black hat® ASIA 2018

www.blackhat.com

March 2018

The 2018 Black Hat Asia Attendee Survey

Cybersecurity Risk in Asia

Survey of Black Hat conference attendees warns of threats to critical infrastructure, enterprise networks, and business data.

TABLE OF CONTENTS

Figures

EXECUTIVE SUMMARY

The latest wave of cyberattacks has raised the level of concern among IT security professionals across the globe, and Asia is no exception. A new survey of attendees to the Black Hat Asia conference – some of the most well-credentialed information security professionals in the region – reveals a high level of concern over targeted cyberattacks and potential breaches of critical infrastructure. A majority of the respondents believe their organizations will have to respond to a major security incident in the next 12 months. Most security professionals in Asia are also convinced that a cyberattack will disrupt critical infrastructure across multiple countries in the region within two years.

The survey polled respondents about the threats and challenges they are most concerned about, the attackers they fear most, and various factors that affect their cybersecurity posture, including budgets, skills availability, and management support. The 96 respondents from over 12 Asian nations included CEOs, CSOs, CIOs and other members of the C-suite, directors of information technology and information security, network admins and security staff. A majority of respondents work in organizations with over 1,000 employees.

The feedback shows that Black Hat attendees in Asia, like their peers in Europe and the United States, feel underprepared for and overwhelmed by the security challenges they confront on a daily basis. Many doubt their ability to defend against data breaches and withstand new threats. There is as much concern about targeted attacks from highly sophisticated adversaries, as well as risks posed by careless, negligent, and malicious insiders. Cybersecurity professionals in Asia feel their ability to properly defend against threats is being seriously hampered by a shortage of skills and budget. Reports about cyberattacks against critical infrastructure targets in the region appear to have engendered fears about major infrastructure disruptions in the region, and most respondents expect more breaches in the near term.

EXECUTIVE SUMMARY

The results of the Black Hat Asia survey show a remarkable consistency with results from our recent Black Hat surveys in the United States and Europe. This consistency illustrates the truly global nature of current and emergent cybersecurity threats, and the common struggles that organizations everywhere have in dealing with them.

The 2018 Black Hat Asia Survey provided several insights on the state of cybersecurity in the region. The following are some key takeaways:

- 62% believe it is somewhat likely, very likely, or almost certain that their organizations will experience a major data breach in 12 months.
- 6% cite targeted attacks by sophisticated cyber adversaries as their biggest security concern.
- 38% view end users who violate security policy or are easily fooled as their organizations' weakest link.
- 57% agree their enterprise data is at risk of compromise by malicious actors in Russia, China, and North Korea.
- Compliance-related spending consumes the greatest portion of security spending for 29% of the organizations.
- 31% believe the primary reason why cybersecurity strategies fail is because of a shortage of skilled professionals.

SYNOPSIS

RESEARCH

Survey Name The 2018 Black Hat Asia Attendee Survey

Survey Date January 2018

Number of Respondents The survey data is comprised of 96 IT and security professionals. The greatest possible margin of error for the total respondent base (N=96) is +/- 9.9 percentage points. UBM was responsible for all programming and data analysis. These procedures were carried out in strict accordance with standard market research practices.

Methodology In January 2018, Dark Reading and Black Hat conducted a survey of IT and security professionals from more than 12 Asian countries, Australia, and elsewhere. The online survey yielded data from 96 management and staff security professionals, predominantly at large companies, with 55% working at companies with 1,000 or more employees. Fifty-nine percent of the respondents are certified ethical hackers (CEH), 45% hold a CISSP certification, and 27% are CISA certified.

ABOUT US

For more than 20 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.

Critical Infrastructure Breaches in Asia May Be Imminent

A majority of IT security leaders in Asia are convinced that a major, successful cyberattack on critical infrastructure in their country, or multiple countries in the region, is imminent. Fifty-two percent, either "strongly agree" or "somewhat agree" that such an attack will happen in their own country in the next two years. An even greater proportion (67%) believes that an attack impacting critical infrastructure across multiple Asian countries will happen in the same period. **(See Figure 1.)**

The jitters may have to do with several recent attacks on critical infrastructure organizations in Asia and the Middle East. One example is a campaign involving the use of TRITON, a sophisticated malware tool designed to cause physical damage to industrial control systems (ICS), which was recently discovered by FireEye researchers at a critical infrastructure facility in Saudi Arabia. Another campaign, reported by researchers at Nyotron, was focused on stealing data from ICS targets in the Middle East for the purpose of conducting surveillance.

Figure 1

Today's Security Issues

Please tell us how strongly you agree or disagree with the following statements.

	Strongly agree	Somewhat agree	Neutral	Somewhat disagree	Strongly disagree
I believe that Asian countries will significantly increase their efforts to harmonize cybersecurity and privacy regulations and protections in the near future.	30%	33%	28%	7%	2%
Recent activity emanating from Russia, China, and North Korea has made Asian enterprise data less secure.	27%	30%	31%	6%	6%
I believe that Asian laws should be changed to allow enterprises to take offensive action against online attackers who attempt to steal data.	26%	27%	34%	8%	5%
I believe that a successful cyber attack affecting the critical infrastructures of multiple Asian countries will occur in the next two years.	23%	44%	23%	9%	1%
I believe that a successful cyber attack on the critical infrastructure of my home country will occur in the next two years.	22%	30%	29%	16%	3%
The shortage of women and minorities in the information security profession concerns me.	21%	26%	35%	14%	4%

Data: UBM survey of 96 IT and security professionals, February 2018

A third, dubbed Operation PZChao, has been wreaking havoc on computers belonging to various critical sectors in Asia since mid-2017, according to BitDefender researchers.

Perhaps understandably, 23% of the Black Hat Asia survey respondents believe that cyber espionage by large nation states represents the greatest threat to Asia's critical infrastructure, followed by potential attacks by organized crime groups (21%). Concerns about terrorist organizations launching cyberattacks are relatively low, with only 10% of the respondents seeing them as a threat to critical infrastructure in the region. **(See Figure 2.)**

Figure 2

Interestingly, 19% believe that a lack of cooperation among Asian governments and the agencies responsible for cybersecurity in each country poses the biggest threat to critical infrastructure security in the region. Fifty-three percent want laws in Asia to be changed so organizations have more freedom to go on the counter offensive against cyber attackers without fear of legal repercussions.

The concerns over critical infrastructure security in Asia are nearly identical to the concerns expressed in the Black Hat USA and Black Hat Europe reports. They indicate a clear lack of confidence among Asia's leading IT security experts over the current state of critical infrastructure protection in the region, and a call to action for better defenses. Sixty three percent are hopeful that governments in the region will better harmonize cybersecurity and privacy legislations in the near term.

Targeted Attacks Threaten Asian Enterprises

Targeted cyberattacks on specific organizations have become a growing problem for security professionals everywhere. In recent years, threat actors have refocused their exploits from the mass, opportunistic attacks of the past to attacks that are highly targeted and focused on specific objectives such as data theft or extortion via ransomware. The responses to the 2018 Black Hat Asia Attendee Survey reflect that trend.

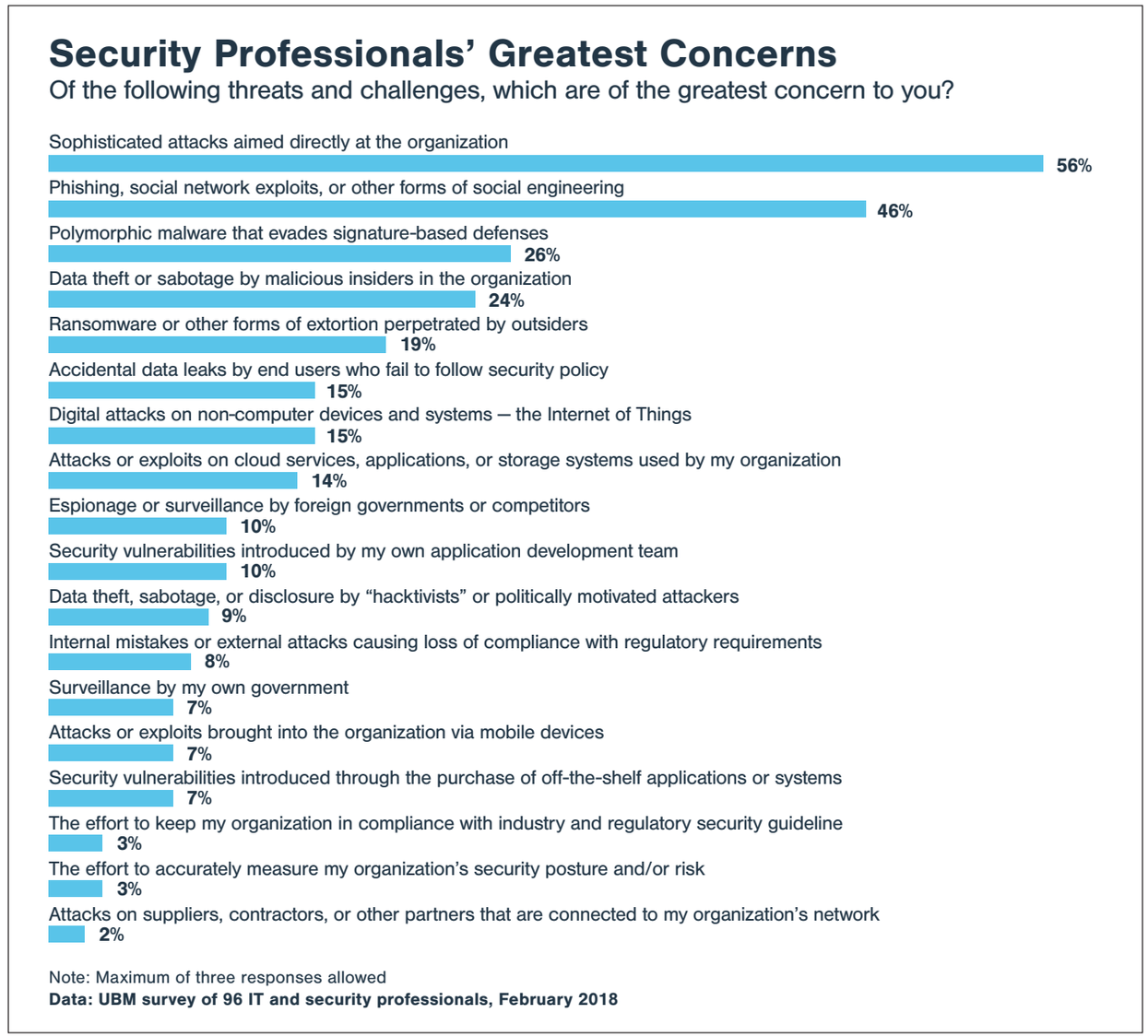
IT and security managers in Asia are more concerned about sophisticated attacks targeted specifically at their organizations than about any other threat. When asked to identity

their three top current security concerns, 56% of the respondents listed targeted attacks as their top challenge. **(See Figure 3.)** The same result emerged when respondents were asked to list the greatest concerns to their organization's top management and executives. Many believe that targeted attacks will continue to be the biggest threat going forward; 35% say they expect it to remain their top concern in 2020. **(See Figure 4.)**

Like their peers in other regions, a majority of the respondents in our Asia survey are concerned about the threat to enterprise data posed by malicious actors in Russia, China, and North Korea. Fifty-seven percent strongly or somewhat strongly agree that recent malicious activity in these countries has made their organization's data less secure.

