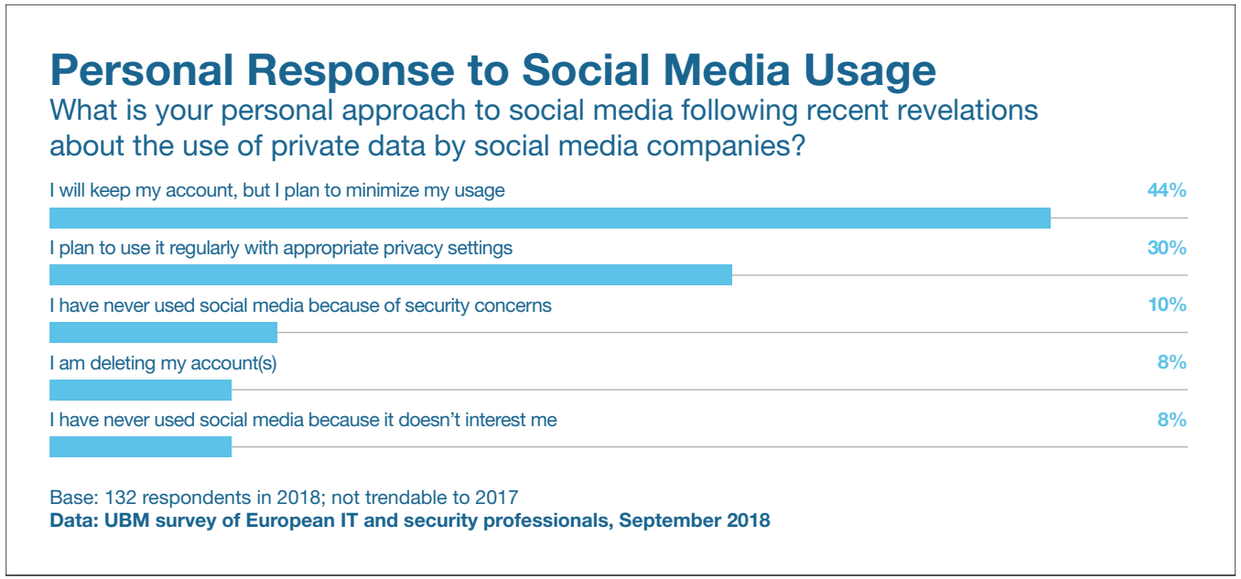

Personal Response to Social Media Usage
What is your personal approach to social media following recent revelations about the use of private data by social media companies?
I will keep my account, but I plan to minimize my usage
44%
I plan to use it regularly with appropriate privacy settings
30%
I have never used social media because of security concerns
10%
I am deleting my account(s)
8%
I have never used social media because it doesn't interest me
8%
Base: 132 respondents in 2018; not trendable to 2017
Data: UBM survey of European IT and security professionals, September 2018

