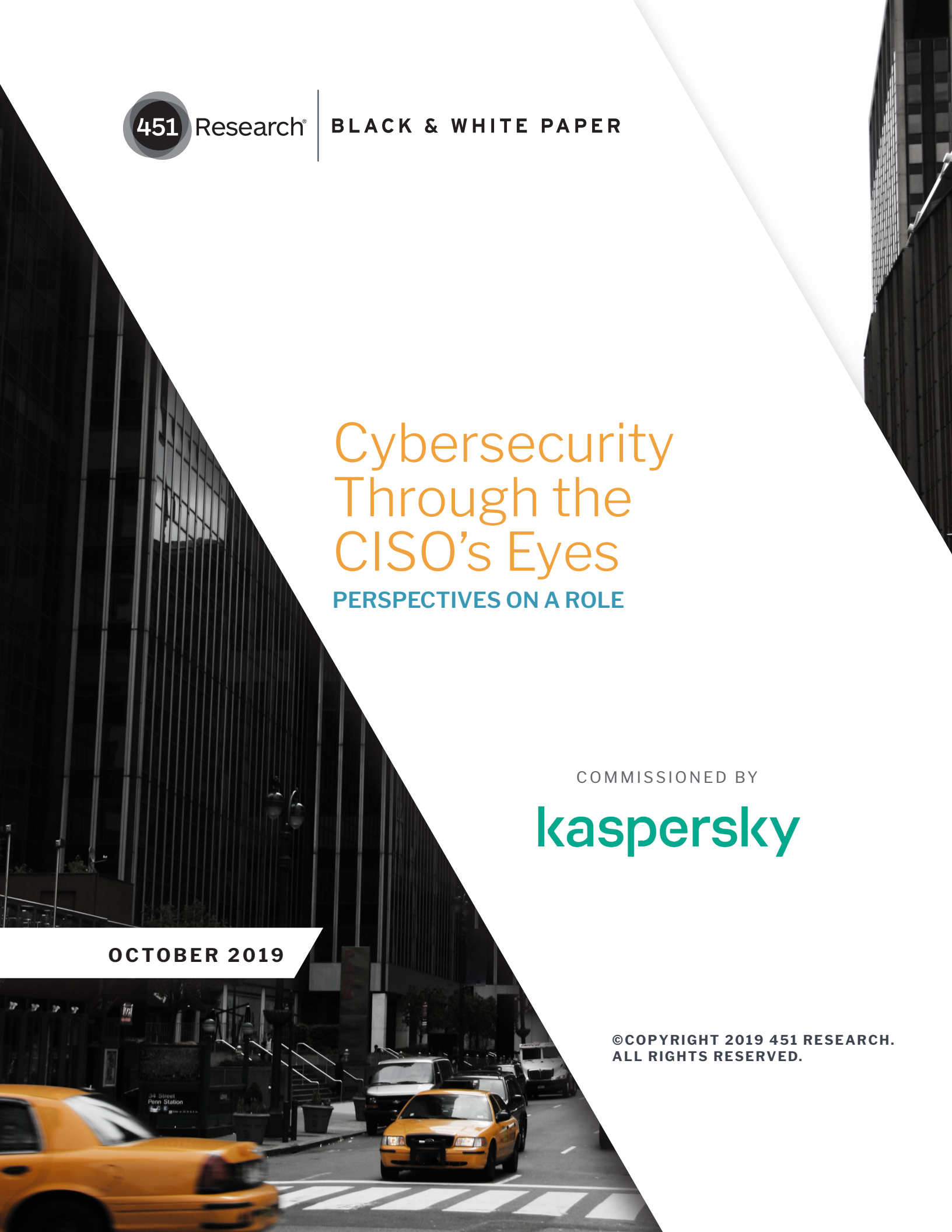
451 Research | BLACK & WHITE PAPER



Cybersecurity Through the CISO's Eyes

PERSPECTIVES ON A ROLE

COMMISSIONED BY

kaspersky

OCTOBER 2019

About this paper

A Black & White paper is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the "on the ground" experience and opinions of real practitioners — what they are doing, and why they are doing it.

ABOUT THE AUTHOR

SCOTT CRAWFORD

RESEARCH VICE PRESIDENT, SECURITY

Scott Crawford is Research Vice President for the Information Security Channel at 451 Research, where he leads coverage of the information security market. A former CISO for a global non-governmental organization (NGO), Scott has served as a security strategist with enterprises in both the public and private sectors.

Table of Contents

Introduction

In Q3 of calendar 2019, 451 Research undertook an independently conducted study, commissioned by Kaspersky, to explore the factors shaping information security from the perspective of the enterprise security leader. We surveyed 305 respondents that have senior or executive responsibility for cybersecurity in enterprises worldwide, with the findings revealing how the nature of cybersecurity – and security leadership – has evolved.

The study results point to the increased attention given to cybersecurity at the highest levels of corporate leadership. The input of senior security leaders is often sought proactively by an organization's board of directors, in order to provide those guiding the business as a whole with strategic direction on mitigating risk exposure. Metrics and maturity in the business discipline of risk management have become far more significant to enterprise security management than in the past.

To be sure, challenges still abound, ranging from a growing attack surface to ongoing difficulties in sourcing security expertise. Regardless, the increased visibility of the business impact of security breaches, record-high penalties imposed for violations of regulations directly influencing security priorities, and an attack surface expanded by innovation in multiple domains have assured that cybersecurity is now a strategic business priority. This study provides the perspective that only those with 'skin in the game' can offer on how that priority is evolving.

Key Findings

- **The practice of enterprise security has evolved from a field of tactical defense into strategic risk management:**
  - 70% of study respondents say that an emphasis on risk management is a top change in the CISO's role.
  - Risk management expertise is among the top three skills that CISOs cite as important.

- **Difficulty in sourcing security expertise is one of the greatest challenges:**
  - 70% find it hard to hire skilled personnel, in multiple roles.
  - Alternatives for finding talent include training personnel with general IT skills (51%) and even training those with little or no prior qualifications (28%).
  - Yet only 12% of study respondents have educational initiatives targeting college students to bring them into the security workforce.
  - 55% consider outsourcing to security service providers. This is a field 451 Research expects to grow at 16.9% CAGR through 2022.