These concerns reflect recent trends in the threat landscape. A 2017 end-of-year report from Flashpoint indicates that state-sponsored attackers from Russia and North Korea – and, to a lesser extent, China – ramped up their activities last year in response to various geopolitical factors. Threat actors from North Korea in particular have increasingly begun hi-

Figure 3

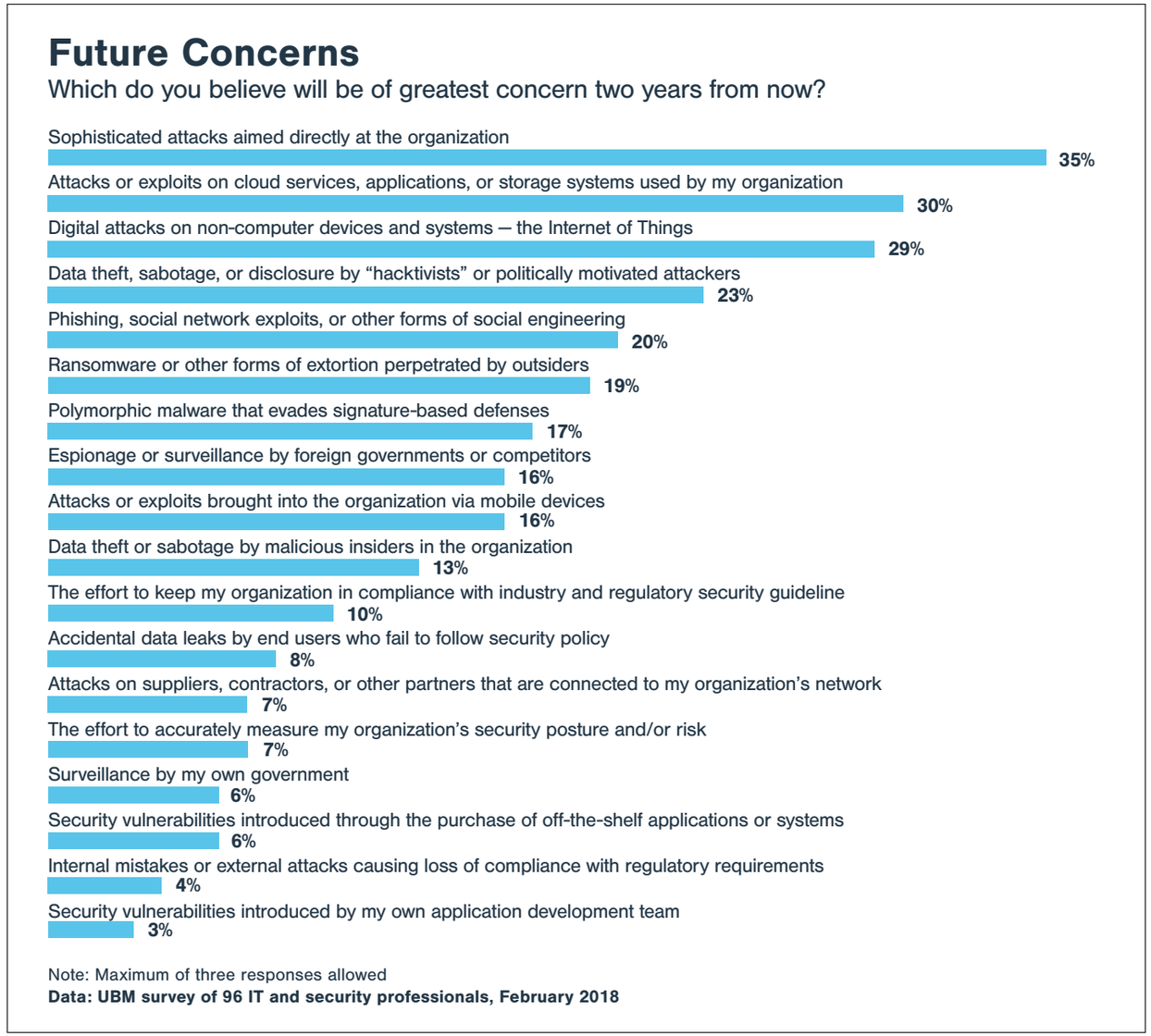


jacking enterprise computers for ransom and cryptocurrency mining in order to raise funds for the government amid tightening economic sanctions. Recent reports about multiple attacks on critical infrastructure organizations in the Middle East and in Asian countries no doubt have contributed to the broader concerns about targeted attacks as well.

Targeted attacks are not the only concern. Forty-six percent of the respondents in the 2018 Black Hat Asia Attendee survey listed phishing and other social engineering scams as another top issue. Twenty-four percent believe it is a major concern for top management as well. The results reveal the high degree of anxiety among enterprises in Asia over the increase in the use of these techniques and, more importantly, the success that attackers have enjoyed by using them. A yearlong study released by Google in November showed that a majority of email account takeovers result from attackers obtaining credentials via phishing and social engineering campaigns.

Beyond targeted attacks and phishing, our respondents had diverse views on their current security concerns. Twenty-six percent cited

Figure 4



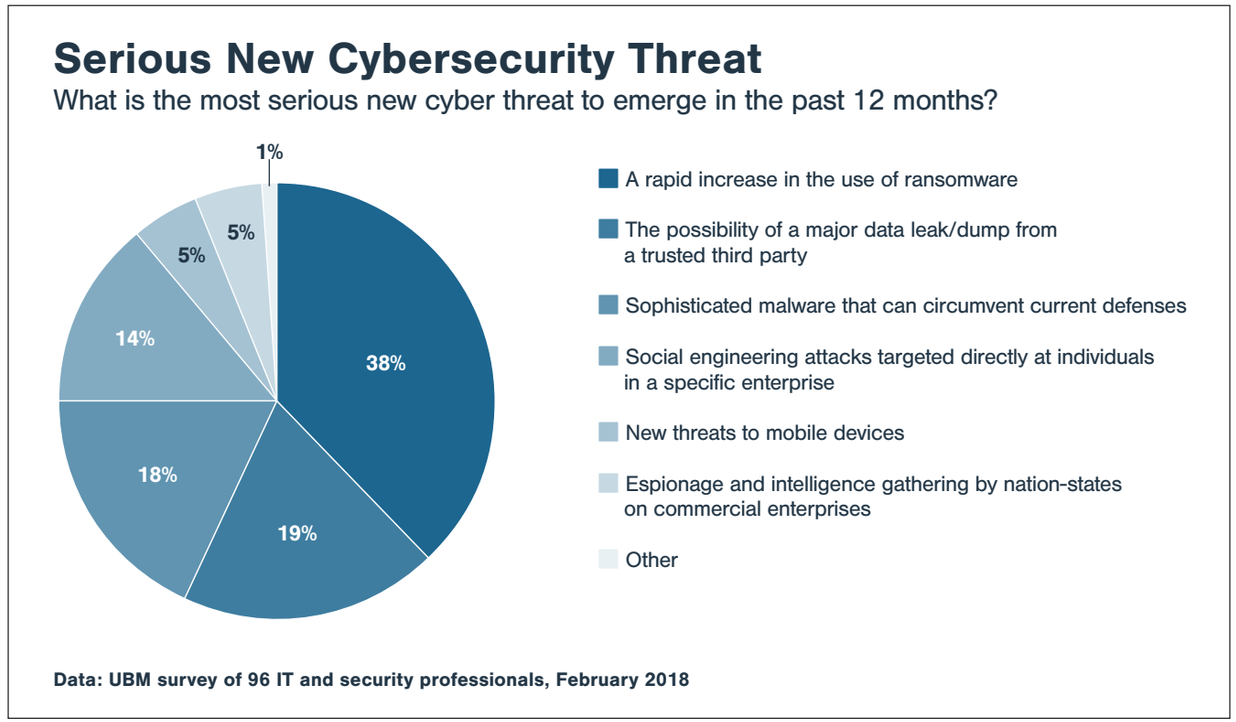
polymorphic malware as one of their biggest issues, while almost an equal proportion (24%) pointed to sabotage and data theft by malicious insiders. Some of the top concerns listed by respondents were accidental data leaks (15%), Internet of Things (IoT) threats (15%), attacks on cloud services (14%), and espionage by a foreign government (10%).

The same diversity of opinion was apparent when we asked respondents to list what they expect their top concerns to be in two years' time. Targeted attacks, as noted previously, remained the top-expected concern for 2020, suggesting that security professionals in the region see it as a long-term issue. There was also some consistency of opinion around the threats posed by attacks on cloud services and on IoT technology, with 30% and 29% respectively listing these as the top concerns anticipated for 2020. Beyond these, however, our respondents cited a diversity of anticipated threats, including phishing (20%), polymorphic software (17%), and espionage (16%).

Somewhat surprisingly, only 19% identified ransomware and other forms of online extortion as a top current concern, despite much publicity around the topic over the past year. Exactly the same low proportion of security and IT managers in Asia think ransomware will be a top concern even two years down the road. Paradoxically, when we asked survey takers to identify the most serious new cyberthreat to emerge in the past 12 months, a plurality (38%) pointed to the rapid increase in the use of ransomware as the top threat. (**See Figure 5.)**

Also somewhat surprising was the relative lack of concern around mobile threats and around data theft and sabotage by politically-motivated adversaries. Only 9% and 7% re-

Figure 5



spectively cited these threats as a major concerns. It may be that the hype around these two issues may be overshadowing the reality.

Skills Shortage, Budget Issues Fuel Uncertainty

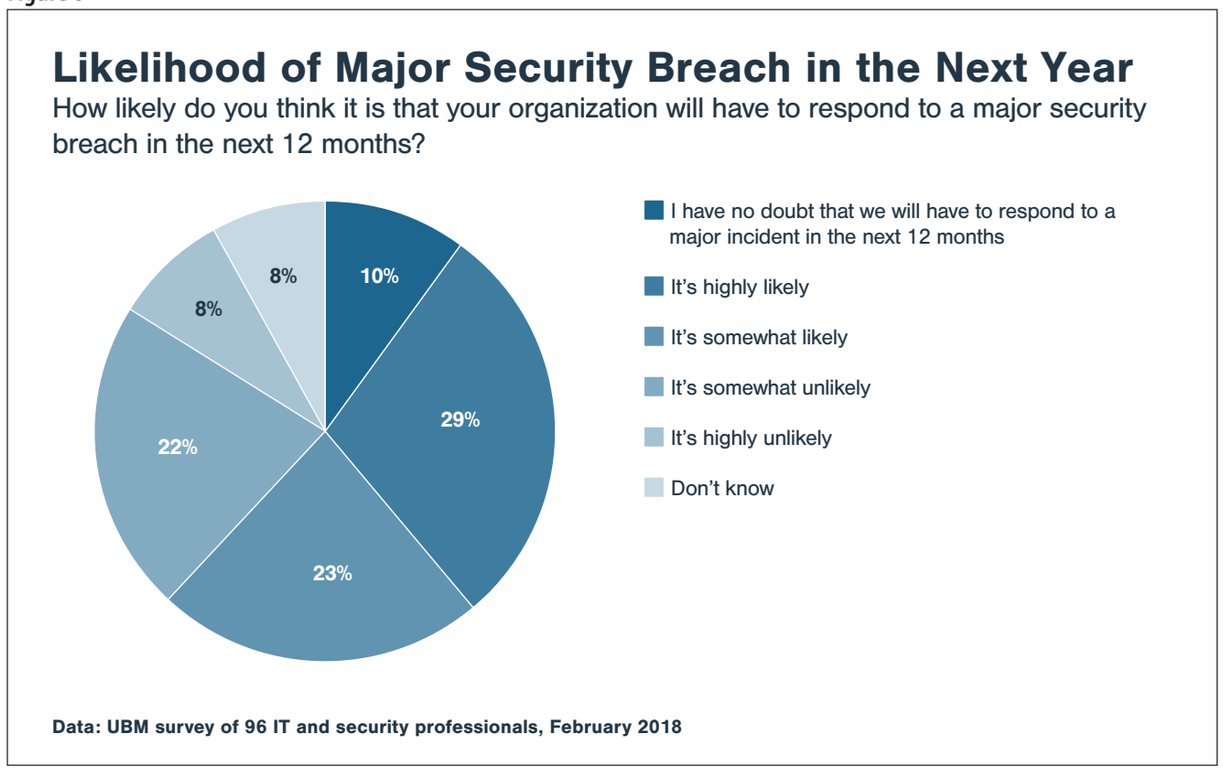
Many security leaders in Asia share the pessimism of their counterparts in Europe and US when asked about their ability to prevent a major data breach from happening in the short-term. Nearly four in 10 organizations (39%) in our Asia survey think it is highly likely or a near certainty that they will have to respond to a major security incident in the next 12 months. Another 23% think it is somewhat likely they will experience a breach. Only 8% believe that a major breach of their organizations is highly unlikely. **(See Figure 6.)**

The pessimism over data breaches appears to be rooted in several familiar factors. The incessant reports about data breaches at other organizations — including many at critical infrastructure facilities in Asia and the Middle East — no doubt are one reason why so many security pros feel a breach is imminent.