Figure 19

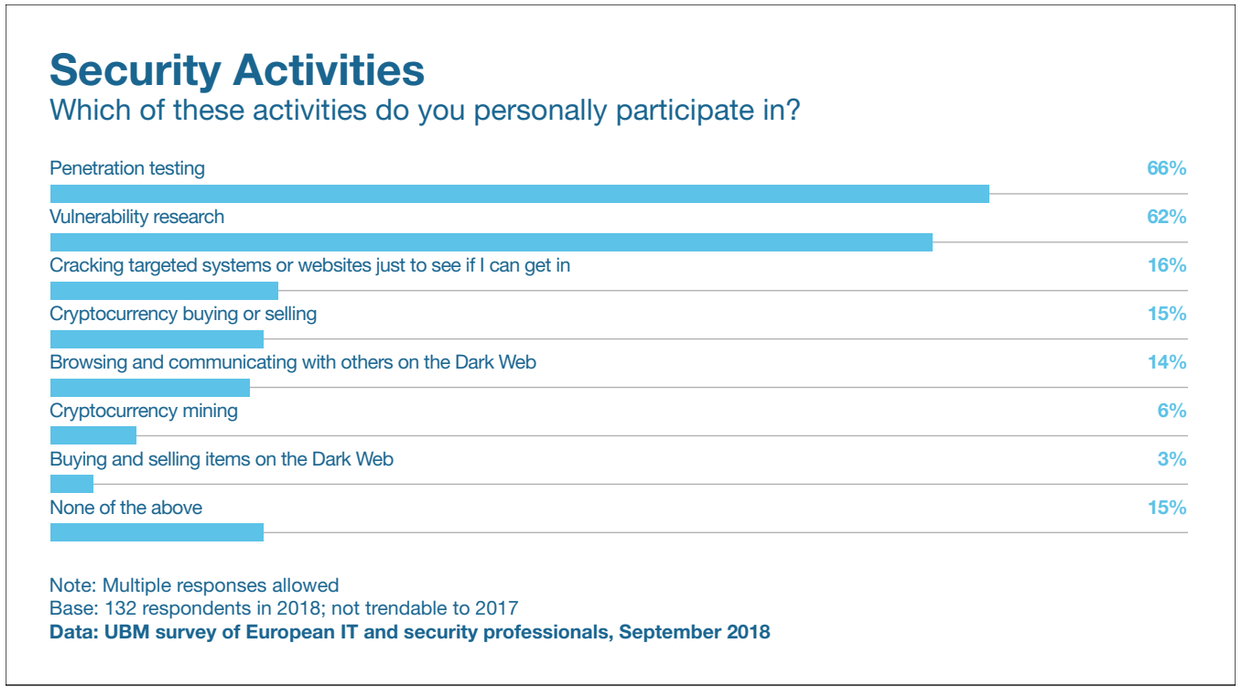

Security Activities
Which of these activities do you personally participate in?
Penetration testing 66%
Vulnerability research 62%
Cracking targeted systems or websites just to see if I can get in 16%
Cryptocurrency buying or selling 15%
Browsing and communicating with others on the Dark Web 14%
Cryptocurrency mining 6%
Buying and selling items on the Dark Web 3%
None of the above 15%
Note: Multiple responses allowed
Base: 132 respondents in 2018; not trendable to 2017
Data: UBM survey of European IT and security professionals, September 2018

