LogRhythm
The Security Intelligence Company

2018 Cybersecurity: Perceptions & Practices

A Benchmark Survey of Security Professionals in the U.S., U.K., and Asia-Pacific Regions

Table of Contents

Foreword

James Carder

CISO & VP, LogRhythm Labs
LogRhythm

As uncertainties—cybersecurity and otherwise—swim around us with increased velocity and frequency, it's always helpful to hear directly from security leaders in the trenches of our industry. These first-hand accounts have the unique ability to shed light on the challenges security professionals and their teams face nearly every day of their work lives. That's precisely what this *"2018 Cybersecurity: Perceptions & Practices"* benchmark survey accomplishes. It provides insights into the state of the cybersecurity practice of 751 mid- to large-sized organizations in the United States, United Kingdom, and Asia-Pacific regions.

From these insights, one thing that comes as a surprise is data that suggests that the U.S. may not be leading the cybersecurity industry in security maturity. In fact, respondents from organizations in the Asia-Pacific region clearly indicate that they are far more likely to have a security operations center (SOC) than their U.S. and U.K. counterparts. The Asia-Pacific region also boasts the largest percentage of IT budget allocation toward cybersecurity. Both of these findings suggest a cultural prioritization toward security investments—one that isn't being matched by the U.S. or U.K.

When prompted on workflow/employee efficiency, it appears evident that security professionals are wasting huge amounts of time and effort on false positives and inefficient processes. Of course, this isn't news to us, but it's important to note how the data acutely quantifies this problem. The majority of IT executives indicate that the average cybersecurity professional wastes as much as 10 hours a week due to software inefficiencies. In an industry already plagued by a shortage in qualified specialists, this is a reality that is not only unacceptable, but also avoidable.

Containment of cyberthreats and breaches is a major challenge for all organizations. It takes time to understand the full scope of an incident and determine how best to neutralize it. This is exacerbated by a lack of resources (human, technology, intelligence) and then compounded when automation and orchestration are not efficiently leveraged to reduce the time necessary to complete the investigative processes.

Now, more than ever, security teams need to be working more intentionally. Corroboration and qualification using threat intelligence and other technologies help teams make informed decisions. Establishing automation and orchestration processes, protocols, and procedures for the most prevalent classes of attacks will improve the efficiency and effectiveness of most any SOC.

As security experts, it's unlikely our constant state of being stretched thin will be relieved anytime soon. But this survey does shine a ray of hope: the majority of IT executives surveyed believe their C-suite is paying more attention to cybersecurity efforts than they did last year. That, combined with the availability of NextGen SIEM and end-to-end security solutions today, gives me optimism that cybersecurity organizations across the globe may soon increase fortification in the fight against cyberthreats.

James Carder
CISO & VP, LogRhythm Labs

The Current State of Security Maturity

Many companies are focused on growing their security maturity – part of that growth is establishing a security operations center (SOC) within their organization. Special threat detection programs can be another indicator of security maturity. More than 70 percent of decision makers have programs in place to detect specific threats such as ransomware, insider or employee threats, and denial of service attacks. For those organizations that currently lack a formal SOC, most plan to add one within the next two years.

Team size is another important indicator, as it can provide insight into an organization's commitment to a well-staffed security program. In this survey, on average, respondents said they employ 12 cybersecurity professionals in their organization. More than half indicated that they employ 10 or fewer professionals on their teams. A huge majority of IT decision makers – 95 percent – use security software to prevent and react to threats. More than a quarter deploy more than 10 security software solutions to manage security threats.

Objective and Methodology

The purpose of this study was to determine the cybersecurity perceptions and practices among organizations in the United States, United Kingdom, and Asia-Pacific regions.

The results of this report are from an online survey of 751 IT decision makers who indicated that cybersecurity was part of their responsibilities. Of these respondents, 250 came from the United States, 250 from the United Kingdom, and 251 from the Asia-Pacific region. The Asia-Pacific region was represented by decision makers in Australia, Singapore, Hong Kong, and Malaysia.

These respondents indicated they were employed in mid- to large-sized companies (minimum 500+ employees).

Perceptions of Information Security

We established a wide perception of information security programs and initiatives among our surveyed IT decision makers. Our survey includes confidence levels in decision makers' ability to detect and respond to threats, their preferred security technologies, and some of the biggest challenges to a successful security program. **Mean time to detect (MTTD) and mean time to respond (MTTR)** are two primary metrics in assessing the success of any information security program.

Level of Security Confidence

When it comes to confidence levels, security decision makers indicated they are optimistic about protection; about half of them believe they are protected from external threats. Despite these levels of confidence, most of the other half of respondents believe that a determined hacker can still breach security measures that are in place. In fact, **more than one-third reported that their company has experienced a breach in the past year**—ranging from 29 percent in the United States to 39 percent in the Asia-Pacific region.

When specifically asked about confidence levels, these decision makers revealed that they are only moderately confident in their cybersecurity measures and abilities—suggesting an attitude that may be more hopeful than truly confident.

Most IT respondents—more than 60 percent—are only somewhat confident that their security software can detect all major breaches. They are only moderately confident that they can protect their companies from hackers.

In addition, the level of confidence in one's security also seemed to sway based on other variables, such as industry or the implementation of programs to target specific types of threats. For instance, **decision makers who did not report having programs to protect against threats such as ransomware, insider threats, and service denial attacks are less confident in their security programs.** That same segment reported slower rates of detection, response, and containment. IT decision makers in manufacturing also reported feeling more vulnerable than in other industries.

Ability to Respond to Cyberthreats

There are many factors that enable a SOC to quickly detect and respond to an incident, including technology, process, programs, and people. When it comes to technology, **a strong majority—nearly 80 percent—of respondents said that a platform for security management, analysis, and response is beneficial, though only about a third rate such a platform as very beneficial.** This response may reinforce the thought that true security confidence cannot be created with technology alone.

The metrics of MTTD and MTTR to a cybersecurity incident are two of the strongest indicators of the readiness and success of a security program. However, **less than half of surveyed respondents indicated that their team is able to detect a major cybersecurity incident within one hour**. When comparing the amount of time it takes to detect an incident versus the time it takes to respond to one, there are minor differences. Conversely, when examining the time required to contain an incident, there was a noticeable drop.

Overall, respondents indicated their organizations are far less likely to contain a major incident in one hour.

When asked to consider how their organization is operating from an end-to-end approach that includes discovery, qualification, neutralization, and recovery from cyberattacks, the respondents reported that they need help on virtually all stages within this framework.

The Challenges Facing Today's Security Teams

When asked about the biggest challenge in detecting and responding to cyberthreats, there is no clear smoking gun. IT decision makers are equally likely to cite the lack of cybersecurity skills, qualified manpower, ineffective software, lack of funding, and insufficient or undefined processes. They are also divided about which security technologies are most valuable, citing firewalls, network security, and security information and event management (SIEM) to about the same degree.

As decision makers are planning for the future and establishing ways to further protect their organizations, there are many things to consider. These decision makers need to carefully plan their budgets and strategies (with what they sometimes deem to be limited resources) to carry out strategies and deploy technologies to stay ahead of cyberattacks. They also must consider the development of programs to tackle specific threats that may put their organizations at risk.

One such threat is the insider or user threat. **Most decision makers—nearly 60 percent—indicate that they expect insider threats to increase over the next year. Less than 10 percent indicate that they expect insider threats to decrease.** Decision makers whose organizations had experienced a breach in the past year held the opinion that insider threats would increase, as did those who are currently using artificial intelligence (AI) or machine learning (ML) as part of their technology stack.

When it comes to budget, the percentage allocated to security from the overall IT budget is often on the lower side. Overall, one-third of respondents allocate 10 percent or less of their IT budget to security. Regionally, the U.S. had the lowest rate, and Asia-Pacific companies the highest. When asked about their comfort level of security funding, decision makers indicated they are moderately comfortable with their companies' level of security funding; however, nearly a quarter indicated they are not comfortable. From a regional perspective, those in the U.S. were less likely to think the level of their security funding is appropriate.

Cybersecurity Team Resources

About 40 percent of IT decision makers employ larger cybersecurity teams of 11 or more professionals, while about half have 10 or fewer.

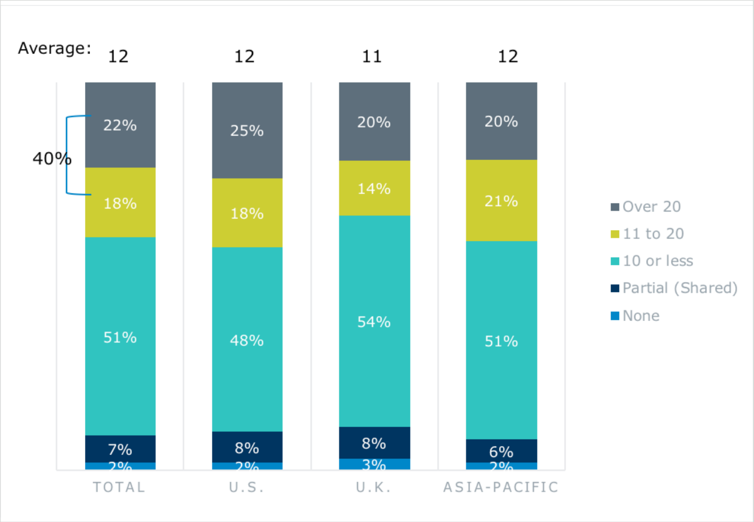


Figure 1. Number of Cybersecurity Professionals Employed

Finance and technology companies are most likely to have more than 10 cybersecurity professionals: 59 percent and 60 percent respectively, vs. 40 percent overall.

Companies that have experienced a breach, and those using AI, tend to have more cybersecurity professionals on staff.

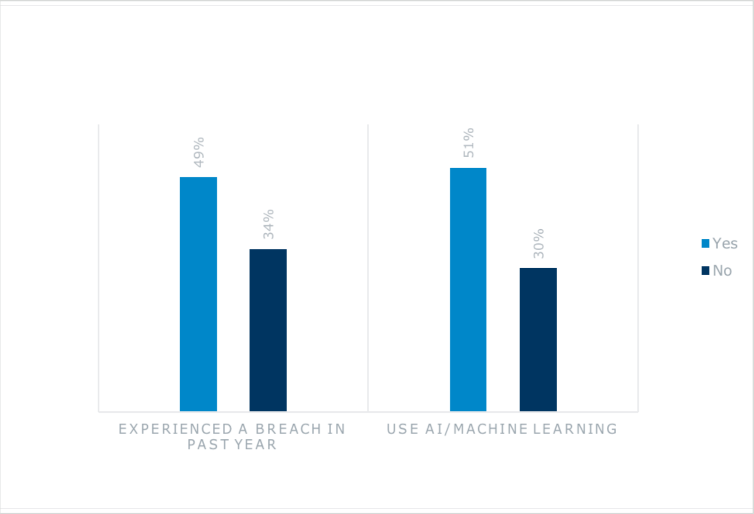


Figure 2. Percent of Organizations with 10 or More Cybersecurity Professionals Employed

About half of decision makers claim to use the highest level of prevention to stop breaches and are optimistic about protection. Most of the others, however, think that determined hackers can still breach security.