Budget and resource availability would appear to be two other big reasons. Fifty-three percent of those who participated in the 2018 Black Hat Asia Attendee survey said they were either a little under budget or "severely hampered" in their ability to fight threats because of a lack of funds. Another 4% suggested they had no funds at all for the security cause. In total, security operations at nearly 6 in 10 organizations in Asia are hampered to some extent by a lack of budget. **(See Figure 7.)**

A relative shortage of security skills — likely, at least partially, because of the lack of budget

Figure 6

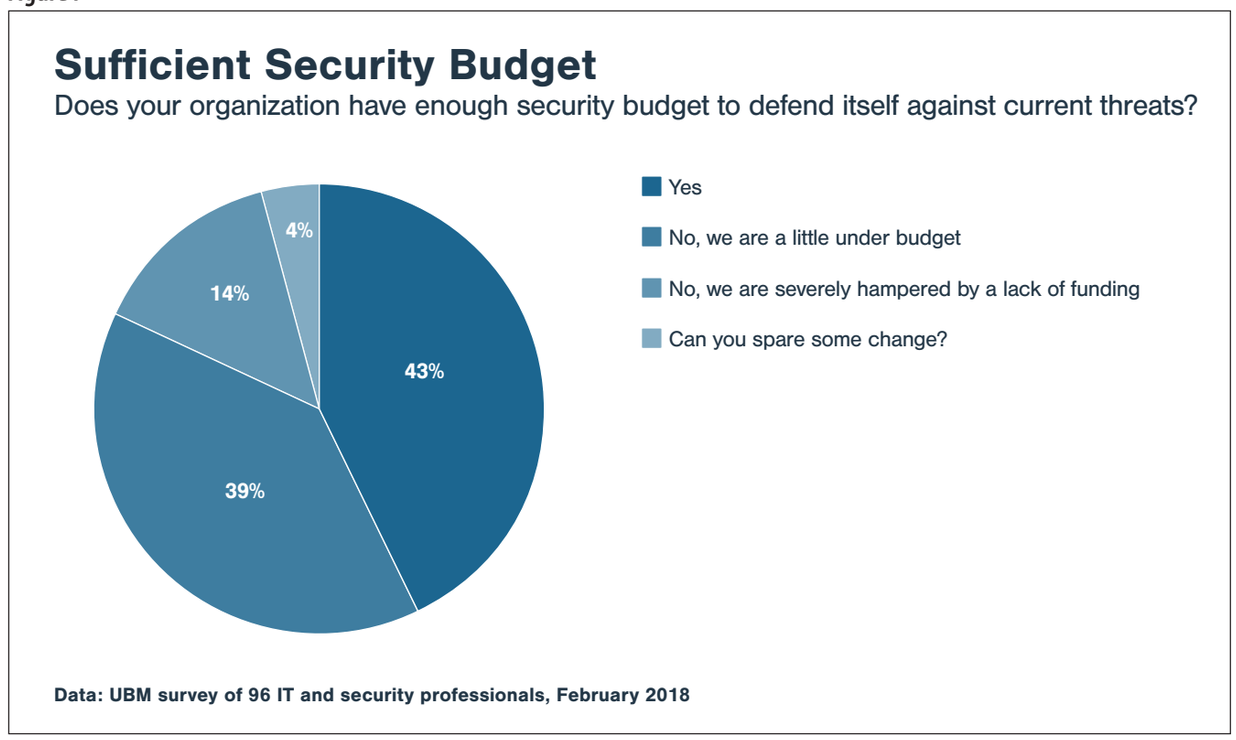


mentioned above — is exacerbating the issue. Fifty-eight percent identified a shortage of security staff as making it harder for them to defend against current threats. Of those, 17% reported being completely underwater; 3% said they had no staff and 38% said they could use a little bit of additional help. **(See Figure 8.)**

Budget and skills shortage have been a perennial problem for cybersecurity managers everywhere. Yet, paradoxically, the complaints about lack of budget come amid signs of substantial increases in enterprise cybersecurity spending over the past two years. Gartner, for instance, expects worldwide enterprise security spending to top $96 billion in 2018, an increase of 8% from $89 billion in 2017 and 17% higher than the $82 billion spent in 2016. The fact that many security leaders still feel underfunded suggests that these spending increases, while encouraging, are not enough.

Meanwhile, the relative shortage of security staff among our Asian survey respondents is a manifestation of a much broader problem. Last year, Frost & Sullivan forecast that there would be a global shortage of 1.8 million information security workers by 2022. That's actually a significantly bigger gap than the 1.5 million worker shortage estimate they had originally predicted in 2015.

Figure 7



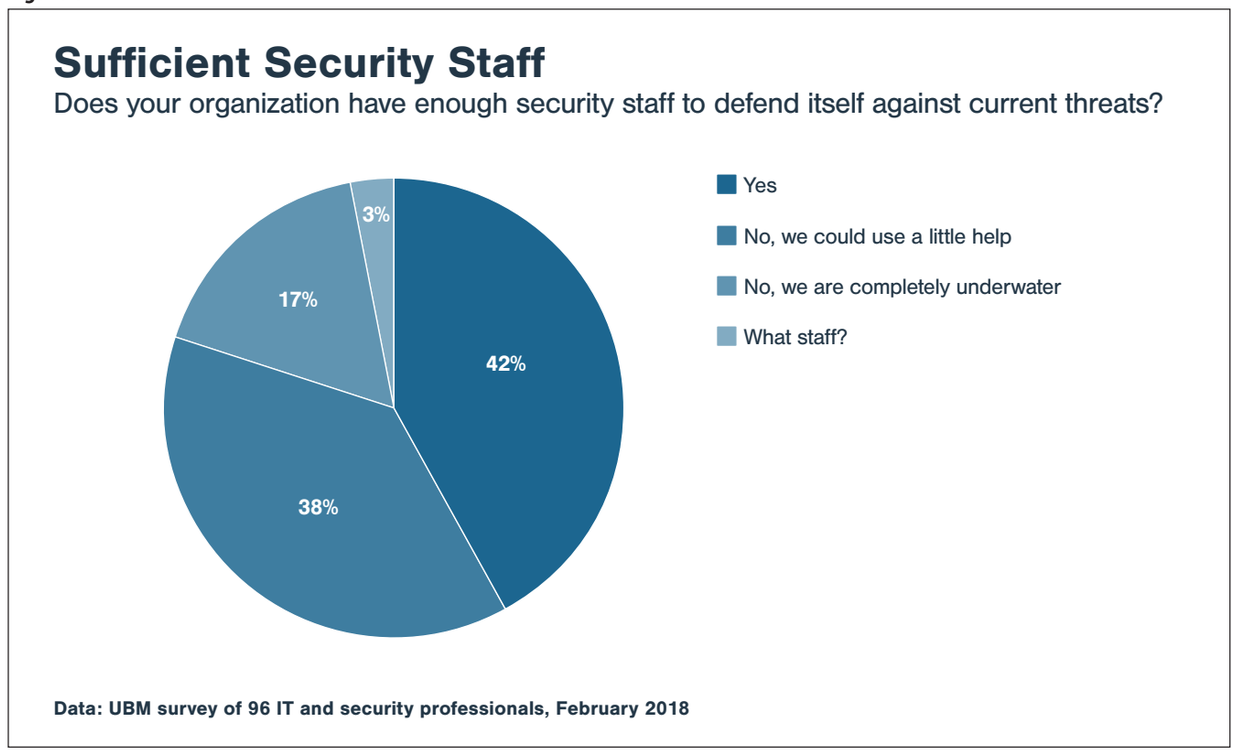
Compared to other regions, the security staffing situation in Asia is actually better — but only marginally so. According to Frost & Sullivan, six in ten organizations in Asia suffer from a shortage of workers, compared to 68% in North America and 66% in Europe. Interestingly, the reasons for the cybersecurity staff shortage at so many organizations in Asia, as elsewhere, go beyond a simple lack of budget. Among the other common reasons was the sheer lack of available skills, staff requirements

not being understood by top management, and staff attrition, according to Frost & Sullivan.

This last point, in particular, is reflected in our survey results: 29% of Asian respondents are actively looking for a new job, and 23% are open to it. Another 30% would listen if a new employer called. A bare 14% love their present jobs and have no immediate plans to move. **(See Figure 9.)** These results suggest that there are more security pros available among the Black Hat Asia audience than among similar audiences in Europe or the United States.

In addition to the concern over staffing shortages, many IT security professionals in Asia seem unsure about their own skills to defend their organizations against data breaches. Fifty-nine percent of the respondents are certified ethical hackers; 45% hold a CISSP certification and 27% are CISA certified. **(See Figure 10.**) Yet only 31% believe they have the skills and the training to handle current threats and perform all the job functions required of them. A surprising 49% believe they could use some additional training, and 15% flat-out feel they are unprepared for their roles. **(See Figure 11.)** The lack of self-confidence behind those numbers may be another reason why so many security professionals believe a data breach at their organizations is imminent.

Figure 8



Security Weaknesses and Spending Plans

What do security professionals in Asia consider as their biggest weaknesses? For many, it is end users who violate security policy or fall prey to phishing and social engineering scams. Nearly 4 in 10 (38%) of the professionals surveyed said such users are the biggest flaw in their armor. **(See Figure 12.)** The sentiment is not surprising, considering the substantial number of recent data breaches

that have resulted from end users opening malicious attachments or clicking on links to rogue websites. About 10% of the breaches that exposed sensitive data in 2017 resulted from employee error, negligence, and related factors, according to the Identity Theft Resource Center.