Figure 20

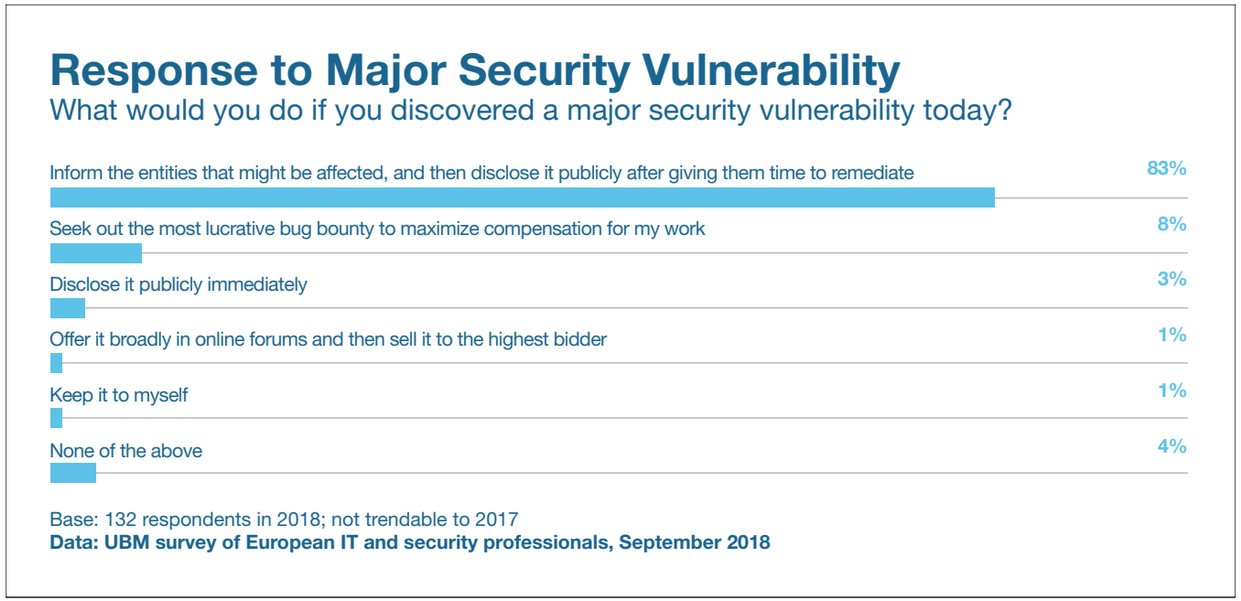

Response to Major Security Vulnerability
What would you do if you discovered a major security vulnerability today?
Inform the entities that might be affected, and then disclose it publicly after giving them time to remediate
83%
Seek out the most lucrative bug bounty to maximize compensation for my work
8%
Disclose it publicly immediately
3%
Offer it broadly in online forums and then sell it to the highest bidder
1%
Keep it to myself
1%
None of the above
4%
Base: 132 respondents in 2018; not trendable to 2017
Data: UBM survey of European IT and security professionals, September 2018