Detailed Findings

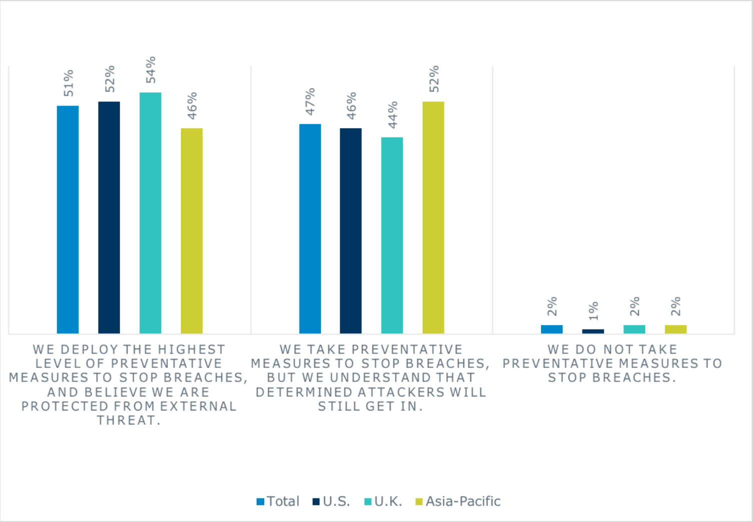


Figure 3.
How Organizations Currently Measure Approaches to Stop Breaches

IT decision makers in larger companies (10,000+ employees) are more likely to use the highest level of prevention and are confident they are protected: 61 percent, vs. 51 percent overall.

Most decision makers say their organization has a SOC. Asia-Pacific companies are more likely, and U.S. companies are less likely to have a SOC.

KEY CHART

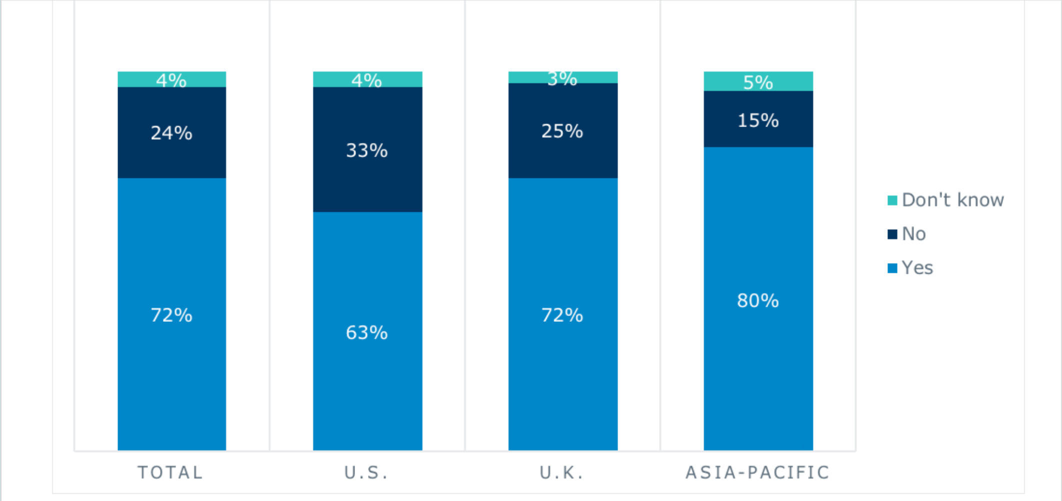


Figure 4. Organizations with a SOC

Among IT decision makers whose companies lack a SOC, most plan to create one within the next two years. Decision makers in the Asia-Pacific region are most likely to act in this timeframe.

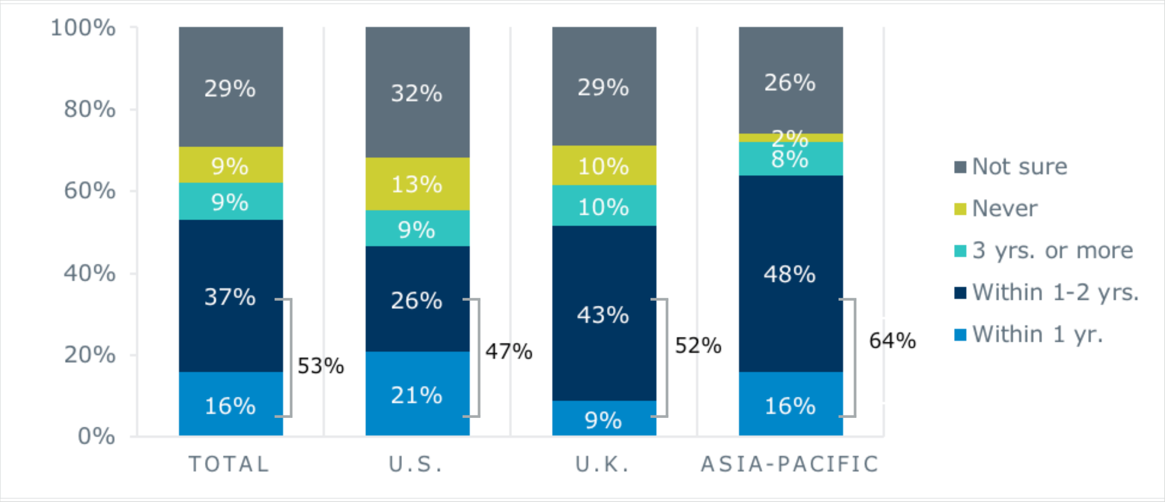


Figure 5. Timeframe in Which Organizations Without a SOC Plan to Open One

Detailed Findings

On average, 95 percent of respondents use security software to prevent and react to threats. More than one quarter of decision makers deploy more than 10 security software solutions to manage security threats. About 40 percent use five or less.

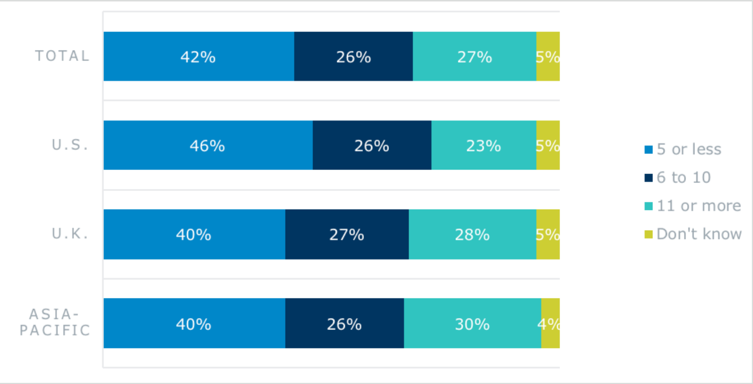


Figure 6. Number of Security Software Solutions Organizations Deploy

Less than half of respondents say their team detects a major cybersecurity incident with an hour.

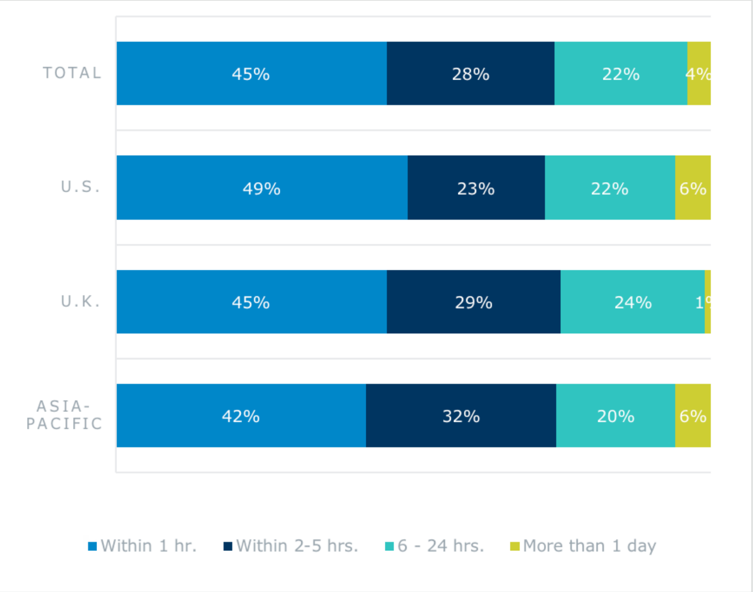


Figure 7. Average Time to Detect a Major Cybersecurity Incident

Comparing the amount of time it takes organizations to detect vs. respond to a major incident shows relatively minor differences.

However, there is a big drop when it comes to the time required to contain threats. These companies, overall and in each region, are far less likely to contain major incidents within the first hour.

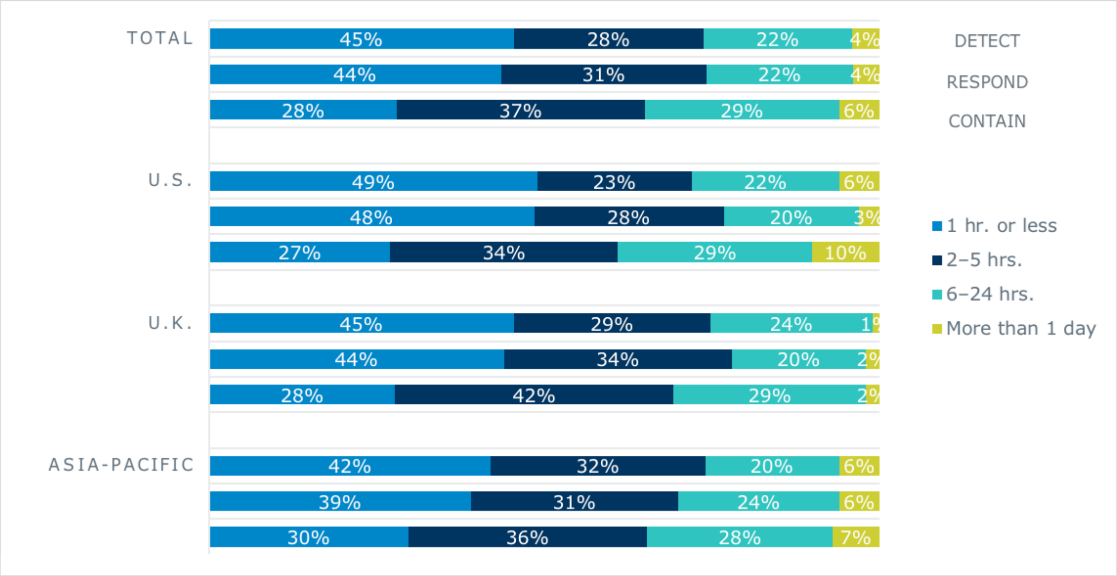


Figure 8. Comparing the Time to Contain a Major Incident

Most respondents who say it takes longer (2+ hours) to detect an incident are decision makers who report that they do not have a SOC (61 percent) or do not have a formal program to protect against ransomware (64 percent), insider threats (68 percent), and denial of service attacks (71 percent).

Detailed Findings

For those in the Asia-Pacific region, the drop in the rate of detection/response/containment in the first hour is slightly lower than for the U.S. and the U.K.

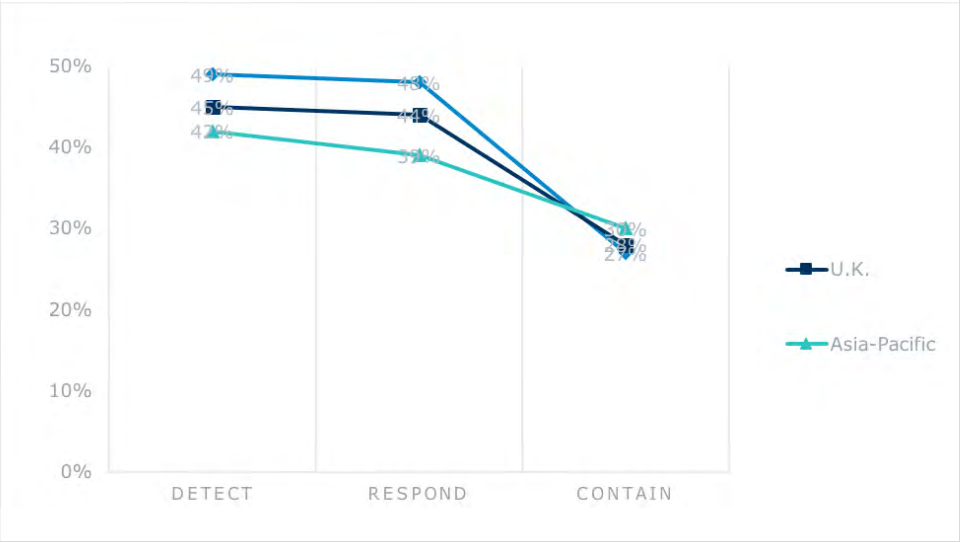


Figure 9. Average Percentage of Those Able to Detect, Respond, and Contain a Major Cybersecurity Incident within the First Hour

KEY CHART

Most decision makers – more than 60 percent – are only moderately confident that their security software can detect all major breaches.