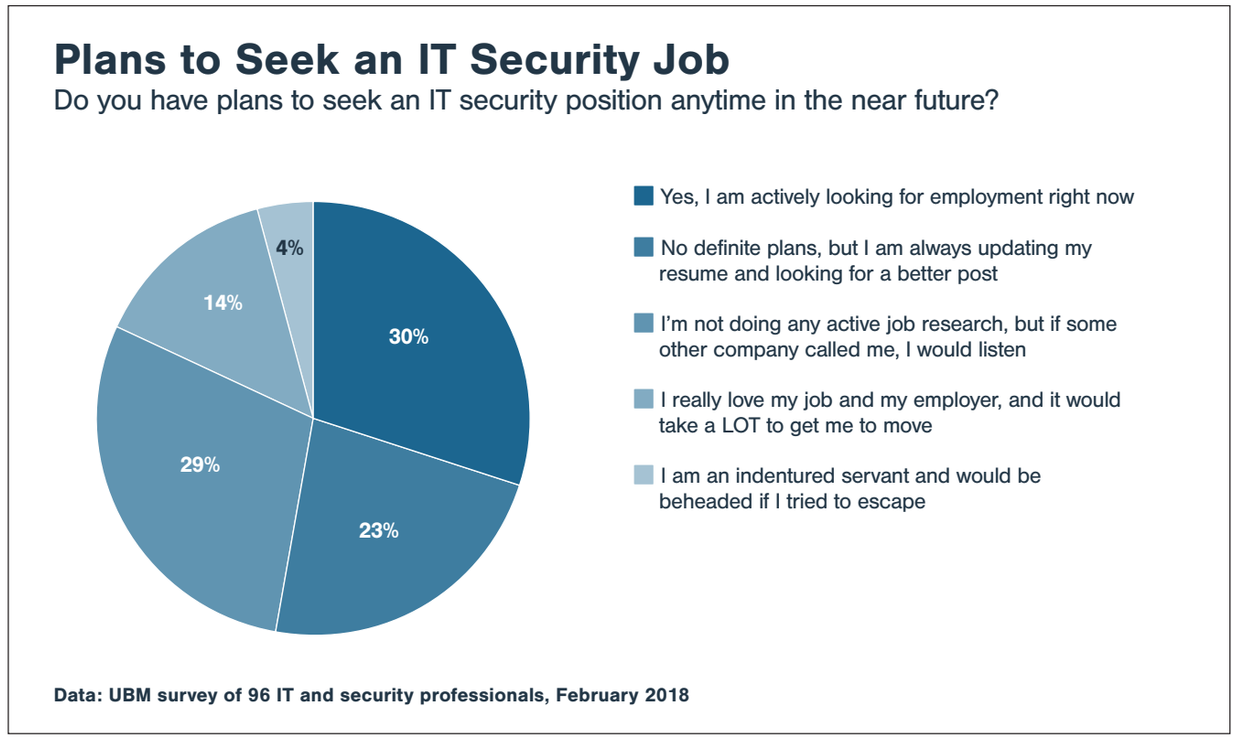
"End users are definitely the weakest link in security systems," says Avivah Litan, an analyst with Gartner. "To effectively defend against their weaknesses enterprises need a combined approach that uses technical and non technical controls," she says. Non-technical controls include security awareness and training and effective workforce management. Technical measures include tools for user monitoring, user behavior analytics, and for protecting against phishing attacks, Litan states.

If bumbling and negligent users are a big concern, malicious insiders are an even bigger threat. Thirty-one percent of those polled in the Black Hat Asia survey said the adversary they feared the most was the insider with knowledge of the organization and trusted access to enterprise systems and data. **(See Figure 13.)** A 2018 report on insider threats from Securonix shows that many organizations feel vulnerable to insider attacks because of too many users with excessive access privileges, and too many devices with access to sensitive data.

The other types of cyber attackers that IT security professionals fear most are people with knowledge of 0-day vulnerabilities, those that have strong technical skills, and those backed by a nation state or cybercrime gang.

Humans are not the only cause for IT professionals' concern. Fifteen percent of the respondents in the Black Hat Asia survey said their biggest weakness stemmed from a lack of planning and a tendency within their organiza-

Figure 9



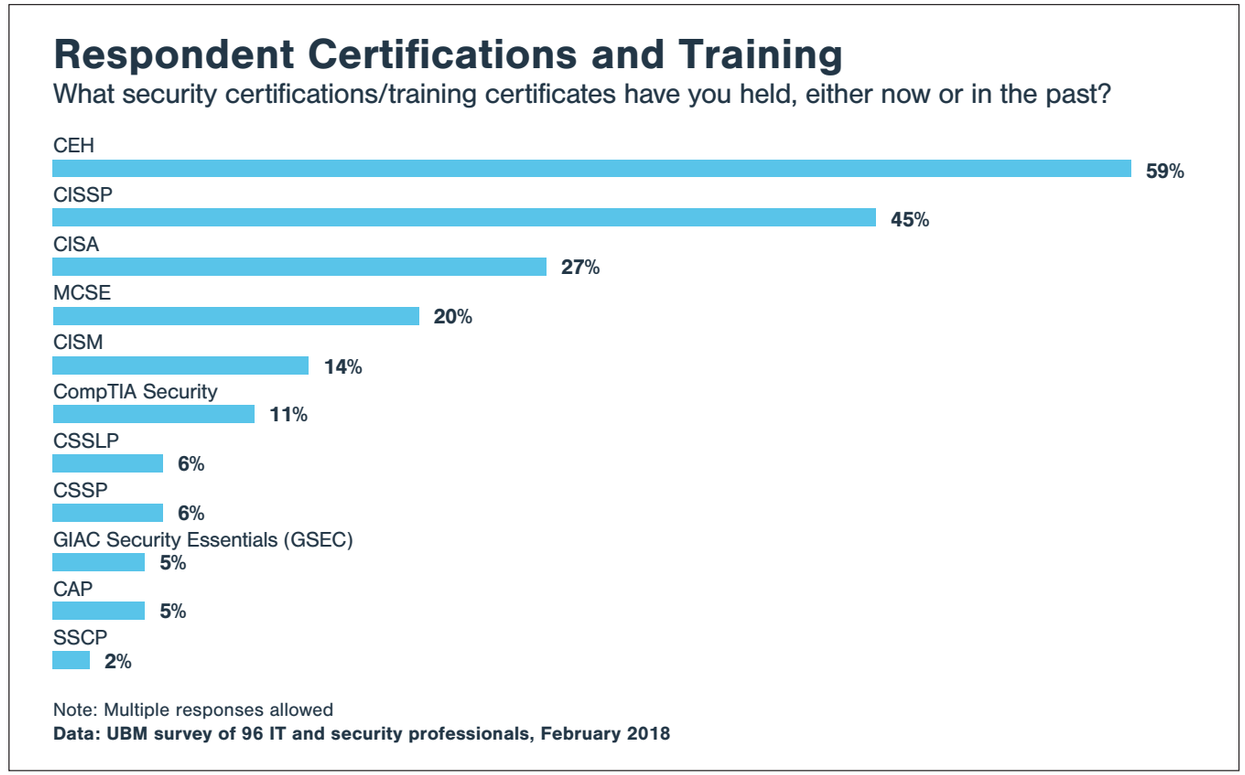
tions to treat IT as a non-strategic, fire-fighting mission. Twelve percent view mobile device vulnerabilities as being the weakest link; 10% are worried about vulnerabilities in in-house apps, and a smaller proportion perceive cloud services, endpoint vulnerabilities and web-based threats as weak links.

How are organizations in Asia spending most of their security dollars, resources, and time? It varies with the respondent. Three areas where there is at least some commonality in spending are targeted threats, compliance-related activities, and phishing/social engineering. When we asked survey takers to list the activities that consumed the greatest portion of their IT security budget, 31% pointed to targeted attacks, 29% said compliance efforts, and 21% said dealing with phishing and social engineering threats.

Beyond these three areas, organizational spending on information security in Asia appears to be quite varied. At 19% of the organizations we surveyed, vulnerability mitigation in off-the-shelf products was a major focus of security spending. For 17%, it was accidental data leaks by end users. Similarly, 17% said a big portion of their IT budgets is consumed by activities related to bringing their organizations back into compliance after an internally or externally caused security incident. Other high-spend security activities included vulnerability mitigation in internally developed apps (17%), insider data theft (16%), and dealing with polymorphic malware (15%).

There is much greater commonality in respondents' views on the greatest time-consumers in Asian IT security. More than 25% of the organizations in our survey said they

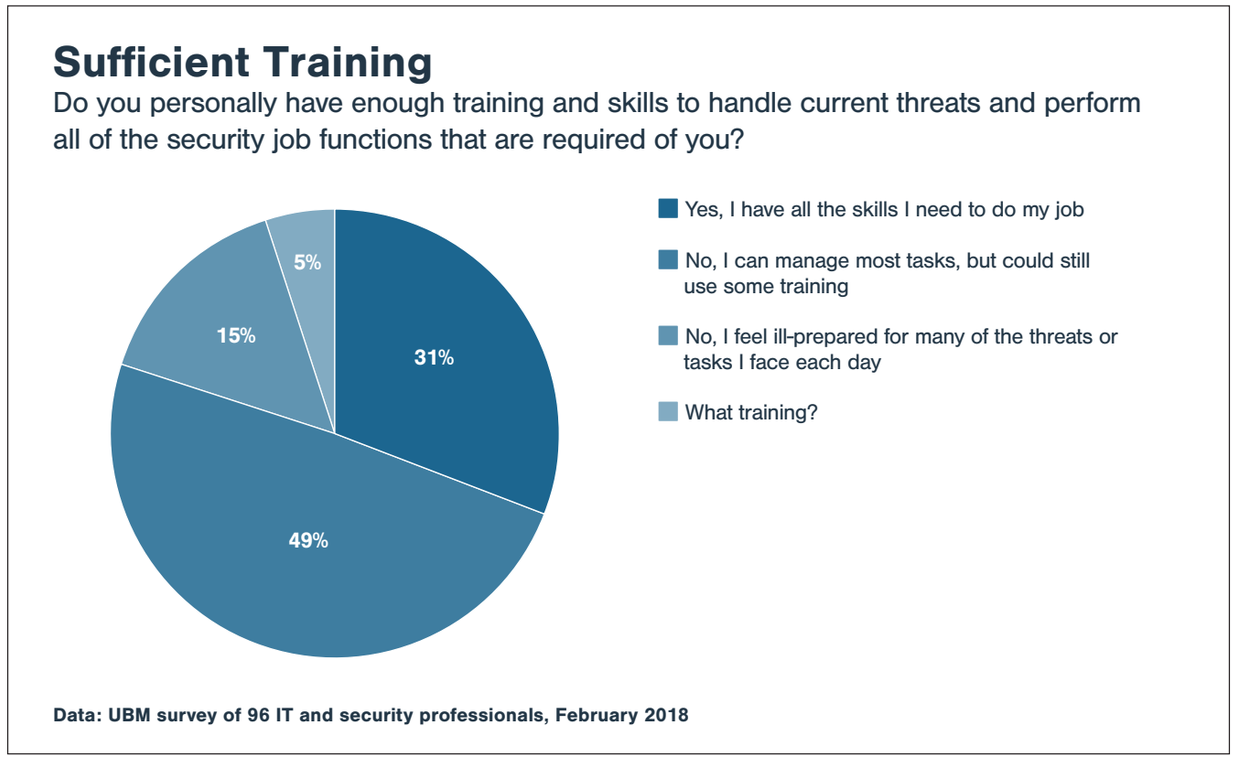
Figure 10



spent the most time dealing with phishing attacks, accidental data leaks, and compliance. Three other activities that appear to be consuming a lot of time are vulnerability mitigation in internal applications, cited by 24% of the respondents, targeted attacks (23%), and risk measurement (23%). **(See Figure 14.)**

The substantial amount of time and money that organizations in Asia appear to be spending on compliance-related activities is noteworthy — and very reminiscent of patterns in other regions of the world. Like their peers in the United States and Europe, IT security leaders in Asia are under pressure to comply with a slew of data security and privacy regulations. Many Asian countries already have or are implementing guidelines that require businesses to comply with specific rules for handling and securing personal and financial data. One example is the APEC Privacy Framework, which requires companies in the 27 countries that form the Asia Pacific Economic Cooperation region to adhere to certain privacy guidelines. Thirty percent of Black Hat Asia survey respondents view the framework as having created more work for them. Sixteen percent think APEC has substantively improved consumer privacy, while 14% say it hasn't done anything to improve privacy. **(See Figure 15.)**

Figure 11



Sixty percent of the organizations in the Black Hat Asia survey are required to comply with privacy requirements in Singapore, 32% in China, 25% in Hong Kong, and 24% in Australia. Many of these companies also have compliance obligations under the European Union's General Data Protection Regulation (GDPR). **(See Figure 16.)** For many, the time and money spent complying with this smorgasbord of regula-

tions is greater than the proportion of resources being spent on preventing threats.