Figure 21

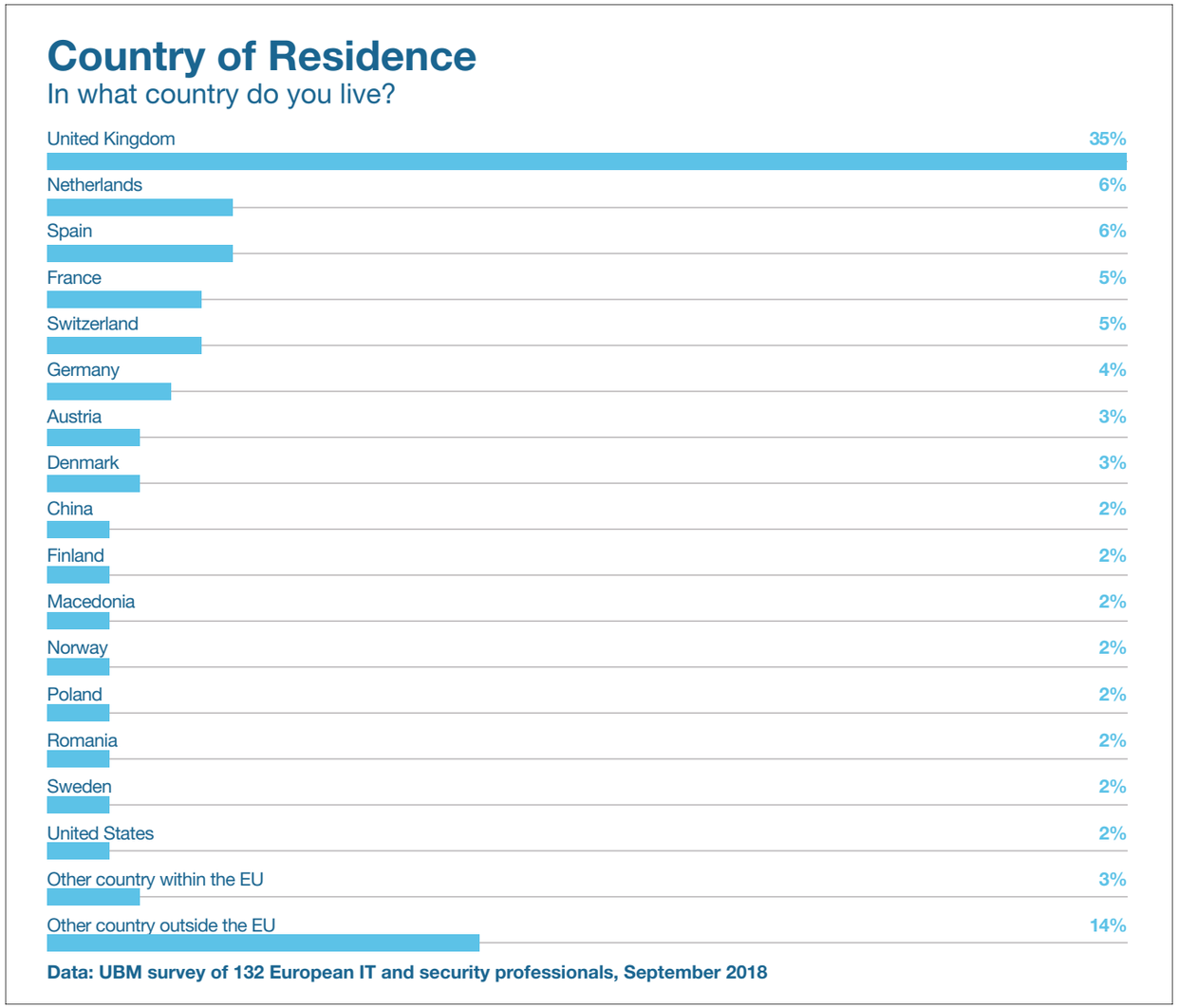

Country of Residence
In what country do you live?
United Kingdom 35%
Netherlands 6%
Spain 6%
France 5%
Switzerland 5%
Germany 4%
Austria 3%
Denmark 3%
China 2%
Finland 2%
Macedonia 2%
Norway 2%
Poland 2%
Romania 2%
Sweden 2%
United States 2%
Other country within the EU 3%
Other country outside the EU 14%
Data: UBM survey of 132 European IT and security professionals, September 2018