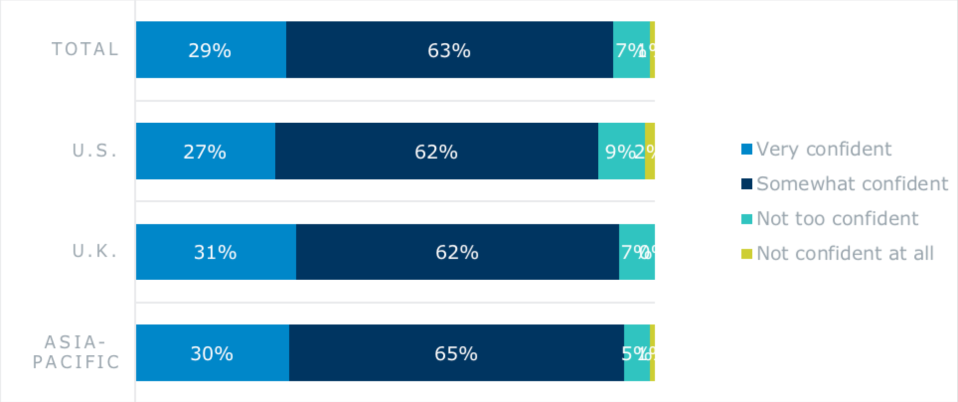


Figure 10. Confidence Level of Ability to Detect ALL Major Breaches with Security Software

Similarly, these decision makers are only moderately confident that they can protect their company from hackers.

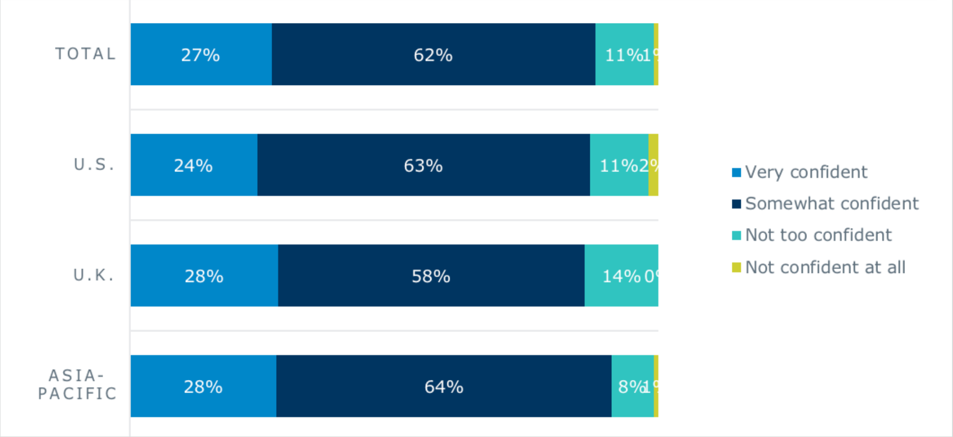


Figure 11. Confidence Level that Organization Can Stay Ahead of Attackers

Decision makers who expressed less confidence in their ability to stay ahead of attackers include executives in manufacturing and those with Telecom titles, as well as those who lack AI and formal programs to protect against ransomware, insider threats, and denial of service attacks.

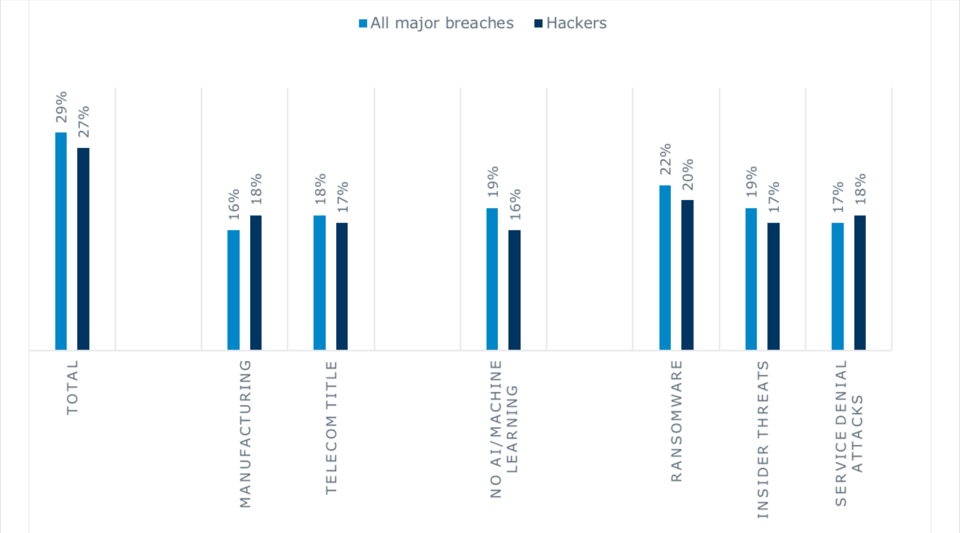


Figure 12. Percent of Those Who are "Very Confident" That Their Company is Protected Against All Major Breaches and Hackers

Detailed Findings

Decision makers are divided in their perceptions of the major challenge to detecting cybersecurity threats.

	Total	U.S.	U.K.	Asia-Pacific
Lack of staff cybersecurity skills	**22 percent**	20 percent	**23 percent**	**24 percent**
Ineffective security software	21 percent	21 percent	**23 percent**	18 percent
Lack of funding and resources	19 percent	**21 percent**	16 percent	20 percent
Insufficient processes or undefined workflows	19 percent	18 percent	19 percent	19 percent
Lack of manpower to monitor threats	18 percent	17 percent	18 percent	20 percent
Other	2 percent	4 percent	2 percent	0 percent

Table 1. The Biggest Challenge to Detecting Cyberthreats

Similarly, no single security technology emerged as most valuable. Firewalls, network security, and SIEM are about equally rated as most valuable.

	Total	U.S.	U.K.	Asia-Pacific
Firewalls	**27 percent**	**26 percent**	**29 percent**	25 percent
Network security	26 percent	25 percent	28 percent	**26 percent**
Security information and event management (SIEM)	23 percent	25 percent	23 percent	21 percent
Endpoint security	17 percent	18 percent	14 percent	19 percent
IDS	6 percent	5 percent	4 percent	10 percent
Other	1 percent	*	1 percent	0 percent

Table 2. Security Technologies That Decision Makers Find the Most Value

Threat Lifecycle Management Defined

Threat Lifecycle Management (TLM) is a framework that puts security teams a step ahead of attackers by providing an end-to-end security workflow that combines people, process, and technology. TLM empowers teams by sorting through the noise to highlight and investigate high-priority threats.

This series of aligned SecOps capabilities begins with the ability to "see" broadly and deeply across an IT environment and ends with the ability to quickly mitigate and recover from a security incident.

Far and away, IT decision makers define "Threat Lifecycle Management" holistically, as an approach involving discovery, qualification, neutralization, and recovery from cyberattacks.

Decision makers think they need help on nearly all stages of Threat Lifecycle Management, especially detecting, neutralizing, investigating, and recovering from cyberthreats.

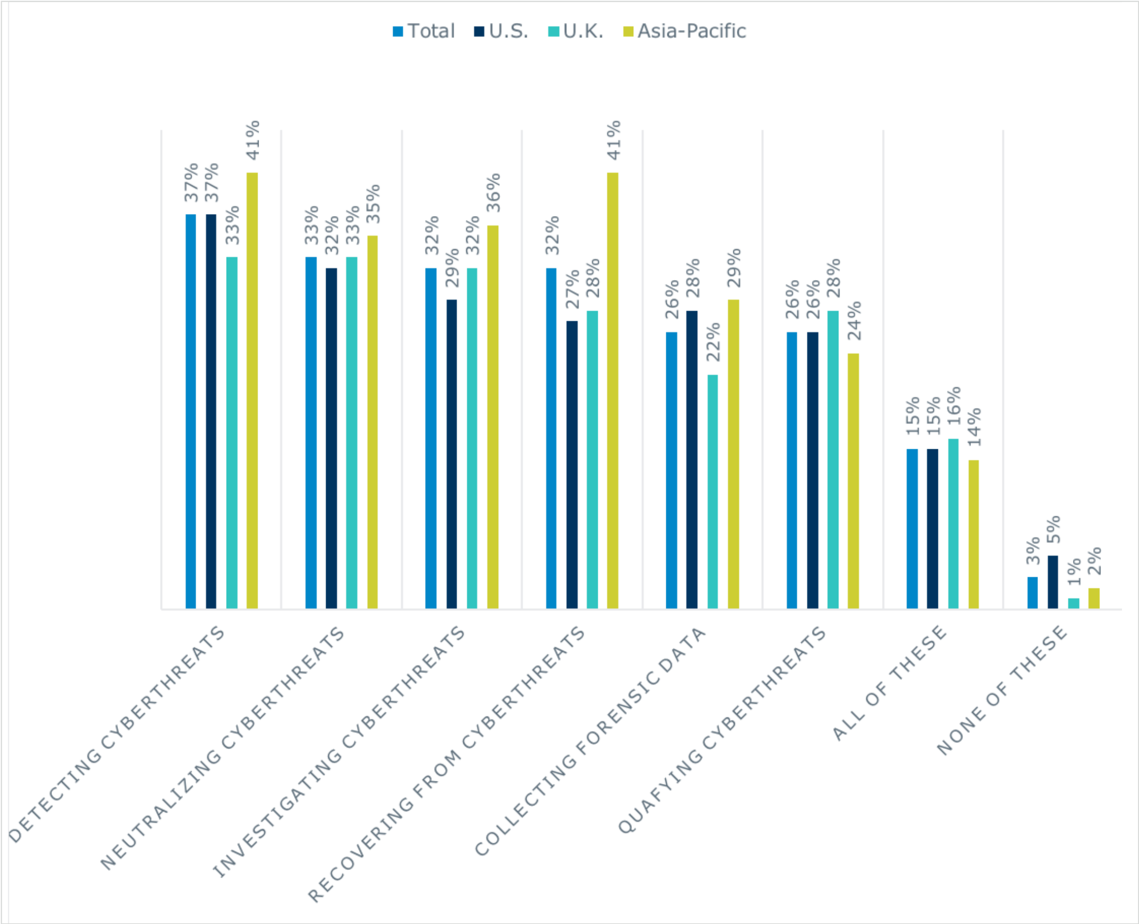


Figure 13. Threat Lifecycle Management Stages Where Decision Makes Indicate They Need Help

Detailed Findings

Roughly six out of 10 decision makers expect insider or employee threats to increase over the next year, while another third expect the level to stay constant. Only seven percent expect any decrease.