"New regulations ignore where you operate as a business. They focus on where your customers reside," says Jeff Pollard, an analyst with Forrester Research. That greatly expands the scope of the compliance problem that businesses face and increases the time and effort required for compliance.

"It's definitely fun to talk about the spy novel aspects of cybersecurity — nation-state hackers, sophisticated malware, and cutting edge incident response work," Pollard says. "But the truth is that compliance efforts are a key element of what enterprise security leaders do to enable their organization to operate internationally."

Conclusion

The results of the 2018 Black Hat Asia Survey reveal a high level of uncertainty among enterprises about their ability to deal with current and emerging security threats. A majority of respondents doubt their organizations' ability to prevent major breaches from happening and believe that a crippling attack on a major critical infrastructure target in the region is imminent. Compliance efforts appear to be consuming a large portion of enterprise security budgets and resources —even as organizations confront new and highly-sophisticated threats.

APPENDIX

Figure 12

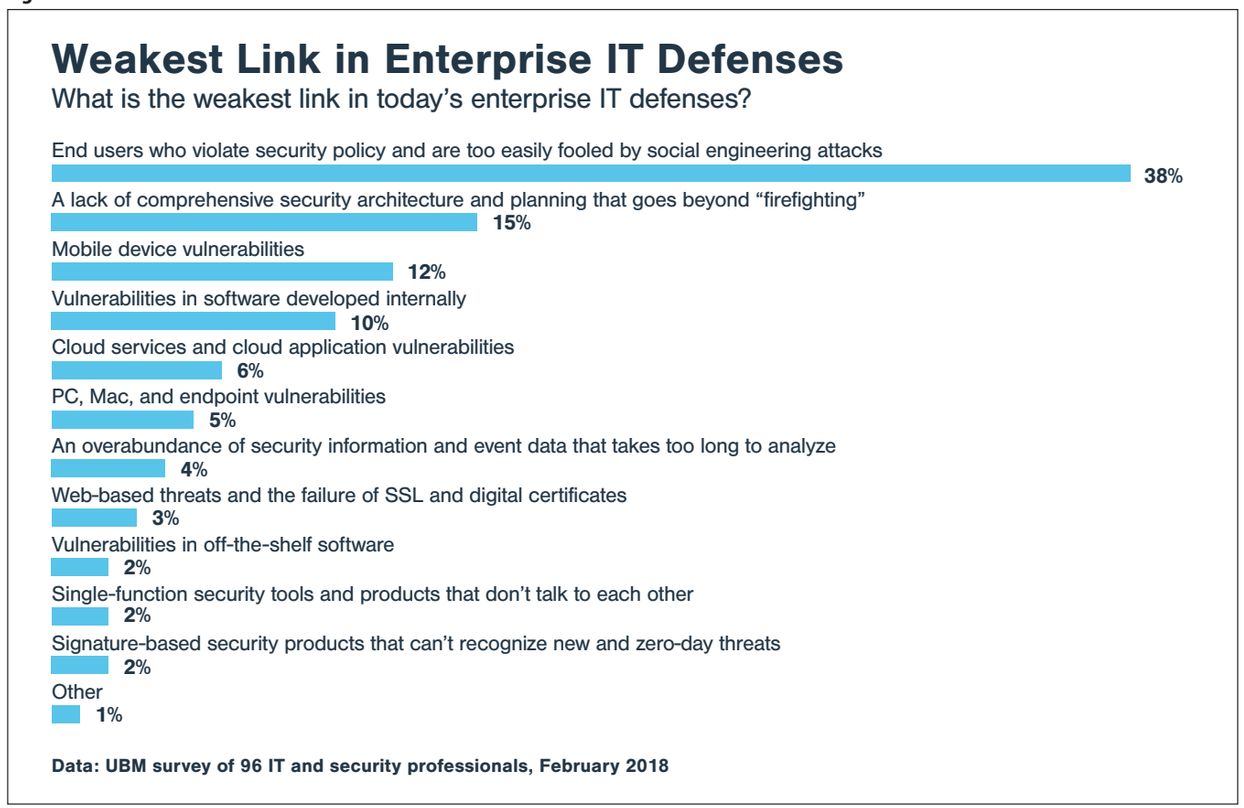
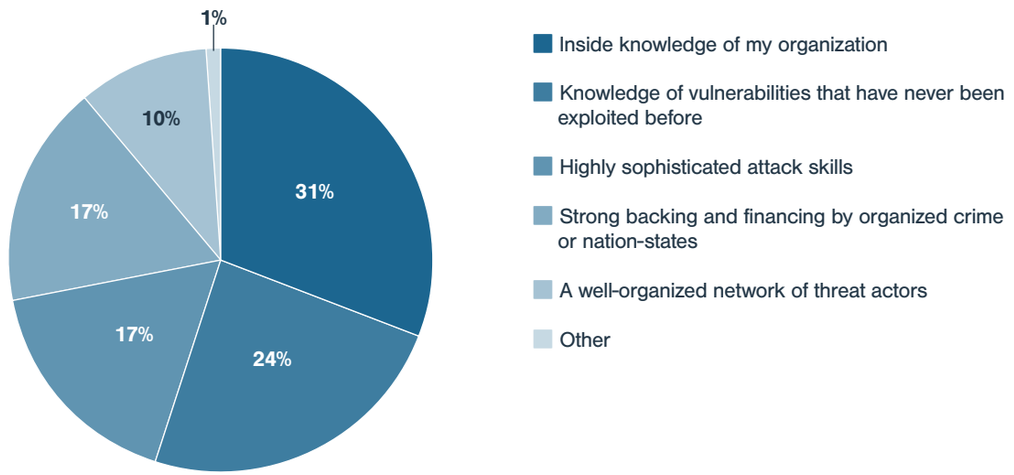


Figure 13

Most-Feared Cyber Attacker

The cyber attacker I fear most is the one who has ...



Data: UBM survey of 96 IT and security professionals, February 2018

Figure 14

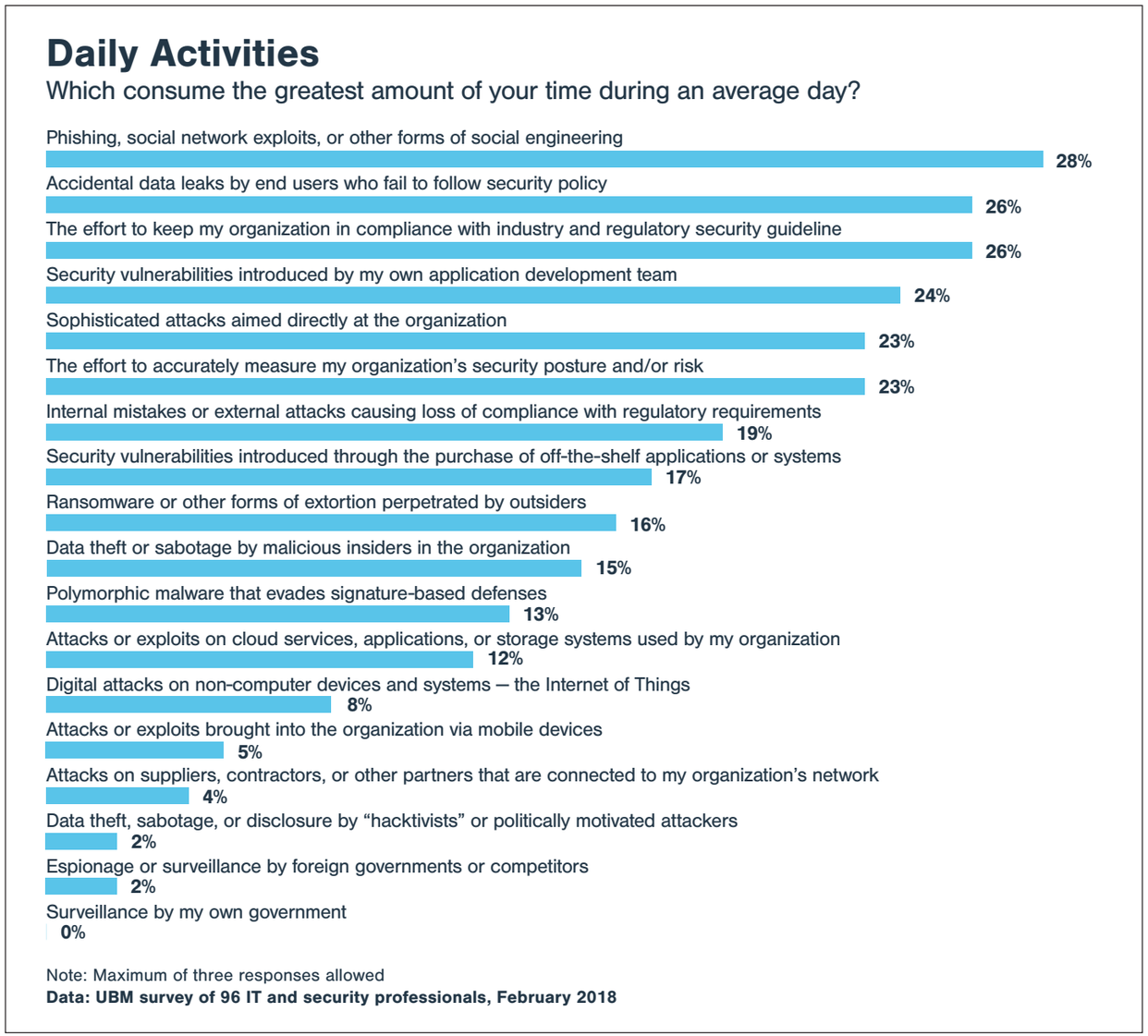

Daily Activities
Which consume the greatest amount of your time during an average day?
Phishing, social network exploits, or other forms of social engineering
28%
Accidental data leaks by end users who fail to follow security policy
26%
The effort to keep my organization in compliance with industry and regulatory security guideline
26%
Security vulnerabilities introduced by my own application development team
24%
Sophisticated attacks aimed directly at the organization
23%
The effort to accurately measure my organization's security posture and/or risk
23%
Internal mistakes or external attacks causing loss of compliance with regulatory requirements
19%
Security vulnerabilities introduced through the purchase of off-the-shelf applications or systems
17%
Ransomware or other forms of extortion perpetrated by outsiders
16%
Data theft or sabotage by malicious insiders in the organization
15%
Polymorphic malware that evades signature-based defenses
13%
Attacks or exploits on cloud services, applications, or storage systems used by my organization
12%
Digital attacks on non-computer devices and systems — the Internet of Things
8%
Attacks or exploits brought into the organization via mobile devices
5%
Attacks on suppliers, contractors, or other partners that are connected to my organization's network
4%
Data theft, sabotage, or disclosure by "hacktivists" or politically motivated attackers
2%
Espionage or surveillance by foreign governments or competitors
2%
Surveillance by my own government
0%
Note: Maximum of three responses allowed
Data: UBM survey of 96 IT and security professionals, February 2018