- **The proportion of women entering the ranks of cybersecurity leadership is growing:**
  - 89% of men report more than two years in their position, compared with 74% of women.
  - 20% of the women responding to the survey have moved into the role in the last two years, compared with 10% of men.

- **At the same time, however, nearly half of all respondents (45%) say that women are underrepresented in their organization.**
  - Only 37% of study respondents either have or plan to implement initiatives to improve female representation in their IT security department.
- **When asked what puts the highest pressure on cybersecurity management, competition for budget (46%) is ranked almost as high as the growth and severity of attacks (49%).**
- **Top concerns range from the rapid evolution of cloud-native technologies to an explosion of 'smart' devices in IoT and a growing and more daunting threat landscape.**
- **Credibility with the business increasingly depends on measurement of success in tackling these concerns. Among the measures described:**
  - 'Mean time to remediation' of high-priority exposures.
  - The impact of security and privacy breaches, internally as well as on peer organizations.
  - Quality and speed of incident response handling – the top-mentioned metric for the security leader's personal performance.

Demographics

The participants sought for this study were those with senior- and executive-level responsibility for directing an information security ('InfoSec') program, including making decisions, developing strategy, measuring performance and coordinating priorities across the business. As such, 88% of respondents reported their title as either Chief Information Security Officer (CISO) or Head of IT Security. An additional 12% reported this responsibility at the C-level.

Geographically, the survey featured a strong global representation encompassing 27 countries, with respondents distributed among the following regions:

- 160 respondents (53%) were from Europe, the Middle East and Africa (EMEA).
- 65 (21%) were from Asian and Pacific countries (APAC).
- 55 (18%) were from North America (NA), specifically the US and Canada.
- 25 (9%) were from the Latin America region (LATAM), including Mexico.

Of the 275 respondents that reported gender, 77% reported as men while 23% reported as women. Geographic distribution by gender and regions described above is illustrated in Figure 1.

In terms of organizational size, 79% of respondents represent large enterprises of 2,000 staff or more, with 54% coming from organizations of between 2,000 and 10,000 employees. 25% represent enterprises of 10,000 employees or more, with 14% in organizations larger than 50,000.

Among industry verticals, technology (20%), financial services (18%), and manufacturing/construction (16%) stood out, followed by retail/hospitality (11%), energy/utilities (9%), healthcare (9%), professional services (4%), and other fields (3% or less each).

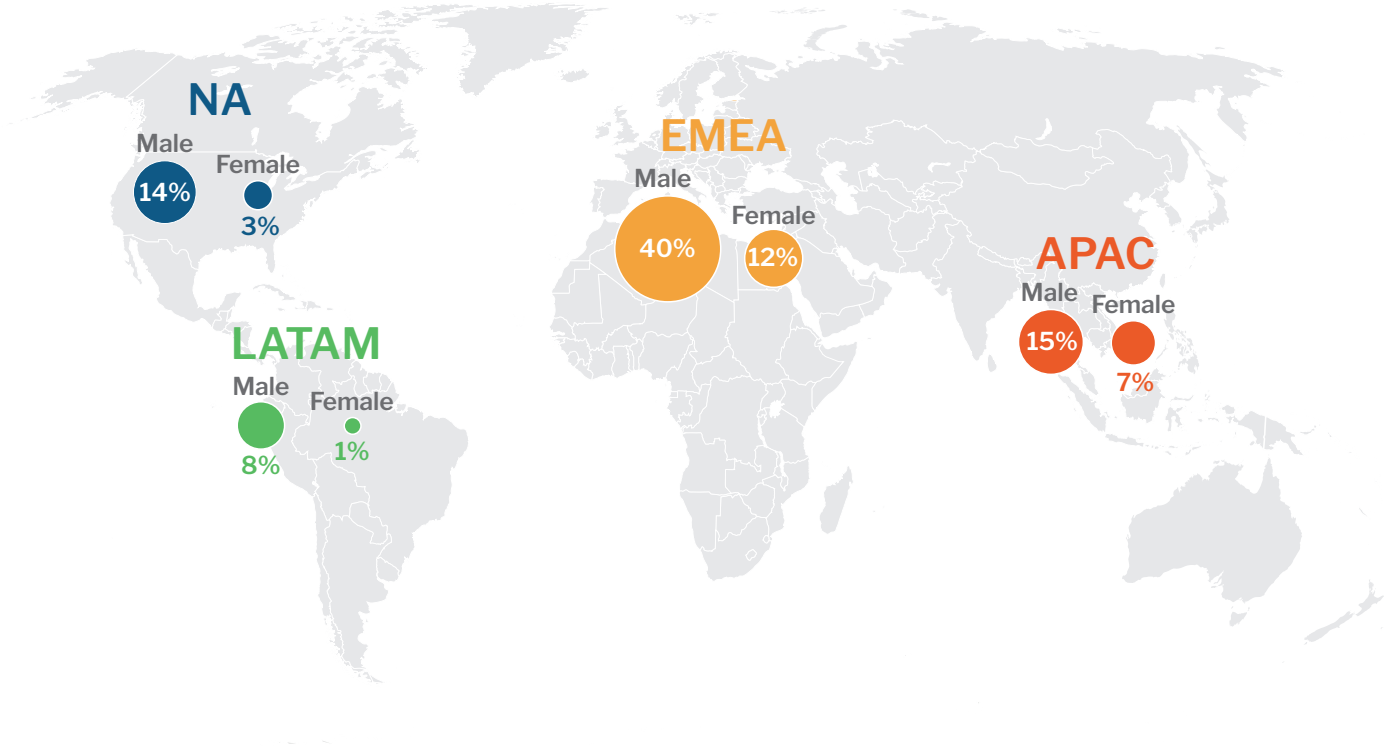
Respondents were predominantly in their late 30s, with mean and median age fairly close together (37.52 and 36.50, respectively). 95% are college-educated, with 57% reporting graduate-level degrees (master's or doctorate). 23% reported personal certifications such as the (ISC)^2 Certified Information Security Systems Professional (CISSP) or ISACA Certified Information Security Manager (CISM) credentials.