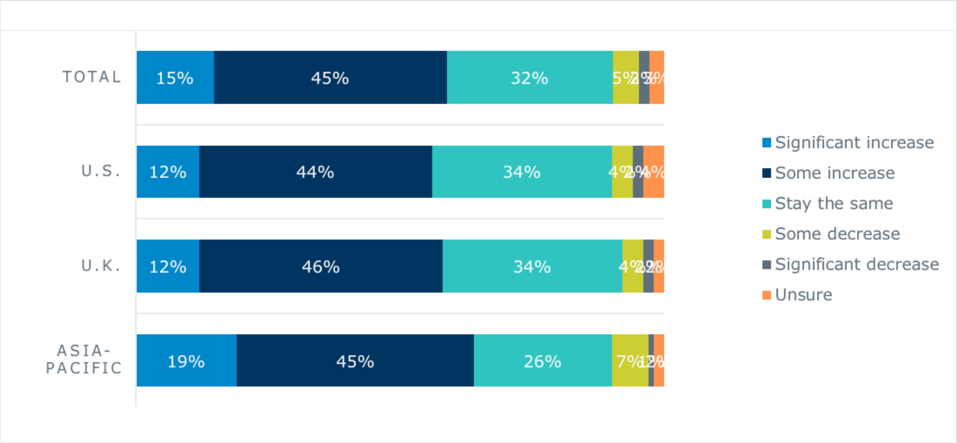


Figure 14. Anticipated Insider/Employee Threats in the Coming Year

Those decision makers who experienced a breach in the past year were 70 percent more likely to expect an increase in insider threats. Those who report that they are currently using AI as part of their security strategy are 70 percent more likely to expect an increase.

More than 70 percent of decision makers have programs to respond to ransomware, insider threats, and denial of services attacks.

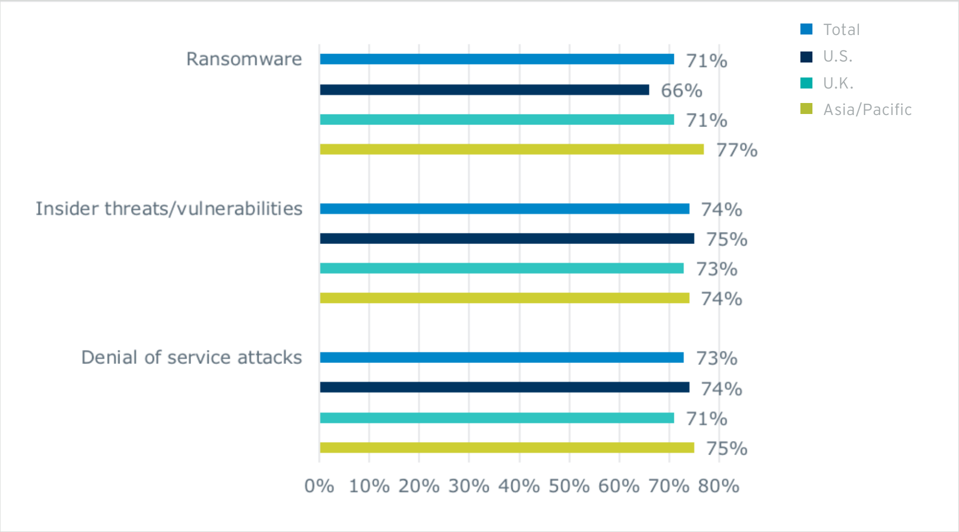


Figure 15. Organizations That Have Formal Programs in Place to Address Ransomware, Insider Threats, and Denial of Service Attacks

KEY CHART

Overall, a third of these decision makers allocate 10 percent or less of their IT budget to security. There is considerable variation by region, with the U.S. directing the lowest proportion of its IT budget to security, and Asia-Pacific companies the greatest.

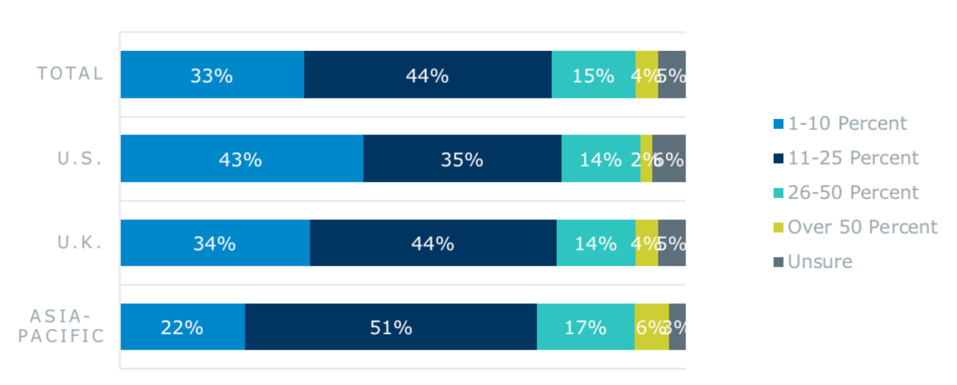


Figure 16. Percentage of IT Budget Directed Toward Security

About three-quarters of survey respondents think their C-suite is paying more attention to cybersecurity issues compared to the previous year—though many think it's only slightly more.

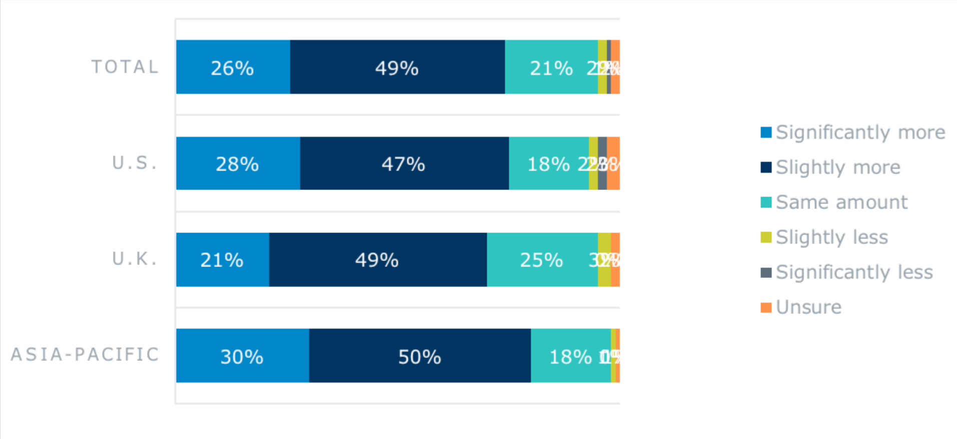


Figure 17. C-Suite Attention on Cybersecurity issues Compared to the Previous Year

	Total	U.S.	U.K.	Asia-Pacific
Loss of brand reputation	**29 percent**	**27 percent**	**31 percent**	**30 percent**
Loss of individual reputation/job security	23 percent	23 percent	26 percent	20 percent
Loss of customers	19 percent	16 percent	18 percent	22 percent
Negative news	16 percent	19 percent	11 percent	16 percent
Stock drop	13 percent	13 percent	14 percent	12 percent
Other	1 percent	2 percent	*	*

* Less than 5 percent

Table 3. Trigger Most Likely to Make Senior Executives/C-Suite Care More About Cybersecurity

More than a third of IT decision makers say their company was hit by a breach in the past year – ranging from 29 percent in the U.S. to 39 percent in Asia-Pacific.

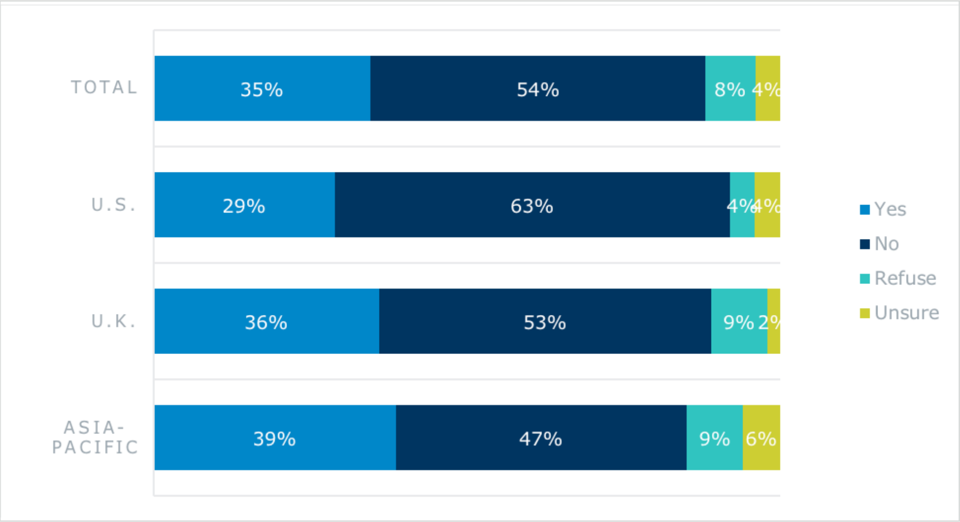


Figure 18. Organizations Reporting a Breach in the Past Year

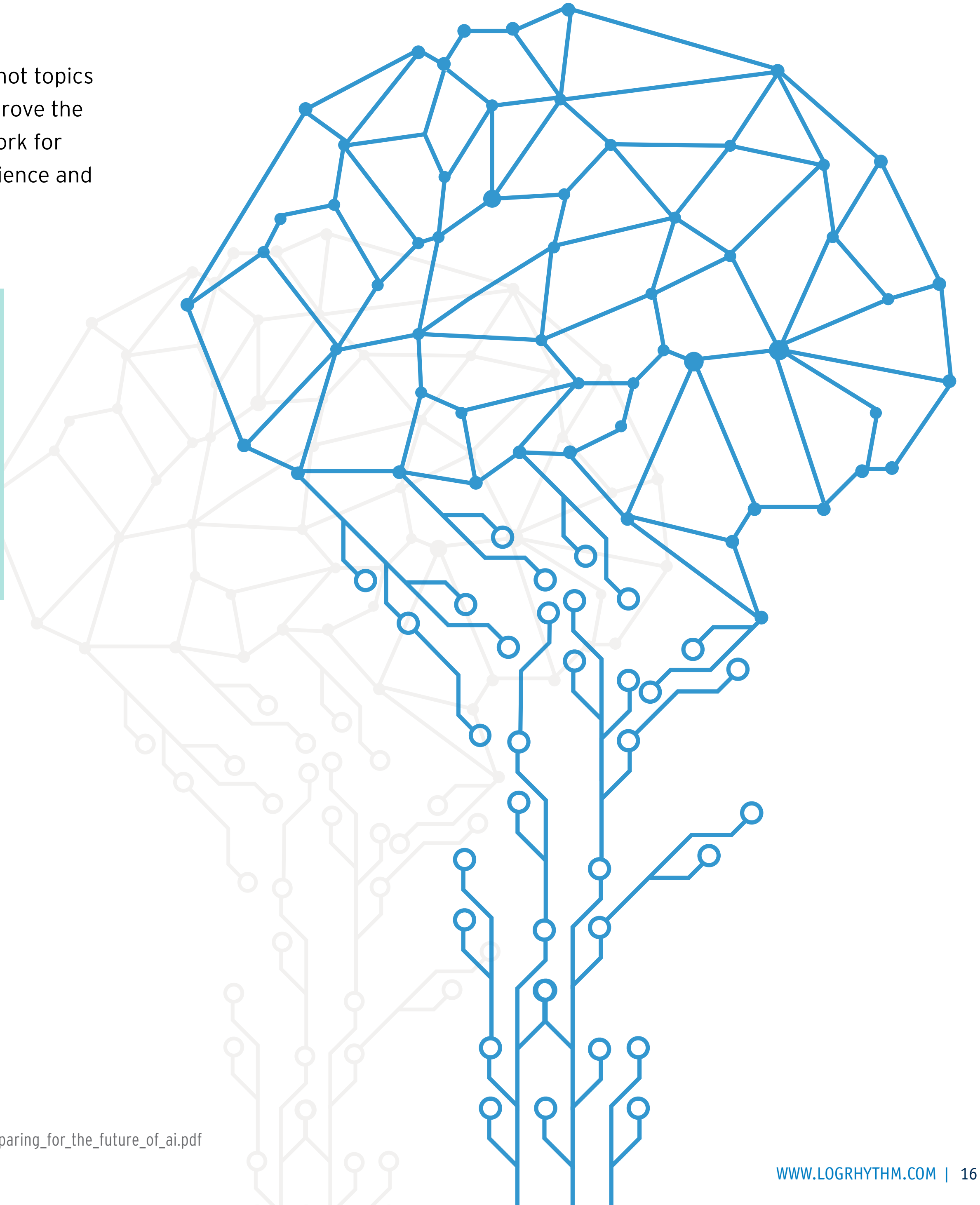
Decision makers in government were the most likely to have suffered a breach (48 percent vs. 35 percent total).