Figure 22

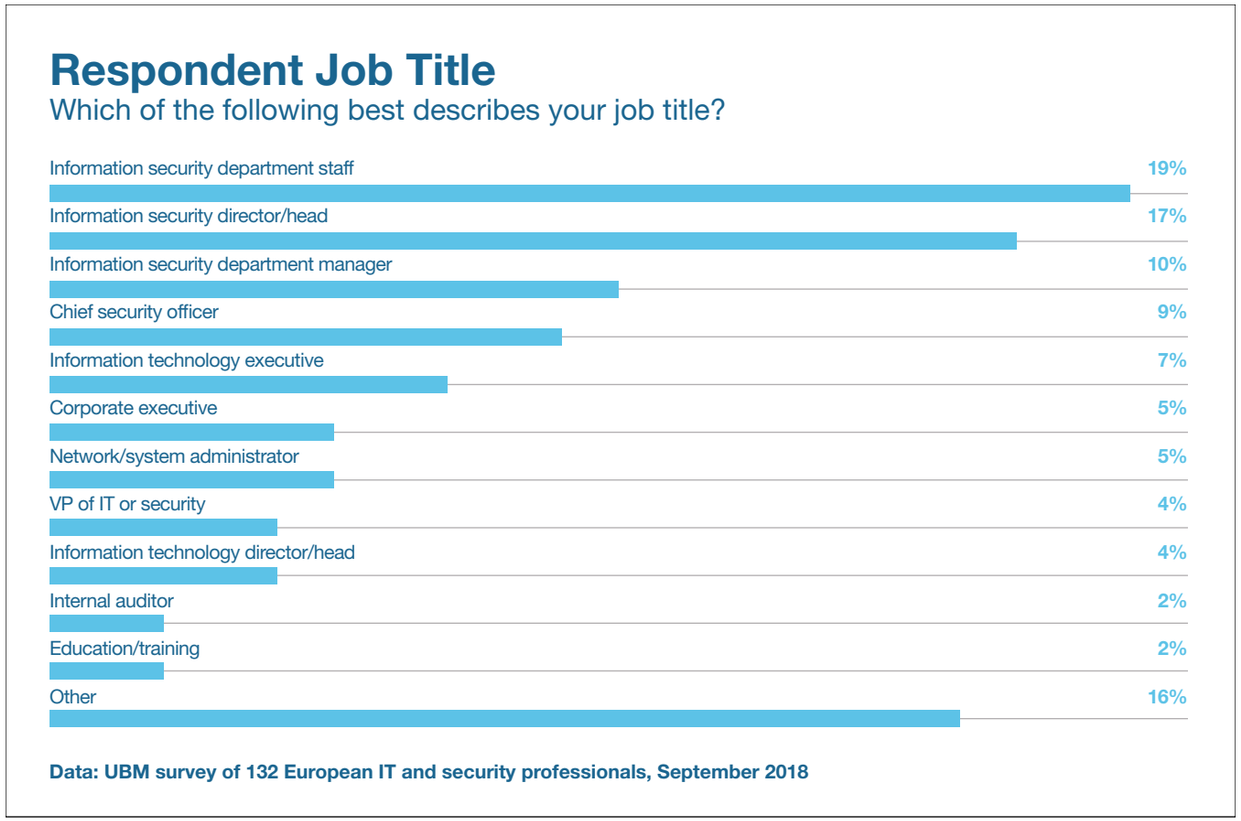

Respondent Job Title
Which of the following best describes your job title?
Information security department staff 19%
Information security director/head 17%
Information security department manager 10%
Chief security officer 9%
Information technology executive 7%
Corporate executive 5%
Network/system administrator 5%
VP of IT or security 4%
Information technology director/head 4%
Internal auditor 2%
Education/training 2%
Other 16%
Data: UBM survey of 132 European IT and security professionals, September 2018

Figure 23

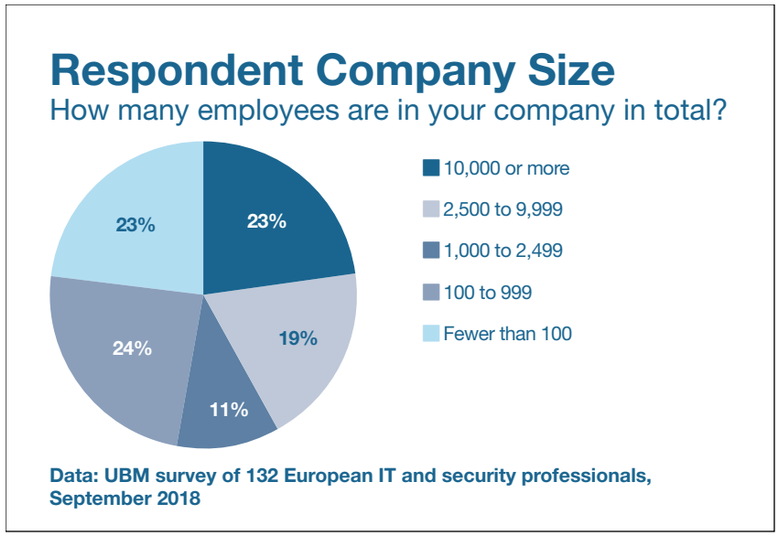

Respondent Company Size
How many employees are in your company in total?
23%
19%
11%
24%
23%
10,000 or more
2,500 to 9,999
1,000 to 2,499
100 to 999
Fewer than 100
Data: UBM survey of 132 European IT and security professionals, September 2018