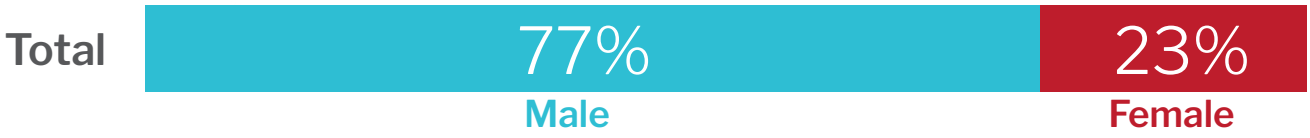
Regarding experience, 40% of respondents reported more than five years in their current position, with 46% reporting 2-5 years of tenure. The proportion of women moving into senior cybersecurity leadership is markedly on the rise. While 89% of men reported more than two years in their position compared with 74% of women, 20% of women have moved into the role in the last two years, compared with just 10% of men.

Figure 1: Distribution of Respondents by Region and Gender

Source: 451 Research Security Leadership Survey, 2019

NOTE: 275 out of 305 Total Respondents Reported Gender





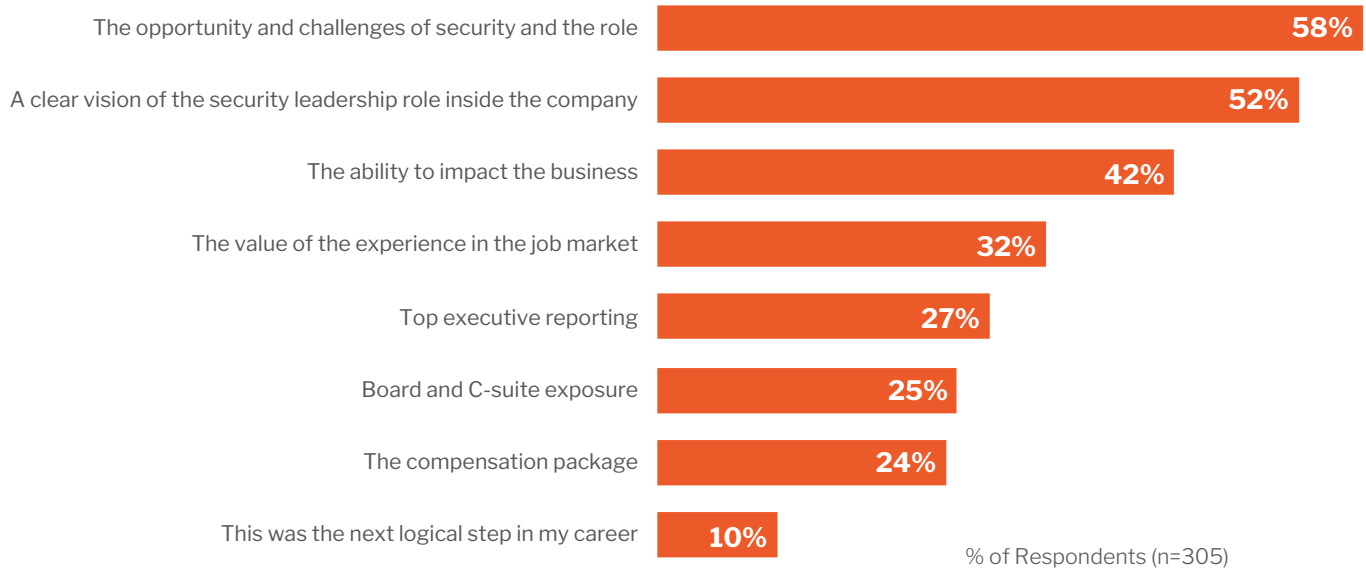
A Role With High Appeal, and Growing Impact

In recent years, cybersecurity has become a far more visible aspect of the modern business. High-profile breaches and privacy concerns consistently grab headlines – and businesses must now view their cybersecurity strategy as fundamental to overall business viability.

These factors, combined with the ever-evolving nature of the InfoSec challenge – unique to technology in its need to incorporate the impact of intelligent adversaries and gamesmanship – attract an equally unique combination of leadership attributes. Those who lead cybersecurity efforts in the business must be conversant in the technical nature of their role, but they must also demonstrate acumen as a business leader. They welcome the opportunity to be business influencers, and they seek out businesses that embrace that influence. Beyond the opportunities and challenges of the role itself, its two most appealing aspects for survey respondents are a clear vision of security leadership inside the company, and the ability to influence the business.

Figure 2: What Most Appealed to You When Considering the Role of CISO, CSO or Equivalent Senior Information Security Executive?[1]

Source: 451 Research Security Leadership Survey, 2019



This impact on the business is one of the factors that has increased markedly, according to this survey – 81% of respondents report having more ability to affect change in recent years than in the past. At the same time, however, 38% report having significant responsibility for security, but not enough authority to affect meaningful change. These findings may not be as paradoxical as they seem, though. Security leaders must often weigh in on business decisions or influence

1. *For questions in this survey where the sum of respondent percentages to all responses exceeds 100%, respondents could provide multiple responses. For questions depicted in this report where the respondent was asked to rank responses, the total number of respondents was 100% of the sample for each response.*