More than a third of IT decision makers say their company was hit by a breach in 2017

The Promise of Artificial Intelligence

Artificial intelligence (AI) and machine learning (ML) have become hot topics in the cybersecurity world. With them comes much promise: to improve the speed to detect threats, as well as to relieve some of the manual work for overwhelmed security teams. A recent report from the National Science and Technology Council (NSTC) stated:

> *"Using AI may help maintain the rapid response required to detect and react to the landscape of ever-evolving cyberthreats. There are many opportunities for AI, and specifically machine learning systems, to help cope with the sheer complexity of cyberspace and support effective human decision making in response to cyberattacks."*[1]



[1] https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

So why have AI and ML become such darlings in the security space?

One reason is that IT security teams are working inefficiently, and the prospect of improving workflow is exciting. More than one-third of those surveyed said they and their team spend at least three hours a day on tasks that could be handled by better software. And **most think that the average cybersecurity professional wastes as much as 10 hours a week due to software inefficiencies.** These teams are dealing with an average of 113 false positives every week – causing them to spend much of their time manually investigating threats that aren't there. This is a huge problem in a landscape that cites a lack of skilled resources.

This paradigm may speak to why so many information security decision makers are looking to AI and ML for the answer. Just under half of respondents indicated they are currently using AI in their security programs. Decision makers in the U.S. are the least likely to incorporate AI into their security programs, and those in the Asia-Pacific region are the most likely to use AI.

The Use Case for AI and ML in Security

Many in the cybersecurity world are turning to AI/ML in order to combat the threat of insider-based threats. However, when surveyed, only 55 percent of respondents considered insider or employee attacks to be a dangerous cybersecurity threat, and just 14 percent viewed these attacks as very dangerous. About one in eight respondents didn't see these attacks as a threat at all.

The Reality of Applying AI/ML to Security

When considering the movement of cybersecurity to the cloud for AI/ML applications, most decision makers are looking for faster threat detection. But, when investigating threats, decision makers indicate that their teams are still taking a group discussion approach to analyze and prioritize threats instead of relying heavily on automation (although they often use software in combination with this approach).

In fact, nearly a third of the respondents indicated that the one feature they would consider most critical for better cybersecurity software is the collaboration and integration with critical technologies. Twenty-two percent cited advanced machine learning to detect threats more efficiently as most critical. This response may indicate that, while employing AI/ML is a growing need, these teams more pressingly need software that helps to streamline processes and other technologies.

Looking Ahead to the Future of AI/ML

AI/ML will certainly have a critical role to play in the evolution of security technologies to help teams become more efficient and effective. When asked about what they think the major "game changer" for security will be in the next few years, survey respondents overall indicated that big data analytics will be primary, followed closely by AI. Regionally, however, decision makers in the U.S. (unlike those in the U.K. and Asia-Pacific) believe AI will make the greatest difference.

KEY CHART

More than one-third of decision makers say they and their teams spend at least three hours a day on tasks that could be handled by better software.

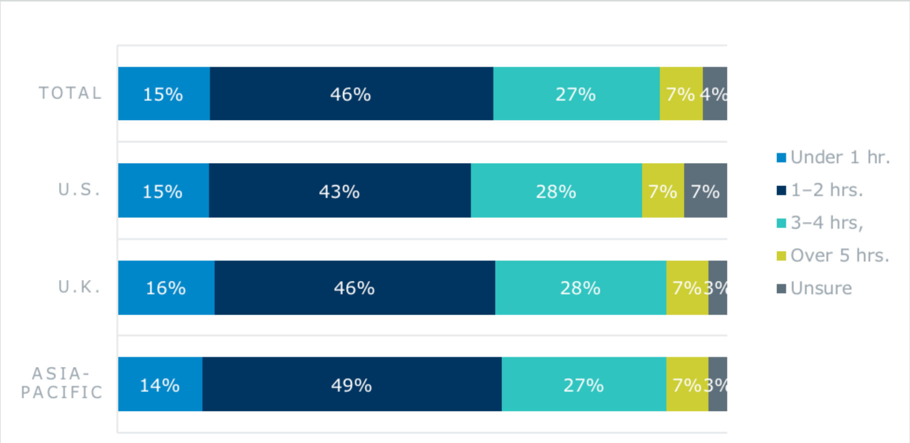


Figure 19. Amount of Time Spent by Security Teams on Mundane, Repetitive, and Administrative Tasks (e.g., Auditing and Assessing Systems, Reviewing Logs, Changing Control Processes, Scanning, and Patching Cycles) That Could Be Handled by More Sophisticated Software

Those in the professional services field reported being even more likely to spend more than three hours a day on these tasks (50 percent vs. 34 percent overall).

Nearly 30 percent of respondents said their team spends at least 11 hours a week manually searching for threats on their network.

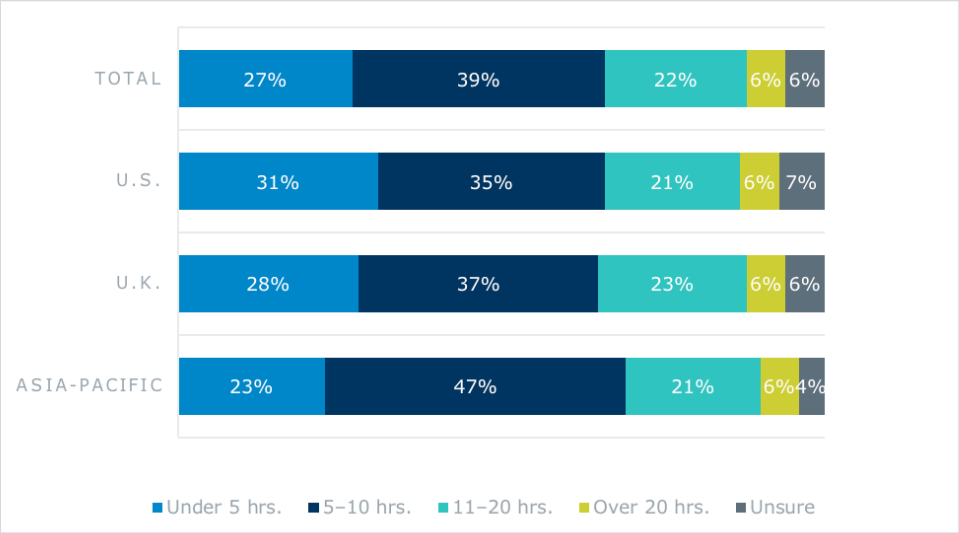


Figure 20. Amount of Time Security Teams Spend Manually Hunting for Threats on Their Network Each Week

Some groups stood out as spending more time than others. For example, those in the finance industry reported spending 10.6 hours per week on average, while those in the health care industry reported spending an average of 10.4 hours per week. In addition, **companies with annual revenues of $250M–$400M reported spending an average of 10.8 hours per week manually hunting for threats. Those who reported being hit by a breach in the last year averaged 10 hours per week.**

Artificial Intelligence in Security

Just 55 percent of respondents consider insider/employee attacks to be a dangerous cybersecurity threat. Only 14 percent view them as very dangerous. About one in eight (12 percent) do not see them as a threat.

KEY CHART

The majority of IT decision makers think the average cybersecurity professional wastes as much as 10 hours a week due to software inefficiencies.

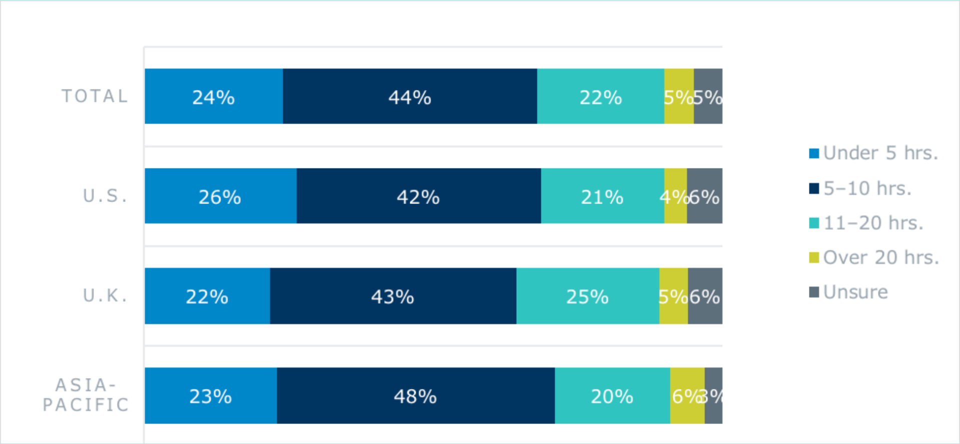


Figure 21. Time the Average Cybersecurity Professional Wastes Due to Software Inefficiencies in a Week

Decision makers in security must deal with an average of 113 false positives every week – ranging from 98 in the U.S. to 128 in the U.K.

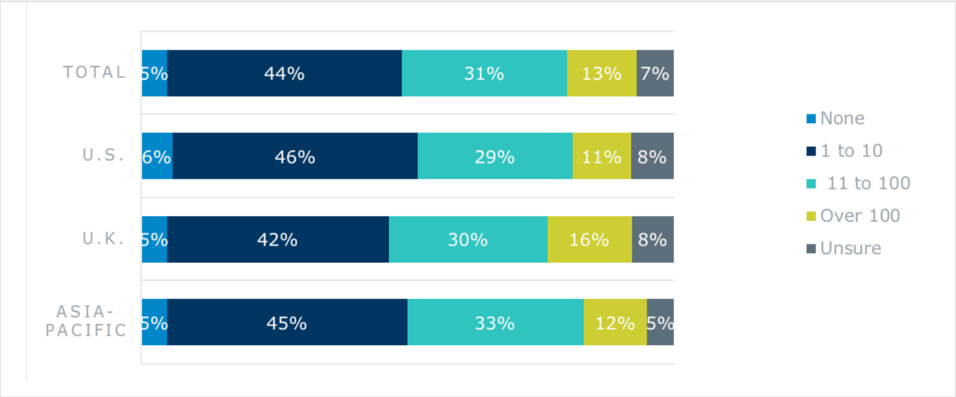


Figure 22. Average Number of False Positives Reported on a Weekly Basis

In addition to reducing the number of false positives, security solutions that integrate AI often help provide teams with a technological advantage over attackers. Decision makers were split in terms of their use of AI. Just under half use it – U.S. respondents are least likely to use AI. Those in the Asia-Pacific region are most likely.