Figure 15

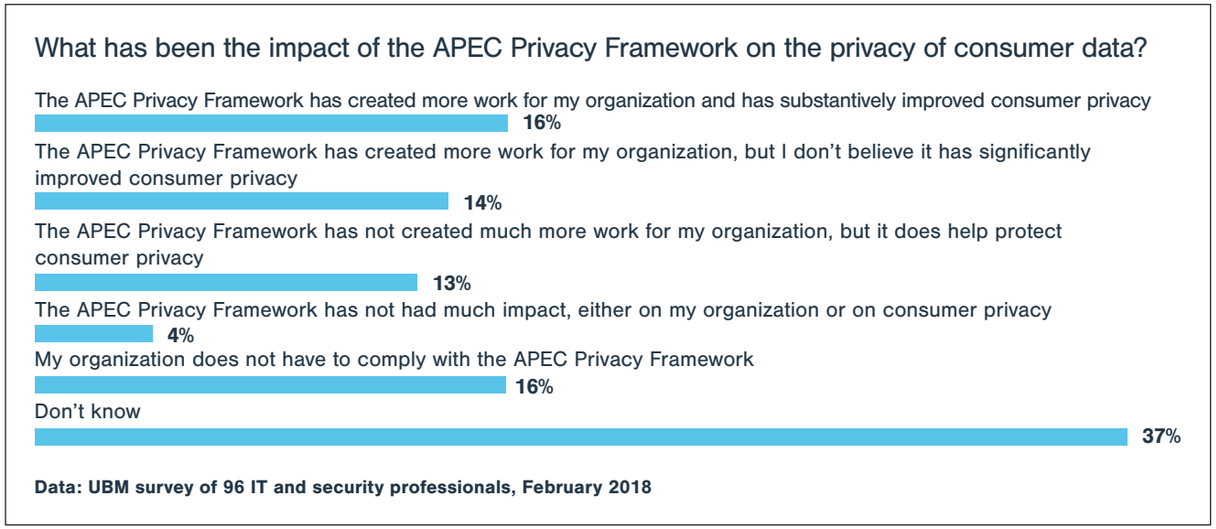
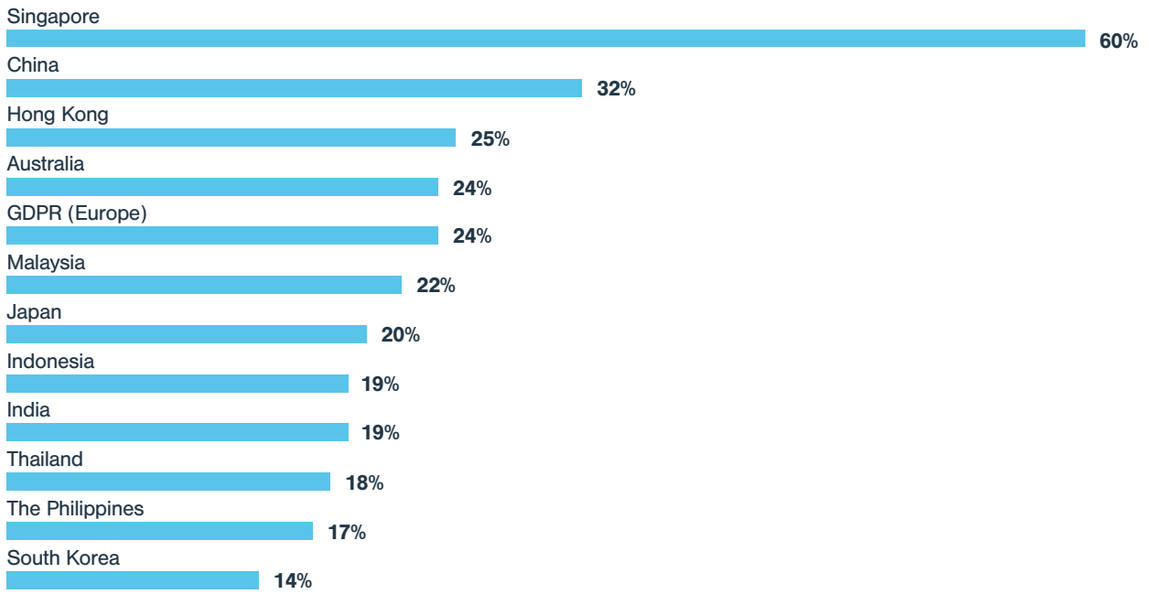

What has been the impact of the APEC Privacy Framework on the privacy of consumer data?
The APEC Privacy Framework has created more work for my organization and has substantively improved consumer privacy
16%
The APEC Privacy Framework has created more work for my organization, but I don't believe it has significantly improved consumer privacy
14%
The APEC Privacy Framework has not created much more work for my organization, but it does help protect consumer privacy
13%
The APEC Privacy Framework has not had much impact, either on my organization or on consumer privacy
4%
My organization does not have to comply with the APEC Privacy Framework
16%
Don't know
37%
Data: UBM survey of 96 IT and security professionals, February 2018

Figure 16

Required Privacy Regulations

Many Asian countries are establishing privacy guidelines that require businesses to comply with specific rules on the handling of personal information.
Where is your organization required to meet these privacy regulations?



Note: Multiple responses allowed
Data: UBM survey of 96 IT and security professionals, February 2018

Figure 17

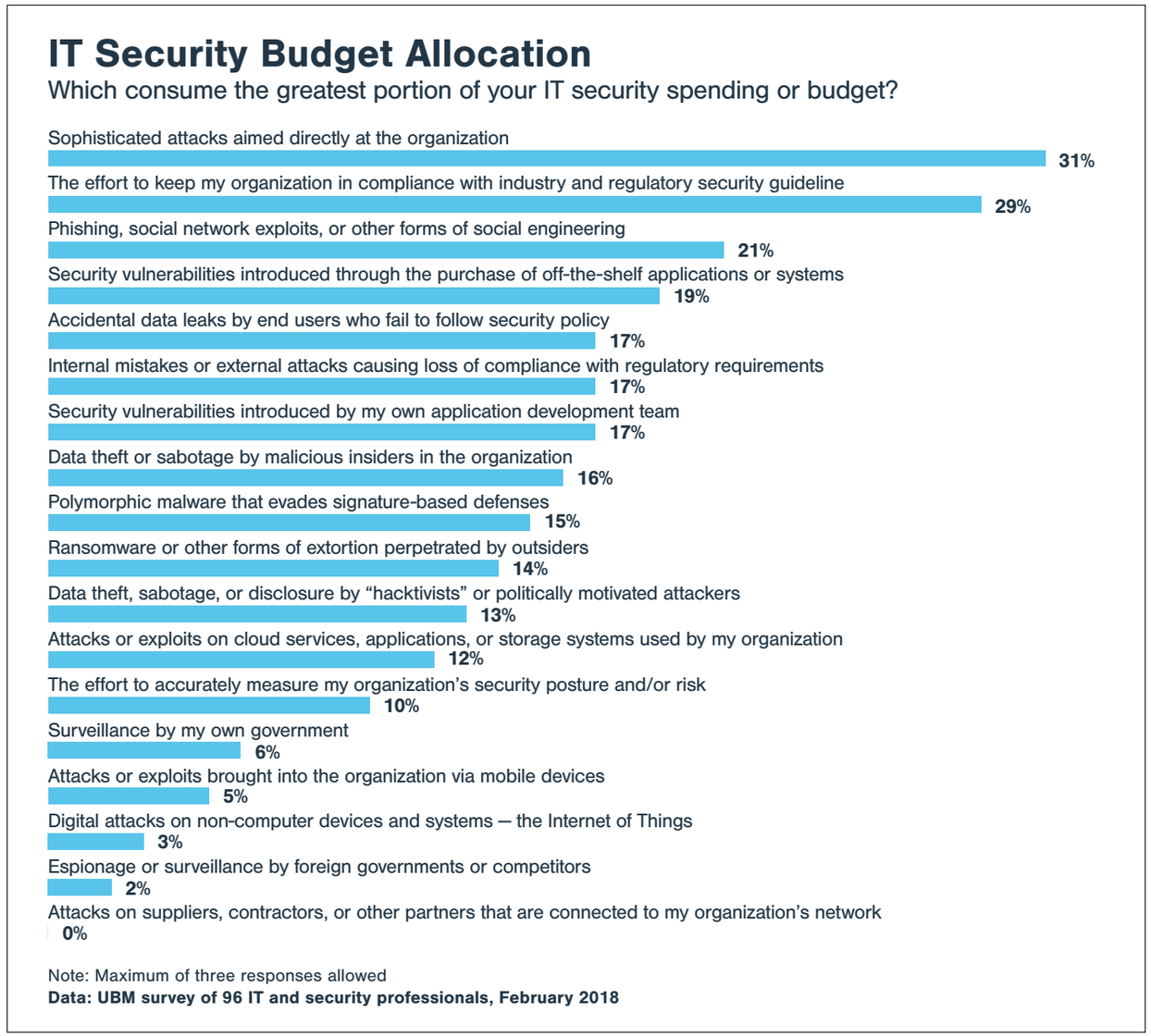

IT Security Budget Allocation
Which consume the greatest portion of your IT security spending or budget?
Sophisticated attacks aimed directly at the organization
31%
The effort to keep my organization in compliance with industry and regulatory security guideline
29%
Phishing, social network exploits, or other forms of social engineering
21%
Security vulnerabilities introduced through the purchase of off-the-shelf applications or systems
19%
Accidental data leaks by end users who fail to follow security policy
17%
Internal mistakes or external attacks causing loss of compliance with regulatory requirements
17%
Security vulnerabilities introduced by my own application development team
17%
Data theft or sabotage by malicious insiders in the organization
16%
Polymorphic malware that evades signature-based defenses
15%
Ransomware or other forms of extortion perpetrated by outsiders
14%
Data theft, sabotage, or disclosure by “hacktivists” or politically motivated attackers
13%
Attacks or exploits on cloud services, applications, or storage systems used by my organization
12%
The effort to accurately measure my organization’s security posture and/or risk
10%
Surveillance by my own government
6%
Attacks or exploits brought into the organization via mobile devices
5%
Digital attacks on non-computer devices and systems — the Internet of Things
3%
Espionage or surveillance by foreign governments or competitors
2%
Attacks on suppliers, contractors, or other partners that are connected to my organization’s network
0%
Note: Maximum of three responses allowed
Data: UBM survey of 96 IT and security professionals, February 2018