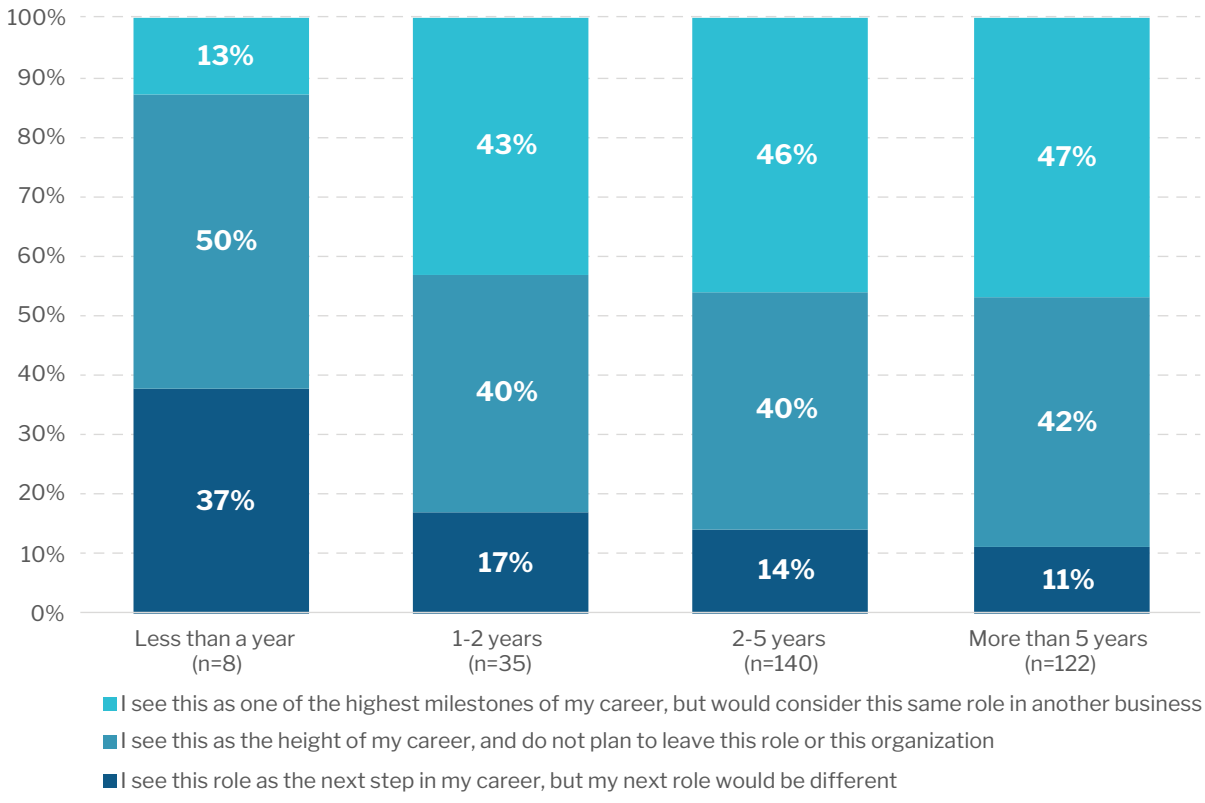
change in behavior for personnel over which they may have no direct authority, despite their growing influence at the highest levels of the business.

The influence of the security leader is also reflected in whom they report to. While 28% of respondents report to the CIO, the largest segment – 41% – report to the CEO. Meanwhile, 22% have a C-level title; 23% report to the board of directors. Even when not reporting directly to the board, the board seeks advice from 89% of respondents – 57% report to the board in regularly scheduled meetings; 60% when an incident has taken place internally; and 50% when an incident has occurred elsewhere. Only 29% report to the board when input is needed on a regulatory or compliance matter. These findings suggest that boards are much more involved in proactive cybersecurity management.

The rewards of the role are indicated by the views that CISOs and other cybersecurity leaders express about their future – 45% see it as the highest milestone of their career, even if they would consider the same role in another business, while 41% see it as the height of their career, and do not plan to leave either their role or their organization. This is even more remarkable considering that the mean age of respondents is 37.52 years. It's worth noting, however, that the longer the respondent's tenure in the role, the less likely they are to see their present position as the height of their career, and the more likely they are to consider the same role in another organization.

Figure 3: Which of the Following Statements Best Describes How You See Your Future in Your Role?

Source: 451 Research Security Leadership Survey, 2019



Taken together, these findings suggest that interest in career mobility increases with time – perhaps not surprisingly, given the potential opportunity and incentives available from another organization seeking that experience. But this increase is slight; nearly as many respondents see themselves continuing in their role with their present organization, with little change in that sentiment with increasing seniority.

These findings further point to a shift away from past perceptions, when the security leader may have been the scapegoat for a significant incident. In fact, in personal interviews with CISOs and other senior cybersecurity executives, none of them indicated any potential today for being penalized or terminated for a breach. Unless the incident were the direct fault of the security organization's actions or inactions, '"My company would support me" is a representative response voiced by security leaders from a wide diversity of regions, from Central Asia to North America.