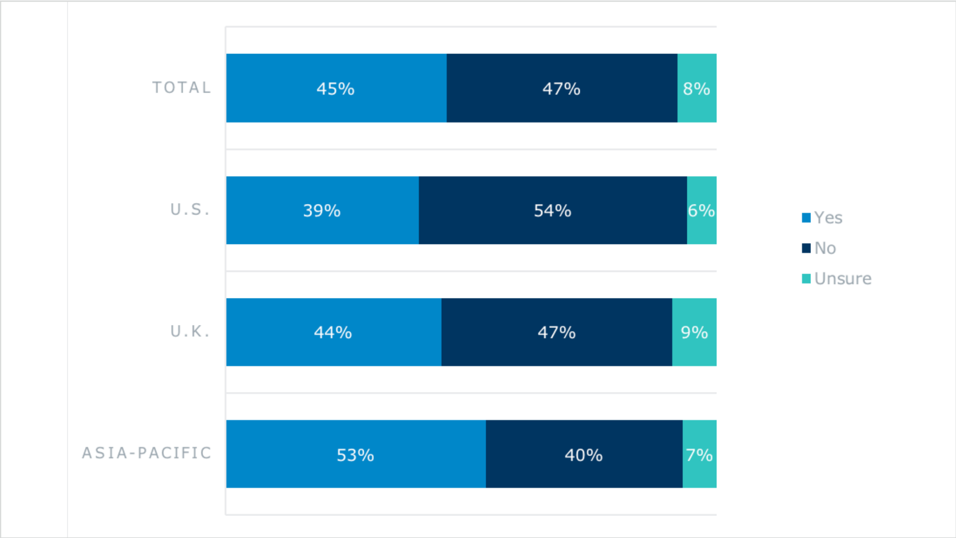


Figure 23. Decision Makers Using AI in Their Security Stack

In addition, those who were most likely to use AI included:

- Finance (56 percent) and health care (55 percent) vs. 45 percent overall
- Those who indicated that they have a SOC
- Those who indicated they are using more than five software solutions
- Those who reported that they have experienced a breach in the last five years

More than 90 percent of IT decision makers believe AI has made at least some improvement in the productivity of their cybersecurity operations. Just under one-third see a significant improvement. Respondents in the Asia-Pacific region are much more positive toward the benefits of AI than others.

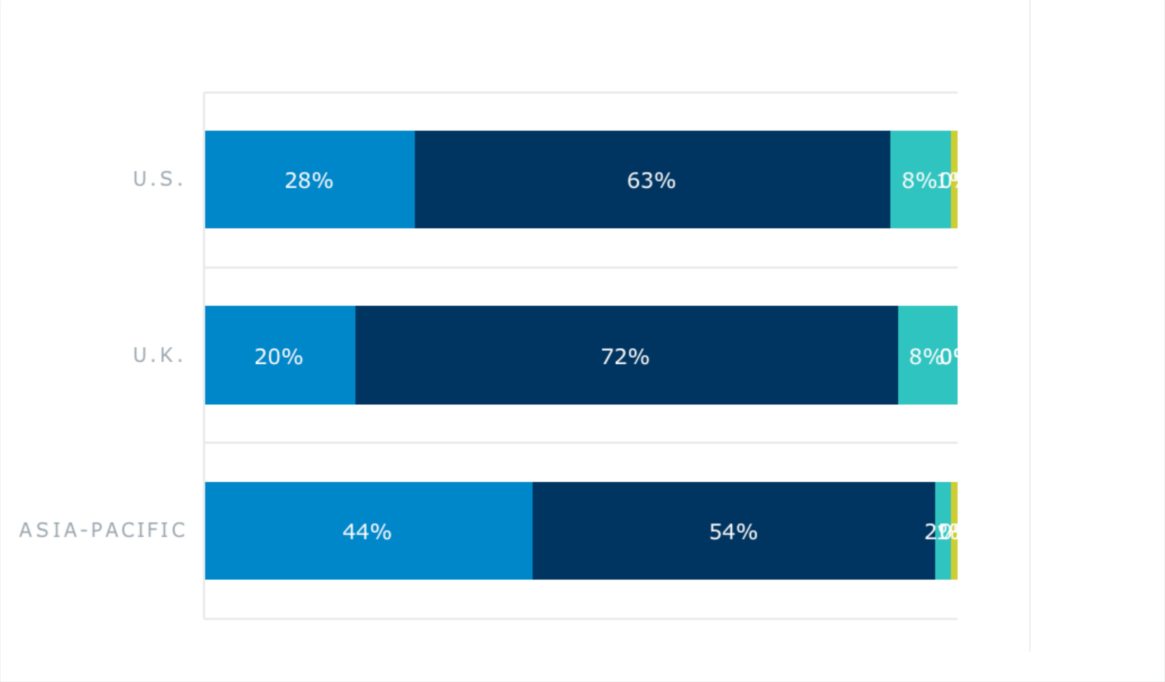


Figure 25. Level of Improvement AI or Machine Learning Has Made on Productivity of Operations (by region)

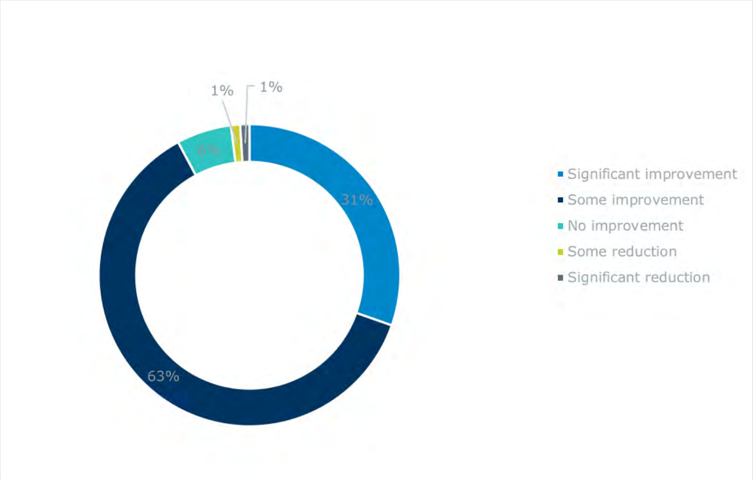


Figure 24. Level of Improvement AI/ML Has Made on Productivity of Operations

Conclusion

This survey provides us with valuable insight into the state of the cybersecurity practices and opinions of hundreds of mid- to large-sized organizations across the globe. From its findings, we're able to observe themes and trends across the security landscape that serve to provide a larger perspective on the biggest security-related challenges organizations face today.

More than one-third of respondents say they and their teams spend at least **three hours a day on tasks that could be handled by better software.** Meanwhile, more than 90 percent of these same respondents also report that they believe AI has made at least some improvement in the productivity of their cybersecurity operations. These report findings, when viewed together, reveal that when applied to security procedures, AI technologies can be instrumental in improving existing inefficiencies in security operations. With security professionals already stretched thin, improved productivity and streamlined operations are highly coveted necessities for IT executives.

With the exception of a few surprise results, this survey largely reinforced common perception that security teams across the board are experiencing a lack of resources – be it budget, personnel, or technological. Yet these shorthanded teams, tasked with defending an organization's entire cyber landscape, can overcome their inevitable shortcomings when equipped with the right tools and technologies that allow their analysts to work with more accuracy, collaboration, and comprehensive visibility. It's time to arm teams with the AI-enabled tools they need to succeed in the critical battle against persistent and damaging cyberthreats.

LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organizations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralizing damaging cyberthreats. The LogRhythm platform combines user and entity behavior analytics (UEBA), network traffic and behavior analytics (NTBA) and security automation & orchestration (SAO) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations center (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.

WIDMEYER COMMUNICATIONS
A FINNPARTNERS COMPANY

Widmeyer Communications

Widmeyer Communications, a Finn Partners Company, has an in-house research and polling practice. The firm has a guiding philosophy that clients gain knowledge and perspective when projects are informed by quantitative and qualitative research. The value added to projects with a research component along with a robust digital research practice helps to differentiate Widmeyer from other firms of similar size.

Widmeyer believes that sound research guides all successful communication activity. Our research team collects and analyzes information to help recognize targets and shape communications strategy.

We never conduct research for research's sake. Rather, we use research to shed light on and help solve our clients' challenges. Our research serves as a strategic roadmap to shape our clients' efforts and tackle the challenges they face.

Appendix

This study was designed to represent IT decision makers in the U.S., United Kingdom, and Asia-Pacific regions equally. Australia, Singapore, Malaysia, and Hong Kong were all included in the Asia-Pacific region

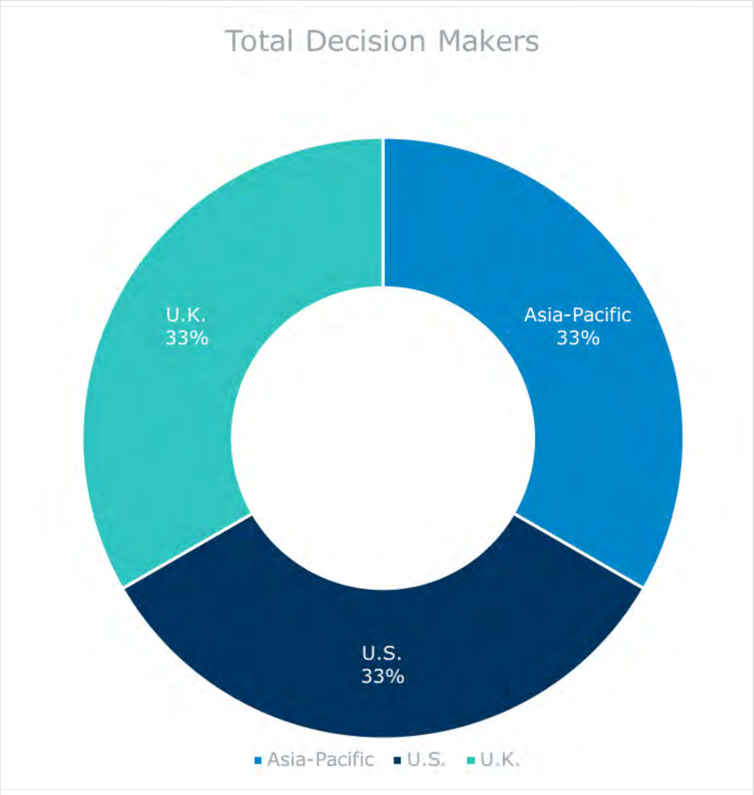


Figure 26. Regional Breakdown of Surveyed Decision Makers

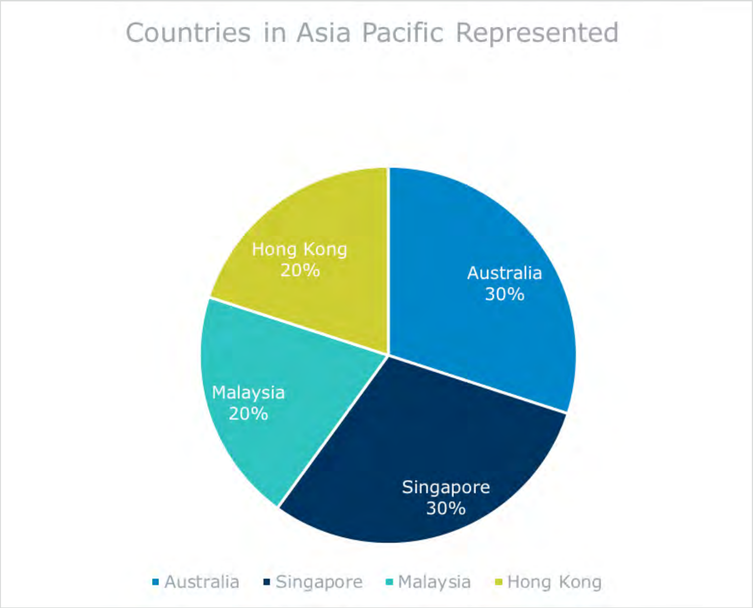


Figure 27. Geographic Representation of Survey and Breakdown of Asia-Pacific

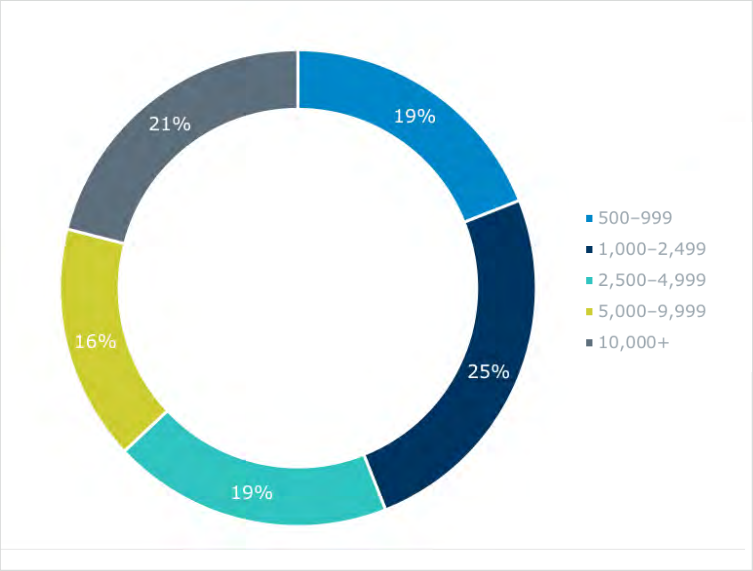


Figure 28. Number of Employees Working for Company/Organization

Appendix

The decision maker respondents represented a wide range of industries.