Figure 24

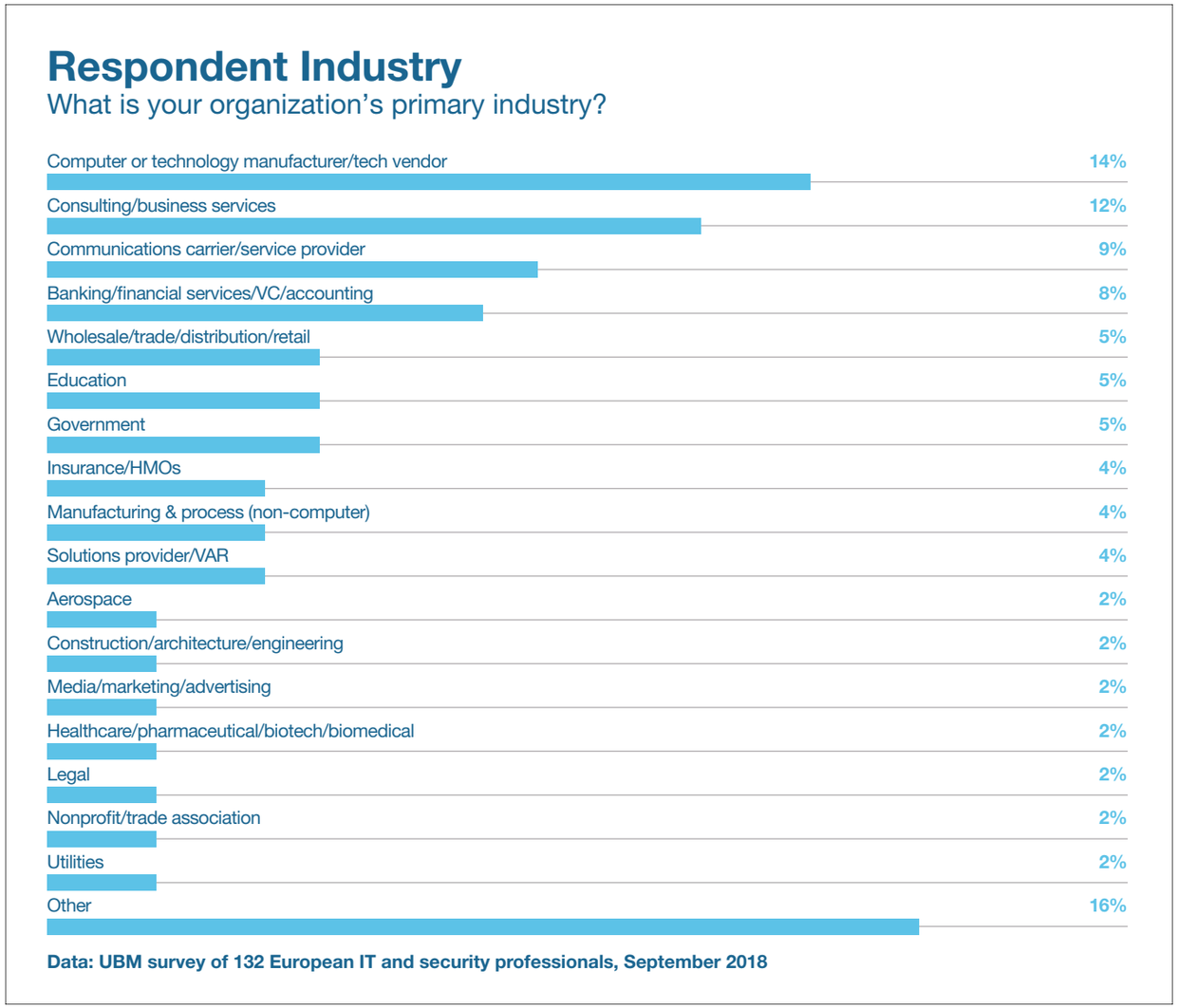
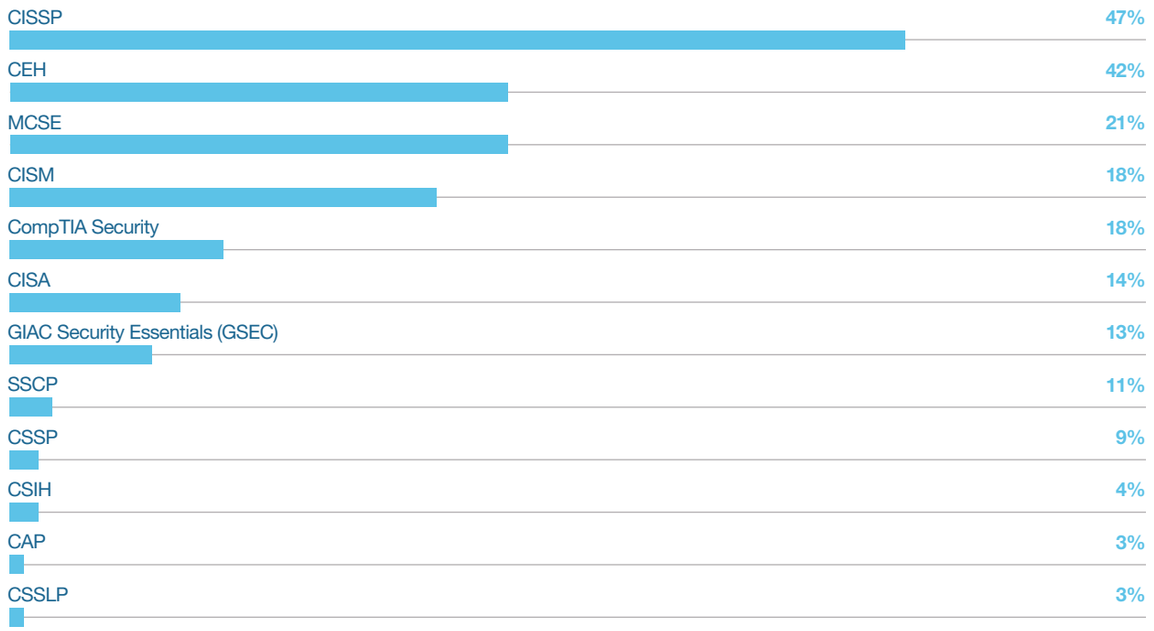