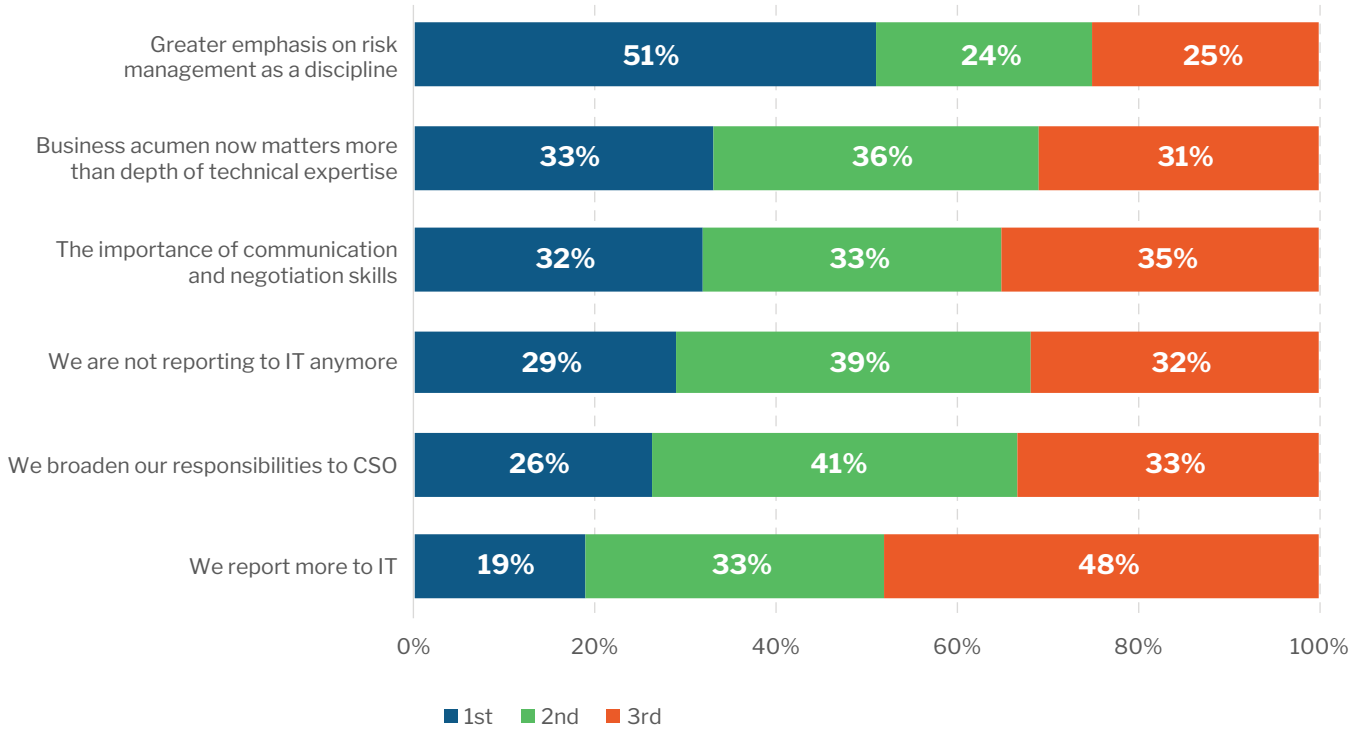
In short, today's cybersecurity leaders are valued more by the business than ever before.

Securing the Enterprise: From Tactical Defense to Strategic Risk Management

When it comes to justifying the priorities of enterprise security, multiple findings point to greater emphasis on 'speaking the language of business' – using principles and metrics accepted by business leaders to communicate the effectiveness of decision-making and investment. We see this reflected in what has changed most for cybersecurity leaders in recent years, and among these changes, one area increasingly stands out: the security leader must now be literate in the maturing discipline of cyber risk management. This evolving demand is also evident in the second-ranked change among respondents: that business acumen now matters more than depth of technical expertise.

Figure 4: What Has Changed the Most for Senior Information Security Leaders?

Source: 451 Research Security Leadership Survey, 2019
NOTE: Ranked 1st (most) to 3rd (least) (% of respondents, n=305)



How do security leaders communicate business value? One interviewee cited the similarity to investing in insurance, with which executives are familiar. The challenge for the security leader is to communicate both the need for, and the effectiveness of, risk mitigation. One of the areas where this becomes most evident is in justifying the security budget.

Those budgets continue to grow: 72% of survey respondents report that their security budget will increase in the coming year, a finding confirmed by 451 Research's Voice of the Enterprise studies, which show the proportion of those reporting rising security budgets growing from 62% to 87% over the past four years. These trends further reflect the increased priority that businesses are giving cybersecurity. As they increase their investment, it's only natural that businesses seek to understand the rationale behind security decisions.

The objective measurement of risk management and risk reduction has thus become a primary factor in aligning with business priorities for the cybersecurity leader. We see this, for example, in the many ways that these executives justify security budgets: objective metrics such as vulnerability mitigation and 'mean time to remediation' for high-priority exposures, the impact of cybersecurity incidents and breaches, and measurements against industry benchmarks are among the metrics used to justify security spending.

Figure 5: How Do Respondents Justify Their Budgets?

Source: 451 Research Security Leadership Survey, 2019

This closely parallels how the CISO's and other cybersecurity leaders' personal performance is measured: at 64%, quality and speed of incident response handling is mentioned by at least 15% more respondents than any other factor. The likely reason is that incidents are inevitable. Measuring the impact of response demonstrates how security keeps attacks contained, remediation effective – and the business safe.

While security budgets are increasing, budget pressures and competition for resources with other business groups are still among the top four factors that put the most pressure on security executives. We'll look at these and other pressures in more detail shortly – but before we do, note that the third-ranked change for InfoSec leaders in recent years is the increased importance of communication and negotiation skills, as shown in Figure 4 above.

Among other significant changes reported by security leaders, changes in the security organization's reporting structure further reflect the significance given to information security among business leaders. Reporting to management or the C-level separately from IT is often a sign of security's independence of IT priorities as a check-and-balance against competing interests – a contention reflected in competition for budget and resources, as we'll see in response to a later question. On the other hand, having security report to IT may suggest a closer working relationship with the information technologies on which the business depends.

It's therefore not surprising, perhaps, that our survey findings somewhat offset each other: 29% of respondents identify 'We are not reporting to IT anymore' as their number one change – but 19% identify 'We report more to IT' as the top change. An additional 26%, however, say their mandate has broadened to the role of Chief Security Officer (CSO), implying responsibilities beyond cybersecurity or information security per se – and further reinforcing the more strategic significance of security to the broader business.