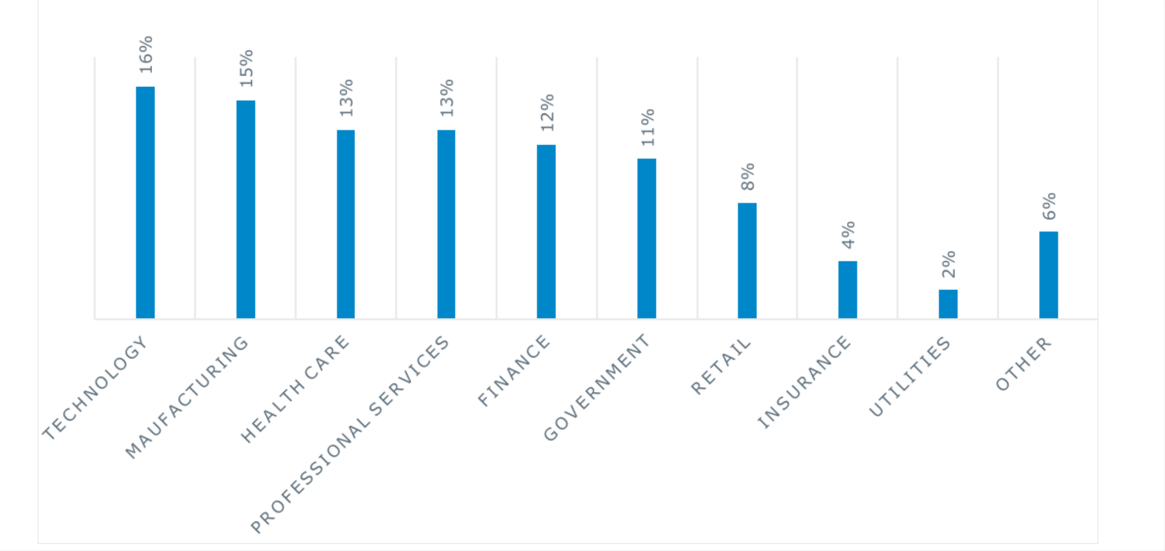


Figure 29. Industries of Decision Makers

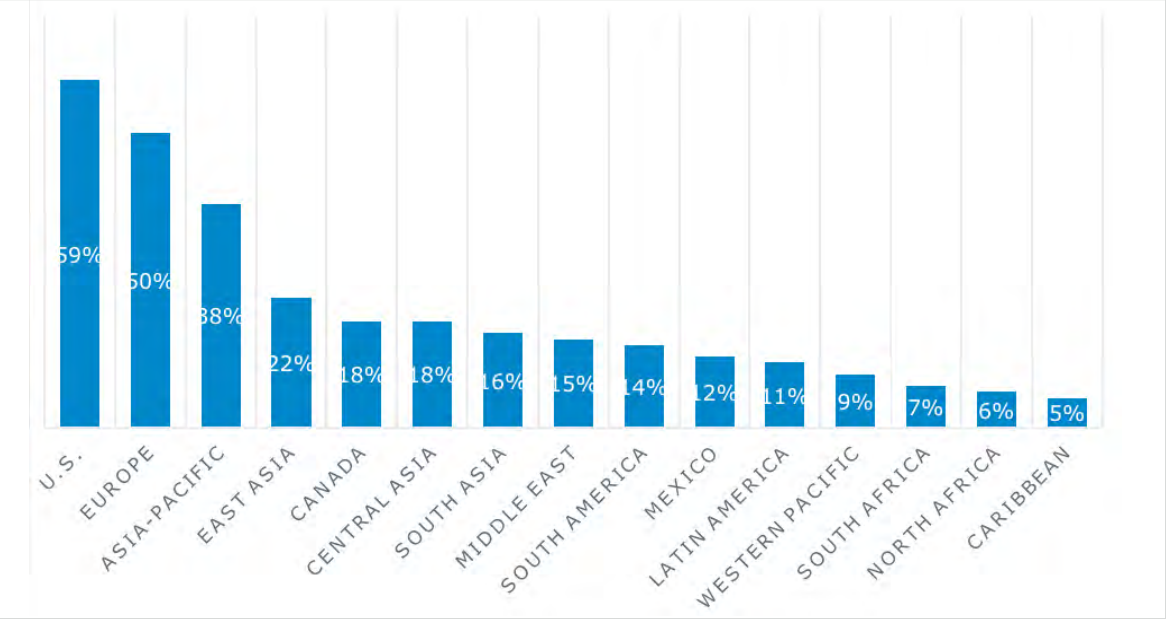


Figure 30. Regions of Company Offices

In terms of annual revenue, those surveyed in the U.S. represented companies with significantly higher revenue than both the U.K. and Asia-Pacific.

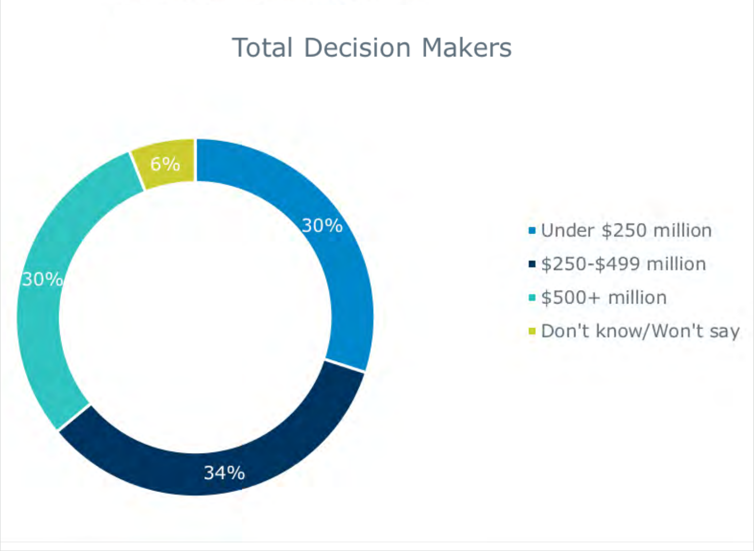


Figure 31. Breakdown of Decision Maker by Organization Revenue Size

Appendix

Just over half of these decision makers are executives with IT in their titles. Another third is in the C-suite.

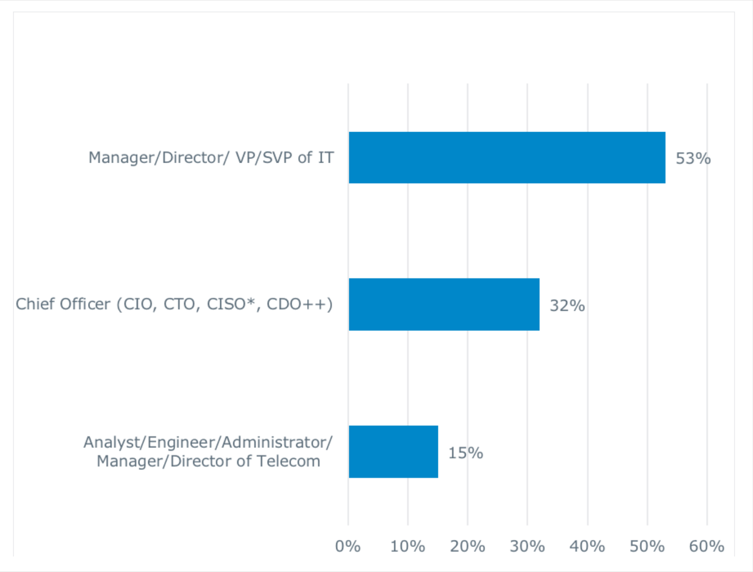


Figure 32. Role or Title of Respondents

For decision makers in the U.S., "IT" is more likely and "Telecommunications" is less likely to be part of a job title than for Asia-Pacific counterparts.

U.S. executives are less likely to hold a C-suite position.

Nearly all of these decision makers (99 percent) are employed full time. Nearly half describe their role in IT cybersecurity services and products as the sole decision maker.