Figure 18

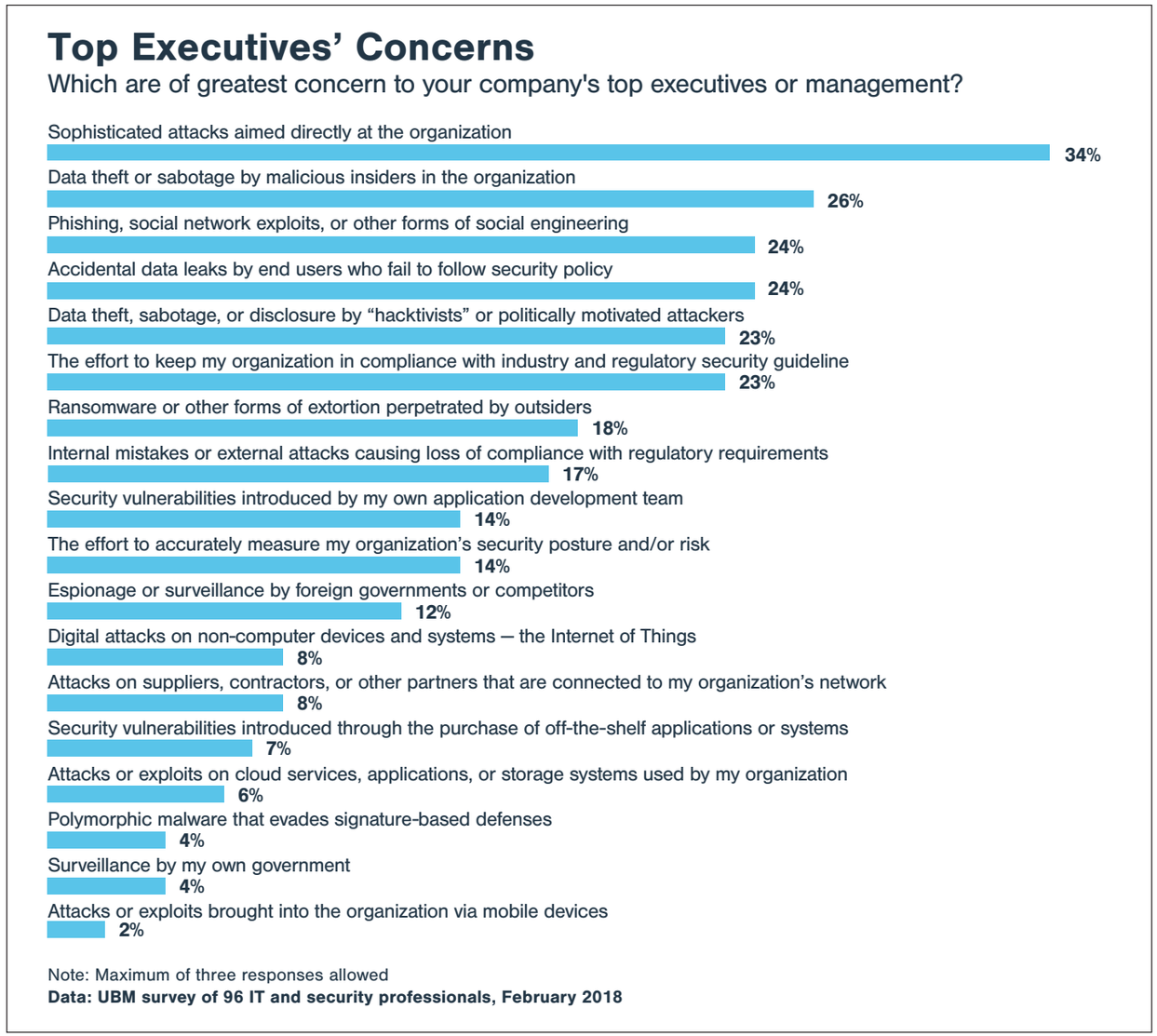

Top Executives' Concerns
Which are of greatest concern to your company's top executives or management?
Sophisticated attacks aimed directly at the organization
34%
Data theft or sabotage by malicious insiders in the organization
26%
Phishing, social network exploits, or other forms of social engineering
24%
Accidental data leaks by end users who fail to follow security policy
24%
Data theft, sabotage, or disclosure by "hacktivists" or politically motivated attackers
23%
The effort to keep my organization in compliance with industry and regulatory security guideline
23%
Ransomware or other forms of extortion perpetrated by outsiders
18%
Internal mistakes or external attacks causing loss of compliance with regulatory requirements
17%
Security vulnerabilities introduced by my own application development team
14%
The effort to accurately measure my organization's security posture and/or risk
14%
Espionage or surveillance by foreign governments or competitors
12%
Digital attacks on non-computer devices and systems – the Internet of Things
8%
Attacks on suppliers, contractors, or other partners that are connected to my organization's network
8%
Security vulnerabilities introduced through the purchase of off-the-shelf applications or systems
7%
Attacks or exploits on cloud services, applications, or storage systems used by my organization
6%
Polymorphic malware that evades signature-based defenses
4%
Surveillance by my own government
4%
Attacks or exploits brought into the organization via mobile devices
2%
Note: Maximum of three responses allowed
Data: UBM survey of 96 IT and security professionals, February 2018

Figure 19

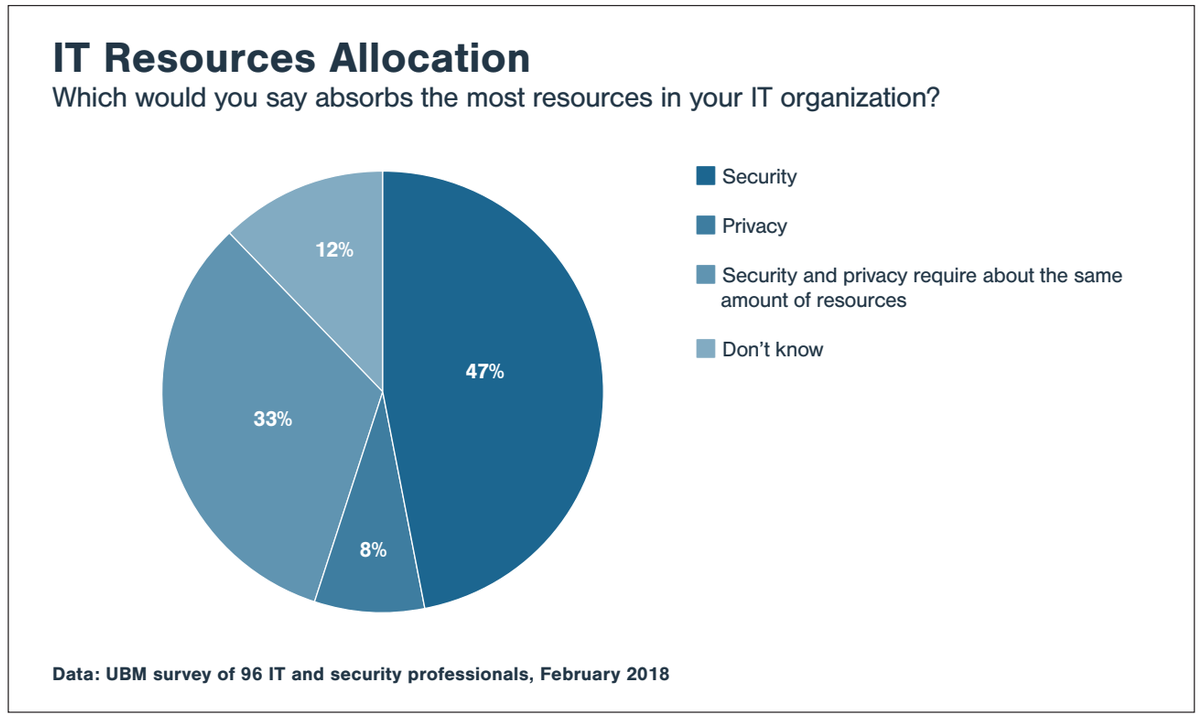

IT Resources Allocation
Which would you say absorbs the most resources in your IT organization?
47%
8%
33%
12%
Security
Privacy
Security and privacy require about the same amount of resources
Don't know
Data: UBM survey of 96 IT and security professionals, February 2018

Figure 20

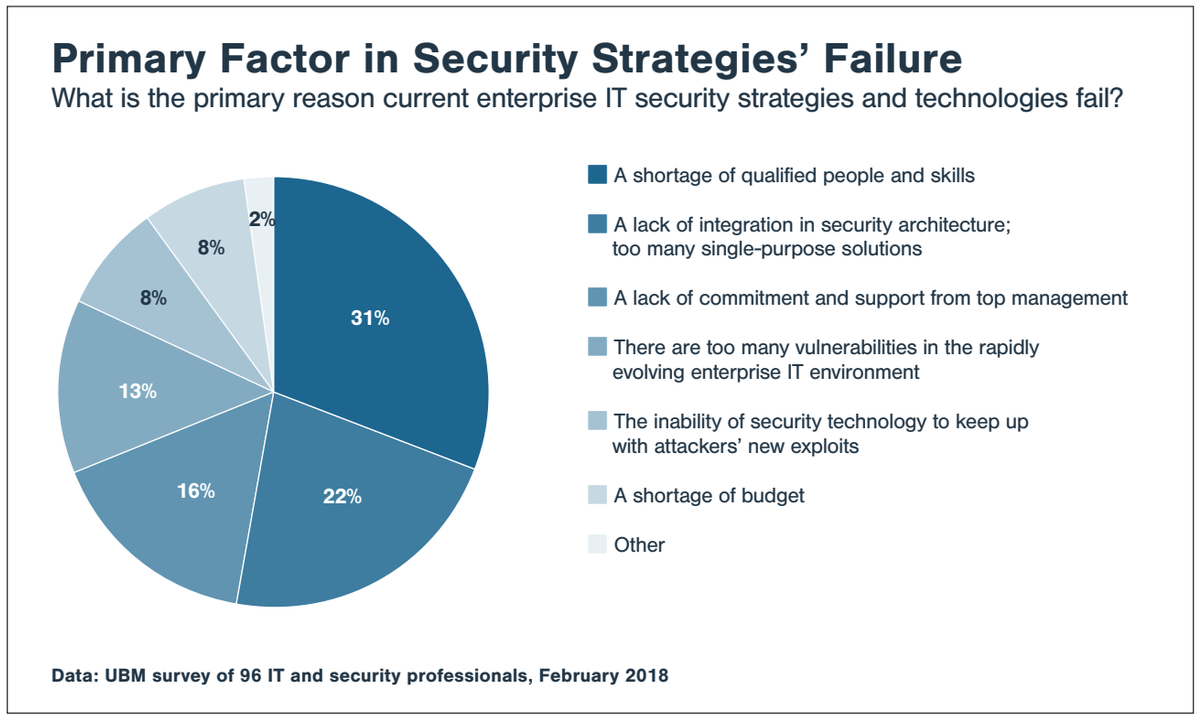

Primary Factor in Security Strategies' Failure
What is the primary reason current enterprise IT security strategies and technologies fail?
31%
22%
16%
13%
8%
8%
2%
A shortage of qualified people and skills
A lack of integration in security architecture; too many single-purpose solutions
A lack of commitment and support from top management
There are too many vulnerabilities in the rapidly evolving enterprise IT environment
The inability of security technology to keep up with attackers' new exploits
A shortage of budget
Other
Data: UBM survey of 96 IT and security professionals, February 2018