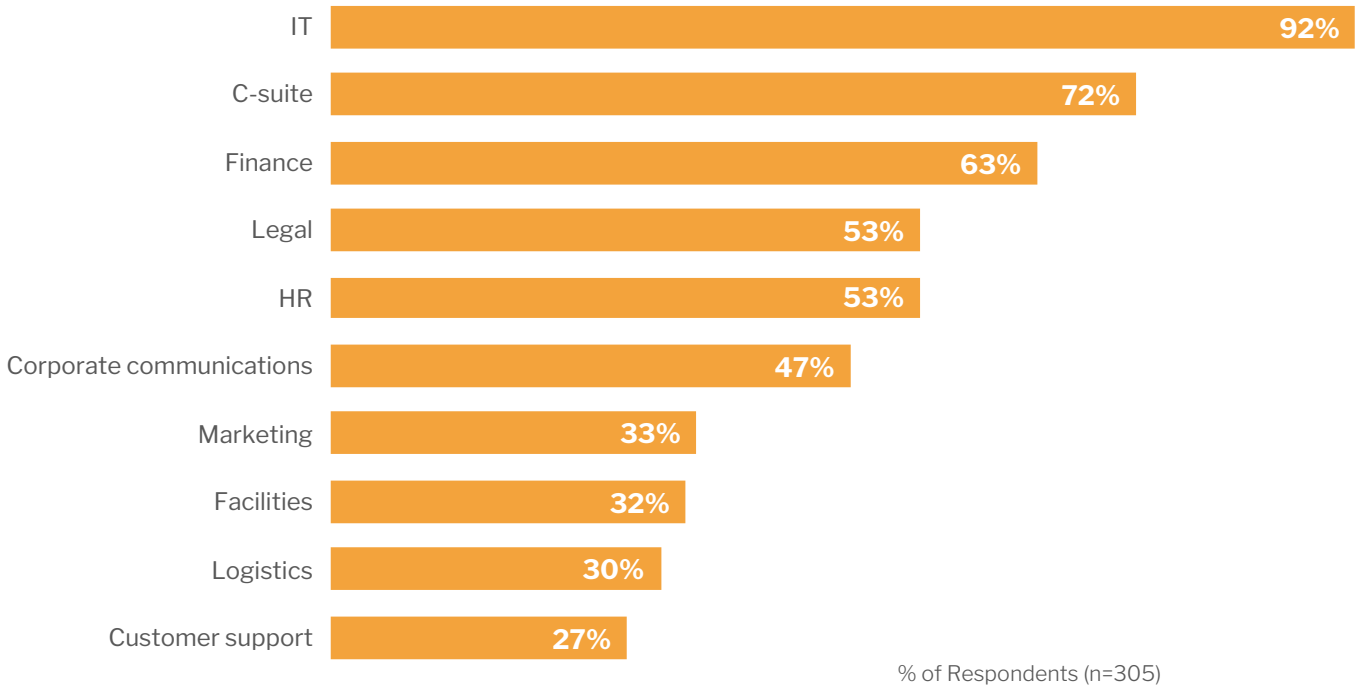
Interaction with IT goes beyond reporting structure, however. In fact, IT is the group that survey respondents interact with most, which is not surprising given their role primarily in mitigating cyber risks. But the need for interaction extends well beyond IT.

Interaction Across the Business

If business acumen matters more for the cybersecurity executive, the ability to communicate that acumen across the business has become important – not only to the credibility of the leader and their security program, but to engaging across interests and groups to keep the business as a whole more secure.

Figure 6: Which of the Following Groups Do Senior Cybersecurity Leaders Interact With Most?

Source: 451 Research Security Leadership Survey, 2019



IT may be the group that our survey respondents interact with most – with 64% working closely with IT on all security matters – but 33% say they do so only when it comes to technical IT security matters. This suggests that more can be done to better align with IT. In personal interviews with CISOs and other security leaders, respondents call out opportunities to work more closely with development teams, for example. Such cooperation is seen as essential as IT increasingly embraces trends such as DevOps with 'agile' methods for producing IT functionality, and 'cloud native' technologies become more central to securing IT.

It's worth noting that interaction with the executive leadership of the business as a whole ranks second on the list in Figure 6 – again reflecting the significance of cybersecurity and cyber risk management to the business at a strategic level. It's not just the language of risk that respondents say they need to master, however. They must also be adept at bridging gaps of understanding with business leaders. As one interviewee expressed, "Executives are mainly from management schools and have their own vocabulary and understanding, but the concepts of information technology, cyberattack and cyberthreats are more complex," noting that these

are areas where executives may be less confident of their grasp, and they may not know exactly how or what to ask to better their understanding. This can result in lost momentum for security initiatives. Security leaders must be skilled in bridging these gaps in understanding to win support for the priorities they believe the business must acknowledge to operate safely.

After IT and the executive suite, cybersecurity leaders' level of interaction with other organizational groups follows in a predictable order: finance (with whom budgets and spending priorities must be worked out); legal (given the implications of cybersecurity policy and incidents at multiple levels); and human resources (for sourcing and retaining personnel, as well as for interactions with people across the business).

Another seeming paradox emerges in interactions with the two groups most concerned with communicating the message, priorities and positioning of the business: corporate communications and marketing. While only 47% of respondents report a high degree of interaction with corporate communications, this may be a function of interaction that's more event-driven than ongoing. Among all respondents, 97% agree (47% agree strongly) with the statement, 'When responding to security incidents, we secure participation from key stakeholders across IT, HR, Compliance, Legal, External Partners and PR/Corporate Communications.' While interaction with corporate communications may not be continuous, respondents do place a high degree of emphasis on cooperation across teams for the sake of incident response.