Respondent Industry
What is your organization's primary industry?
Computer or technology manufacturer/tech vendor 14%
Consulting/business services 12%
Communications carrier/service provider 9%
Banking/financial services/VC/accounting 8%
Wholesale/trade/distribution/retail 5%
Education 5%
Government 5%
Insurance/HMOs 4%
Manufacturing & process (non-computer) 4%
Solutions provider/VAR 4%
Aerospace 2%
Construction/architecture/engineering 2%
Media/marketing/advertising 2%
Healthcare/pharmaceutical/biotech/biomedical 2%
Legal 2%
Nonprofit/trade association 2%
Utilities 2%
Other 16%
Data: UBM survey of 132 European IT and security professionals, September 2018

Figure 25

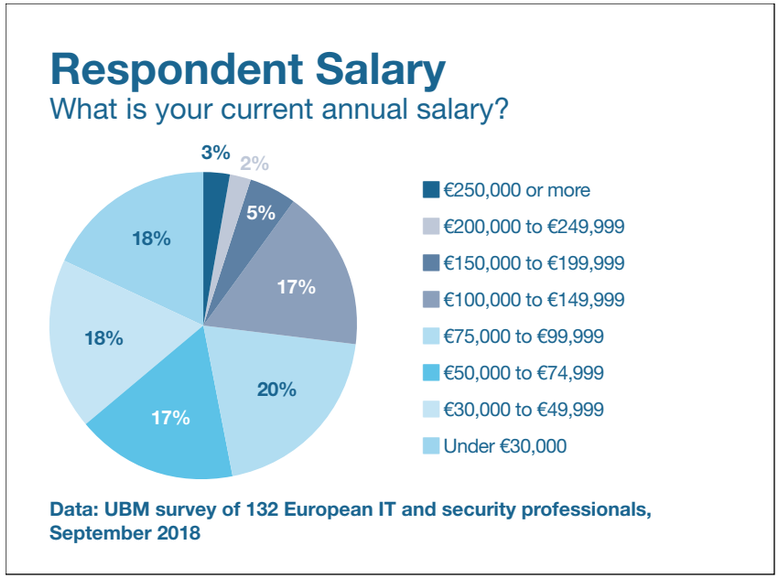
Respondent Security Certifications and Training Certificates

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



Note: Multiple responses allowed
Data: UBM survey of 132 European IT and security professionals, September 2018

Figure 26


Respondent Salary
What is your current annual salary?
3%
2%
5%
17%
20%
17%
18%
18%
€250,000 or more
€200,000 to €249,999
€150,000 to €199,999
€100,000 to €149,999
€75,000 to €99,999
€50,000 to €74,999
€30,000 to €49,999
Under €30,000
Data: UBM survey of 132 European IT and security professionals, September 2018