Figure 21

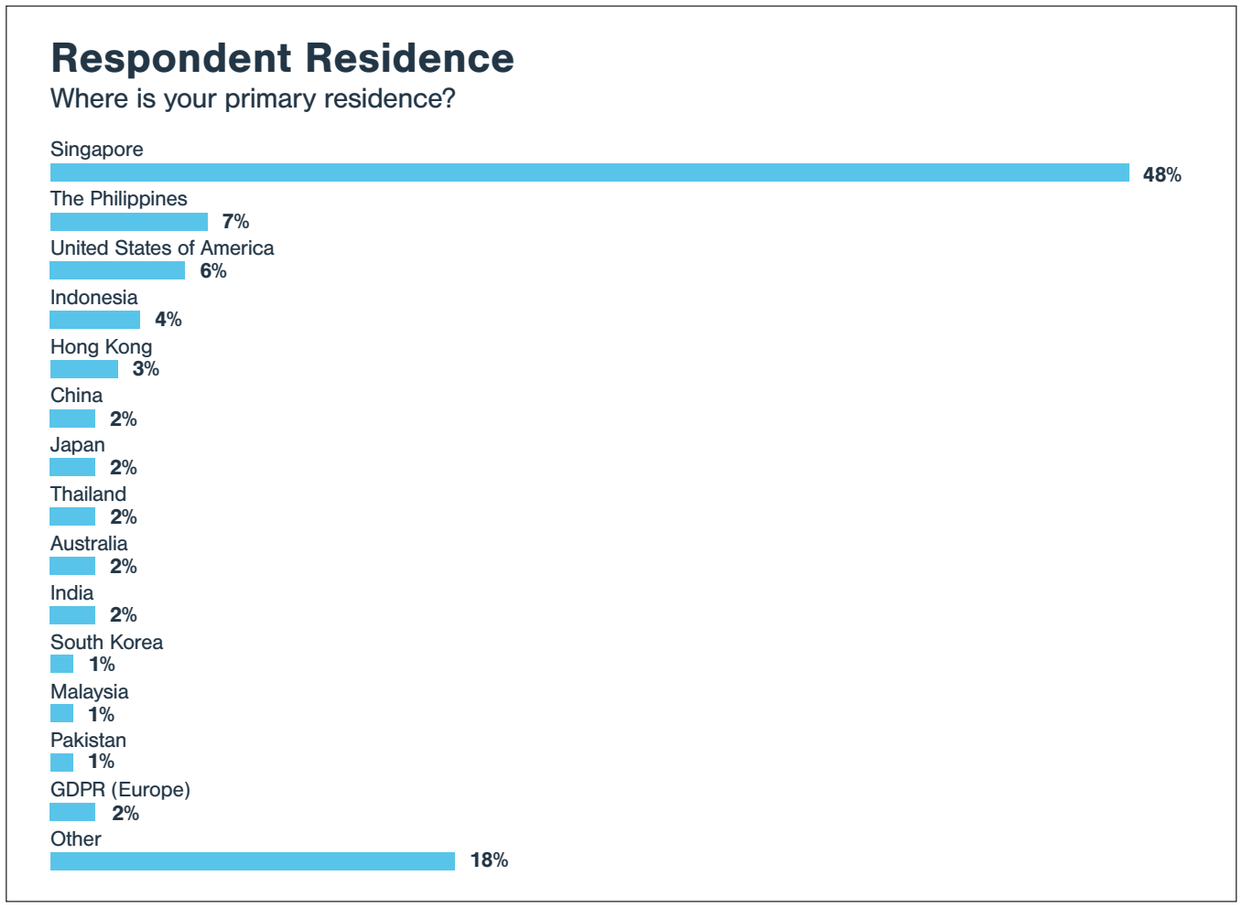

Respondent Residence
Where is your primary residence?
Singapore 48%
The Philippines 7%
United States of America 6%
Indonesia 4%
Hong Kong 3%
China 2%
Japan 2%
Thailand 2%
Australia 2%
India 2%
South Korea 1%
Malaysia 1%
Pakistan 1%
GDPR (Europe) 2%
Other 18%

Figure 22

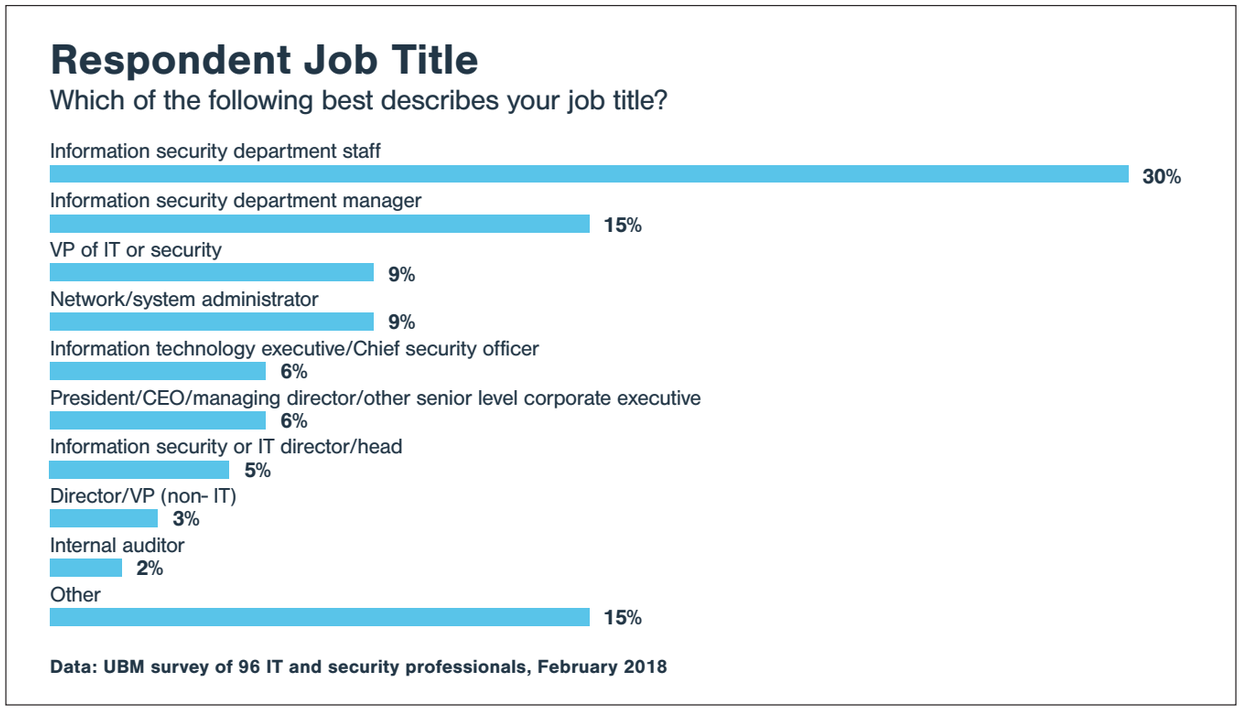

Respondent Job Title
Which of the following best describes your job title?
Information security department staff
30%
Information security department manager
15%
VP of IT or security
9%
Network/system administrator
9%
Information technology executive/Chief security officer
6%
President/CEO/managing director/other senior level corporate executive
6%
Information security or IT director/head
5%
Director/VP (non- IT)
3%
Internal auditor
2%
Other
15%
Data: UBM survey of 96 IT and security professionals, February 2018

Figure 23

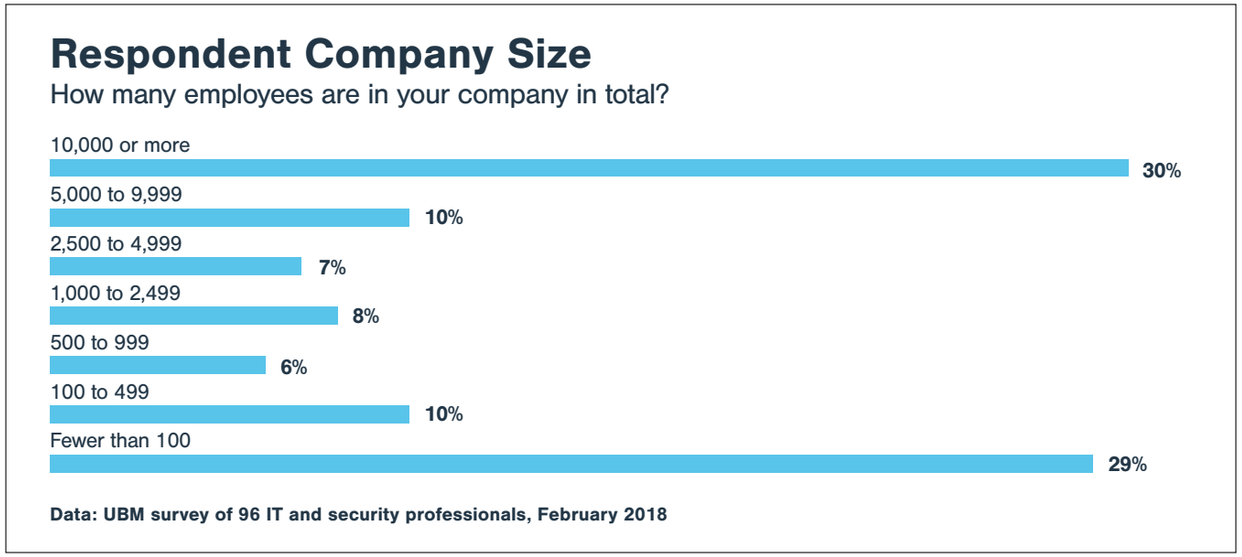
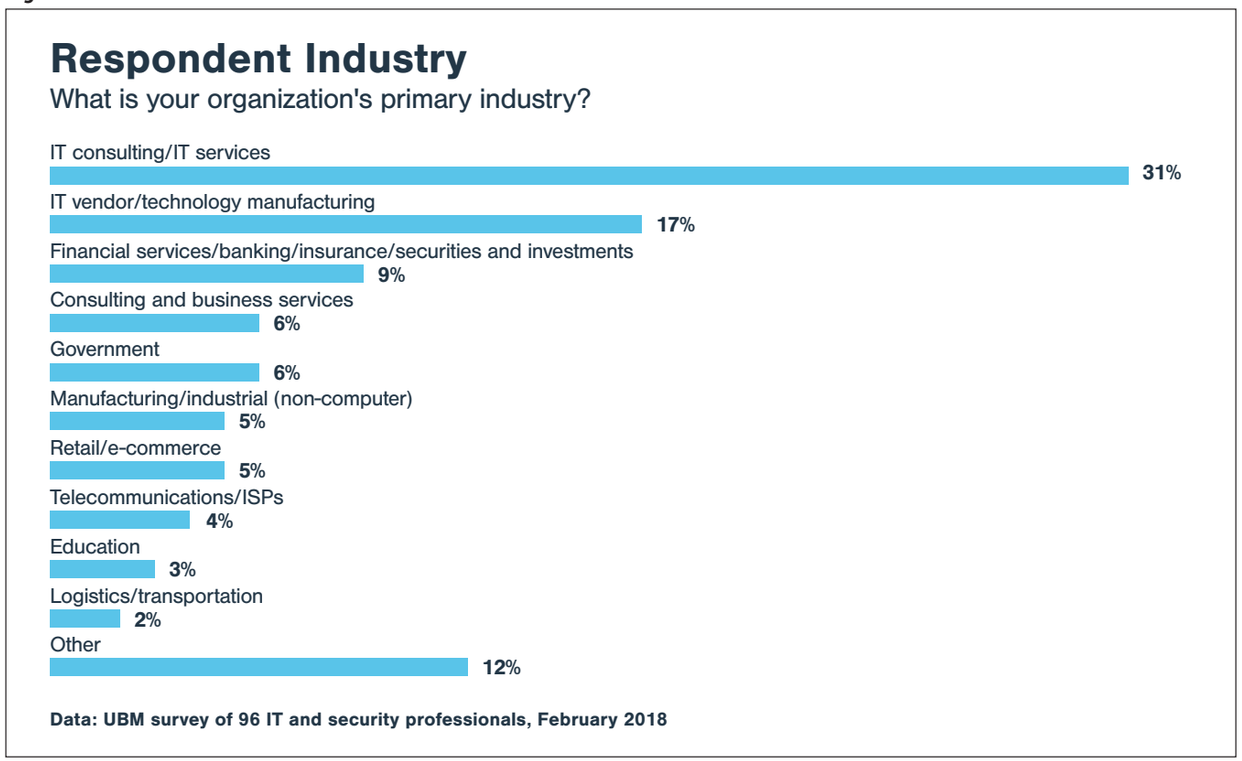

Respondent Company Size
How many employees are in your company in total?
10,000 or more
30%
5,000 to 9,999
10%
2,500 to 4,999
7%
1,000 to 2,499
8%
500 to 999
6%
100 to 499
10%
Fewer than 100
29%
Data: UBM survey of 96 IT and security professionals, February 2018

Figure 24


Respondent Industry
What is your organization's primary industry?
IT consulting/IT services
31%
IT vendor/technology manufacturing
17%
Financial services/banking/insurance/securities and investments
9%
Consulting and business services
6%
Government
6%
Manufacturing/industrial (non-computer)
5%
Retail/e-commerce
5%
Telecommunications/ISPs
4%
Education
3%
Logistics/transportation
2%
Other
12%
Data: UBM survey of 96 IT and security professionals, February 2018