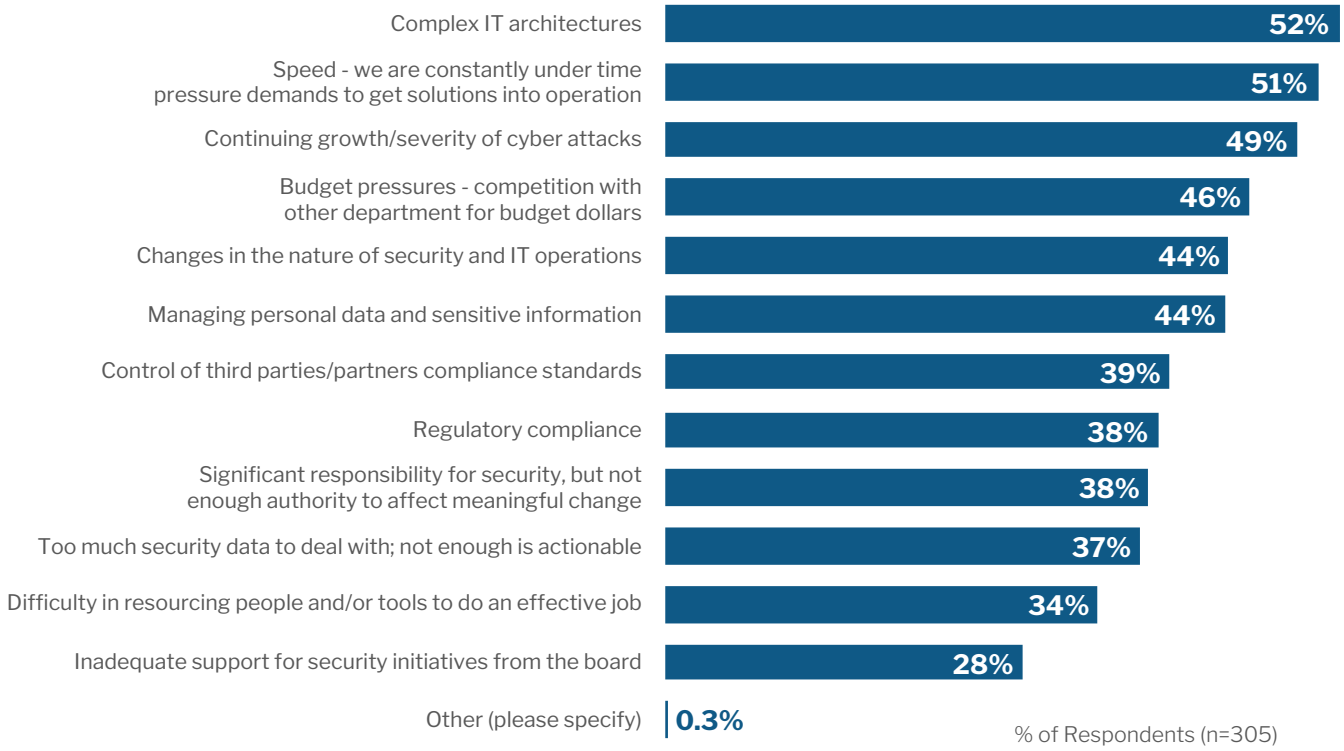
Our study found that quality and speed of incident response is the top metric identified for measuring the security leader's performance. Accordingly, 93% of respondents agree (44% strongly agree) that 'they clearly define and communicate incident response roles and responsibilities to all stakeholders.' But there is still room for improvement. When asked specifically about having a 'comprehensive communications plan in the event of an incident,' confidence drops somewhat: while 88% agree with that statement, only 35% agree strongly. Breach simulations, including so-called 'tabletop' exercises, may represent another area where more can be done to optimize security performance across the business – while 84% agree that they regularly run such exercises, only 32% agree strongly.

Tackling Demands in Multiple Dimensions

The issues that place the most pressure on cybersecurity executives are a direct indication of those that concern businesses the most. Respondents to this study described those pressures on multiple fronts.

Figure 7: What Puts the Most Pressure on Your Role as a Senior InfoSec Executive?

Source: 451 Research Security Leadership Survey, 2019



In terms of the most pressing issues for InfoSec leaders, a variety of responses are grouped fairly closely together in their frequency of mentions. Not unexpected among the top responses are the growing complexity of IT, with its increasing intersections with operational technology (OT) and the Internet of Things (52%); the rapid pace of security operations (51%); and a growing threat landscape (49%).

The next most frequently mentioned issue may be surprising, however: budget pressure and competition with other departments for available resources is a concern cited nearly as often (by 46%) as the top three responses. This may seem like a paradox as security budgets continue to grow, but budget challenges come from multiple directions. Difficulty in distinguishing IT spending from security spending is the most-reported obstacle here (54% of respondents). Resolving this conflict may therefore play a role in changing reporting structures for the security organization: as noted above, 19% of respondents say the biggest change they've seen in recent years is that they report more to IT than in the past, but 29% say the biggest change is that they no longer report to IT.

These findings seem to highlight a dilemma: is it better to distinguish security's priorities from those of IT? Or is it better for IT and security priorities to be more closely aligned? Difficulty in distinguishing security's budget from IT's may be a bellwether for just how difficult it is for organizations to answer these questions. Each enterprise may come to its own conclusions, but there does not yet seem to be consensus.

Demonstrating the effectiveness of the security investment is the next most frequently mentioned pressure on InfoSec leaders (47%). As noted earlier, this has been a factor in focusing security leaders on measuring and managing risk, and developing credible metrics for security operations as well as personal performance.

Competition from other business or IT initiatives is next on the list of pressures, at 43% of respondents, and this further reflects the ongoing dilemma regarding security investment – and not just with IT. Many organizations prioritize their strategic business initiatives, and rightly so: these are the profit centers on which the business depends. Security, on the other hand, is often viewed as a cost center, and its contribution to helping the enterprise achieve its business goals may be placed behind primary objectives of reaching customers and generating revenue.

But the damages wrought by security incidents can have a substantial business impact – and many organizations are awakening to the fact that the true cost of this impact may not be fully known until it's too late. Nevertheless, this contention is one of the few sources of ongoing friction between security executives and competitors for budget dollars reported in personal interviews.

These factors all highlight pressures within the enterprise. What concerns security leaders beyond the enterprise, in the evolution of technology and the threat landscape? When asked what sources of risk worry them the most, fundamental changes in the nature of IT – such as cloud and 'cloud native' approaches and DevOps trends – again rise to the top, mentioned by 42% of respondents as their most significant concern. But mentioned virtually as often as these trends at the center of IT are those at the edge: 40% rate the risks introduced by IT/OT integration and newer 'smart' technologies as a top concern.

Also mentioned about as frequently are risks in the hardware and software supply chain (41%). This lines up with the risks posed by exposure to third parties such as partners, contractors and suppliers of all types mentioned by those interviewed for this study. Said one respondent, "We share data with many third-party business partners. Even though we have a business agreement in place, we are not 100% sure of how they protect data in their environment." Third-party issues also reflect concerns about the software supply chain surfaced by incidents such as the 2017 Equifax breach, where initial compromise was achieved through exploit of a vulnerability in the Apache Struts open source framework.