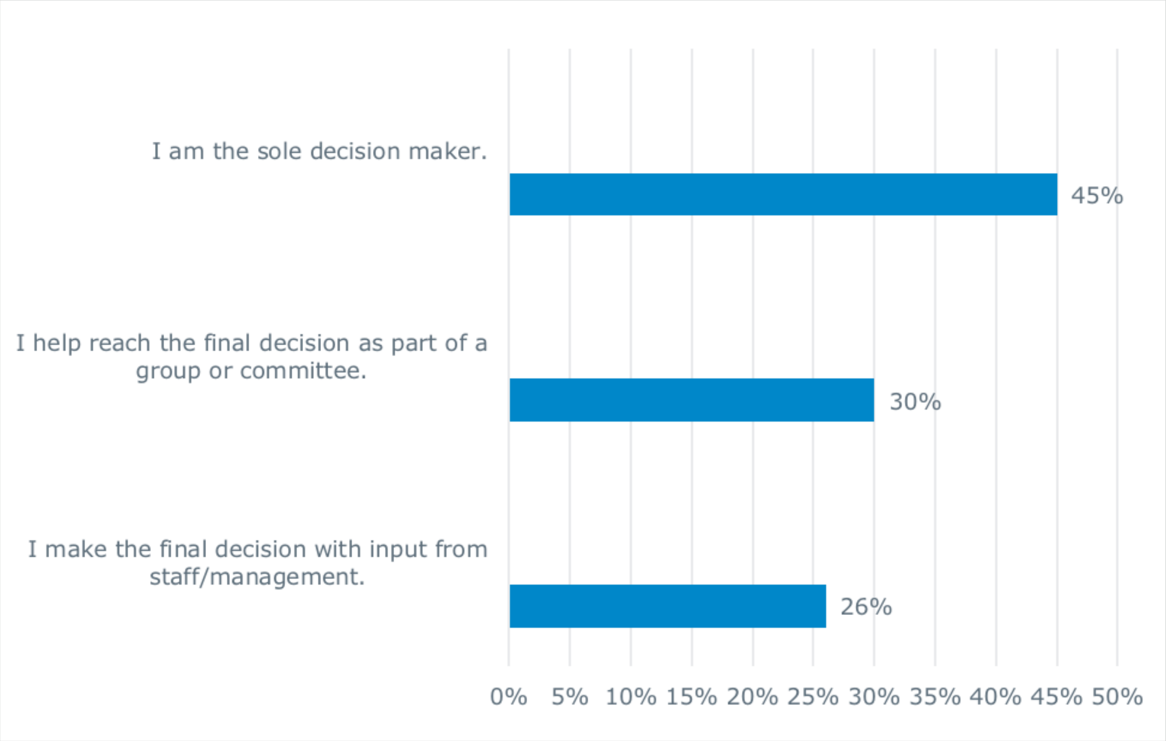


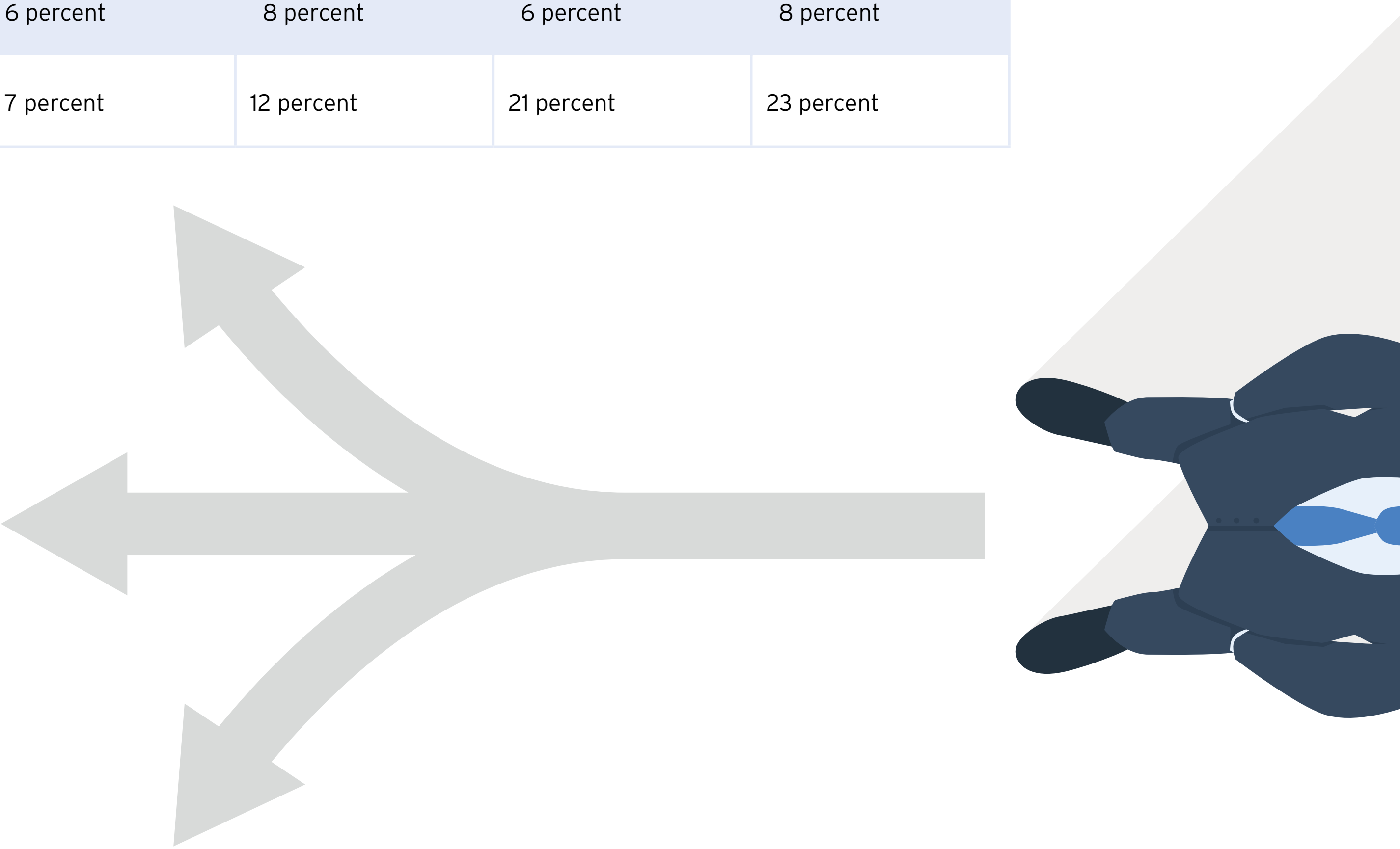
Figure 33. Role in IT Cybersecurity Services and Products of Decision Makers

Appendix

Roughly one-third of these executives are the sole decision maker in a wide variety of other areas as well, and most have real input into final decisions.

	General Staffing/ Recruiting	Outsourced Service Providers	Pricing Decisions for Division/ Business Unit	Financial Products	Advertising/ Sales/Marketing Materials
Sole decision maker	33 percent	38 percent	37 percent	32 percent	28 percent
Make final decision with input from staff/ management	26 percent	25 percent	23 percent	21 percent	22 percent
Help reach final decision on committee/group	25 percent	25 percent	21 percent	21 percent	19 percent
Provide input into final decision	7 percent	6 percent	8 percent	6 percent	8 percent
Have no input in final decision	10 percent	7 percent	12 percent	21 percent	23 percent

Table 5. Role of Decision Makers in Other Areas



Of the surveyed respondents, more than half have been employed by their company for at least six years. One in 12 aren't actively working in cybersecurity. About two-thirds have served in that area for three years or more. The average is just over five years.

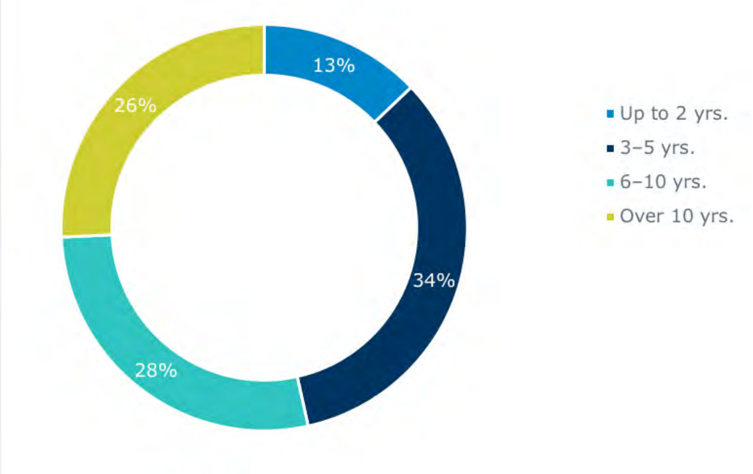


Figure 34. Number of Years Worked for Current Company

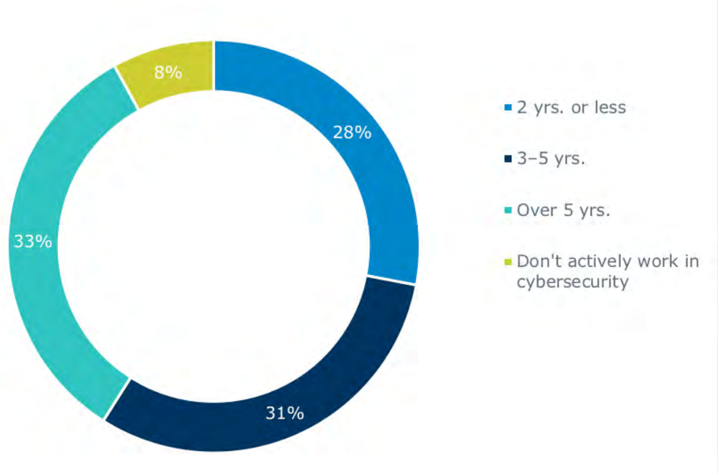
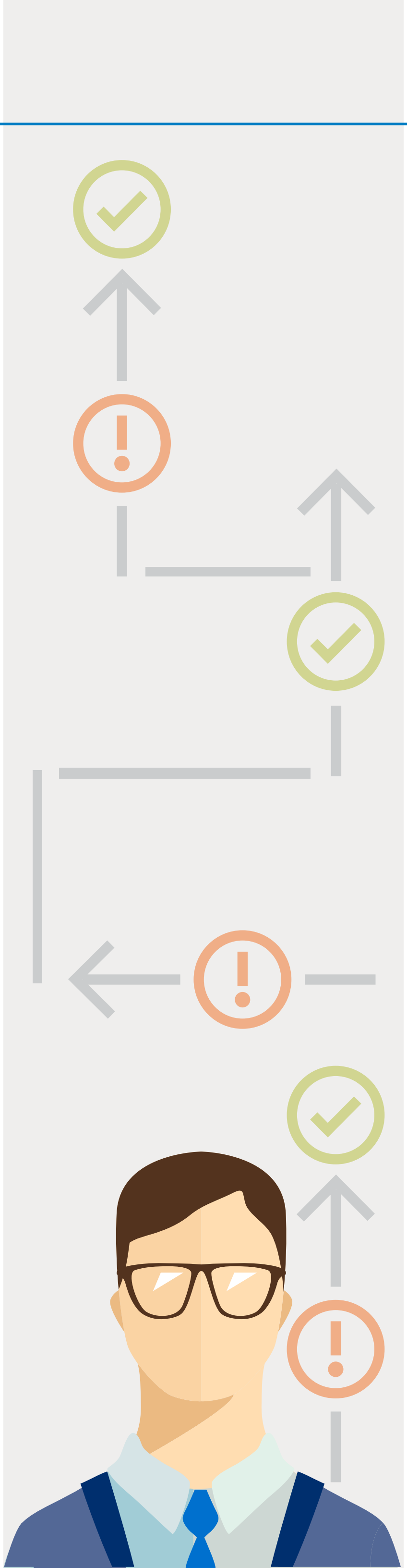


Figure 35. Number of Years Worked in Cybersecurity



The majority of these IT decision makers are between 35 and 49 years old. More than 70 percent are male.

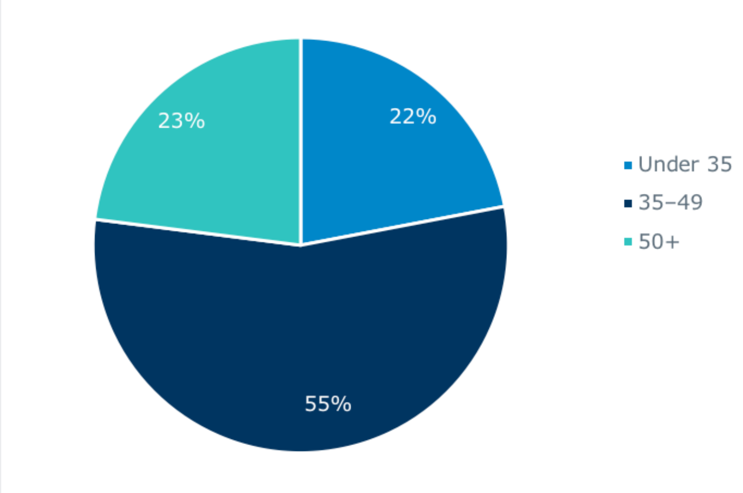


Figure 36. Age of Respondents

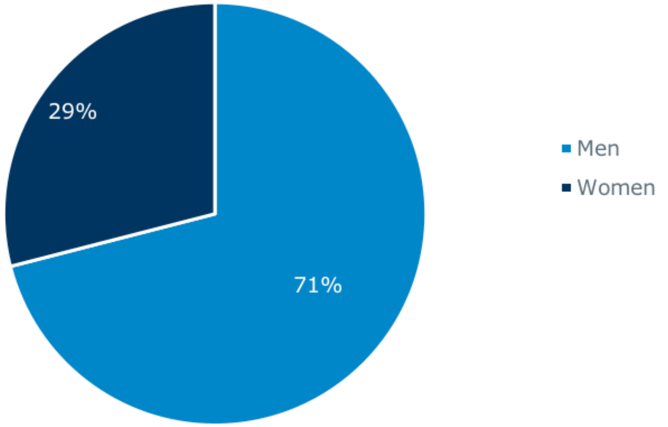


Figure 37. Gender of Respondents

Contact us:

TOLL FREE 1-866-384-0713

FAX (303) 413-8791

EMAIL info@logrhythm.com

Worldwide HQ, 4780 Pearl East Circle, Boulder, CO, 80301

LogRhythm®

The Security Intelligence Company