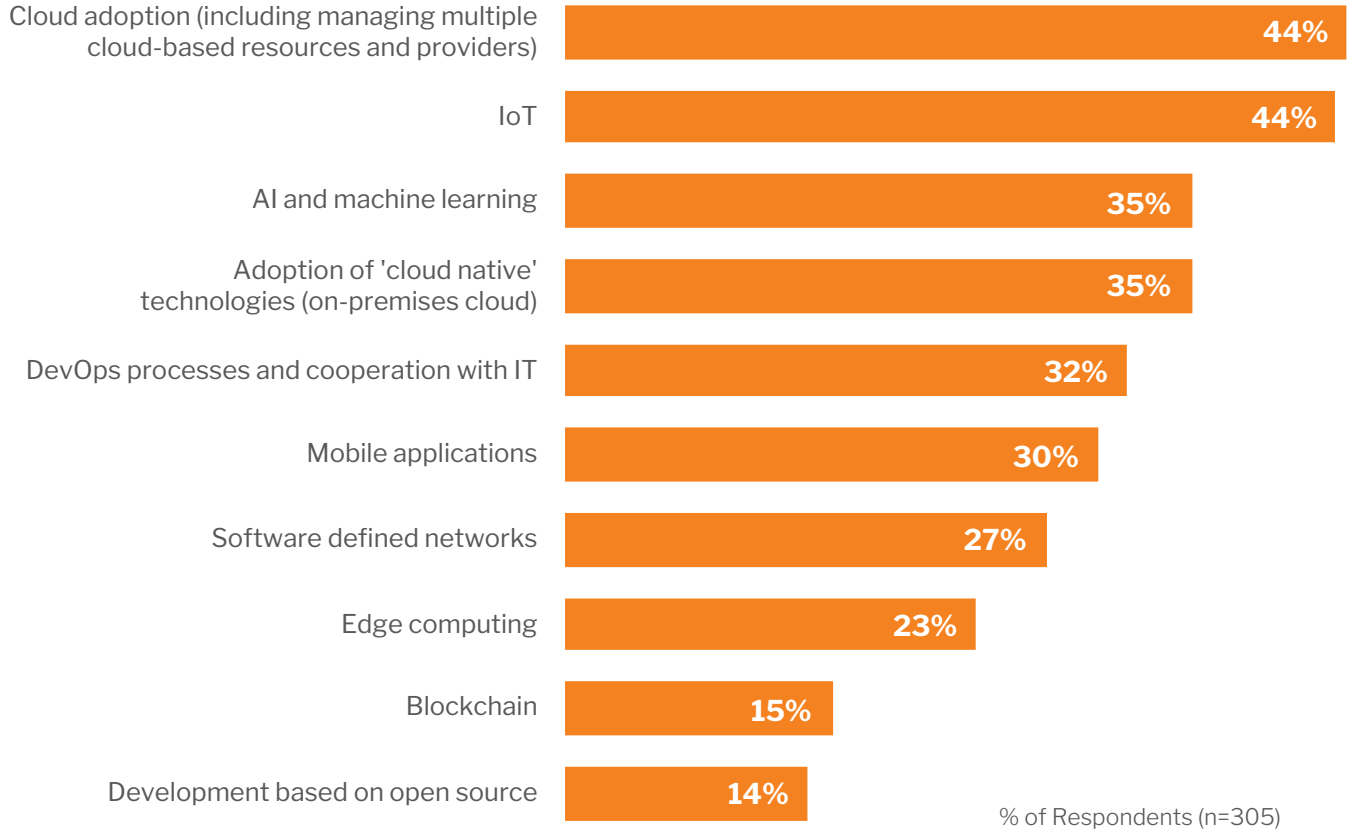
When asked to identify the most worrisome threat actors, study respondents mentioned financially motivated cyber criminals (30%) far more than the next most frequently cited categories of malicious insiders and 'hacktivist' groups (18% each). This top response reflects not only widespread 'industrialized' attacks with impact across an entire landscape of targets, but also the ongoing threat of high-profile and high-impact attacks such as ransomware and worms targeting persistently vulnerable IT exposures.

Looking Ahead: Facing the Demands of Tomorrow

Going forward, security leaders see the forces of change coming from multiple directions in the next five years.

Figure 8: Which of the Following Technology Trends Will Have the Biggest Impact on IT Security Over the Next Five Years?

Source: 451 Research Security Leadership Survey, 2019



As with an earlier question, where respondents rated the risks presented by fundamental IT change, the growth in adoption of cloud technologies and the expansion of IoT are the trends InfoSec leaders mention most often when asked what they expect to have the greatest impact on cybersecurity going forward. The advance of artificial intelligence and machine learning places third in frequency of mentions – although this is the trend most often mentioned by interviewees in Europe and APAC. The adoption of cloud-native technologies places next, along with the DevOps processes that often accompany these new approaches to IT. Software-defined networks and edge computing, meanwhile, are also related to more-often-identified factors such as cloud and IoT. Blockchain may not be highlighted as strongly among respondents, but its appearance here suggests the need to focus attention on the business opportunity it presents, which may foreshadow future priorities.

Tough Times for Sourcing Expertise

It's no secret that it has become difficult for enterprises to source skilled cybersecurity professionals; 70% of respondents to this survey agree with that statement. This parallels a 451 Research Voice of the Enterprise 2019 study in which 66% of respondents reported that they didn't have enough information security personnel. Even more respondents to 451 Research VotE surveys report 'moderate' to 'significant' difficulty in recruiting for information security: a total of 87-89% of respondents have fallen into these combined categories over the past three years.

The difficulty extends across multiple roles, with few differences. All of the following areas were mentioned by 40-49% of respondents in this survey: threat intelligence, network security specialists, data security and encryption, expertise in cloud security platforms, application security, programmers to build and automate security functions, and Qualified Security Assessors (a certification established by the Payment Card Industry Security Standards Council to validate adherence to the PCI Data Security Standard).

Among options for sourcing expertise in this challenging climate, hiring fully qualified personnel is still the top choice (64%). But service providers are next most often mentioned, by 55% of respondents. We see this reflected in our recent 451 Research Hosting, Cloud & Managed Services Market Monitor report, which projects a 16.9% compound annual growth rate (CAGR) for managed security services through 2022.

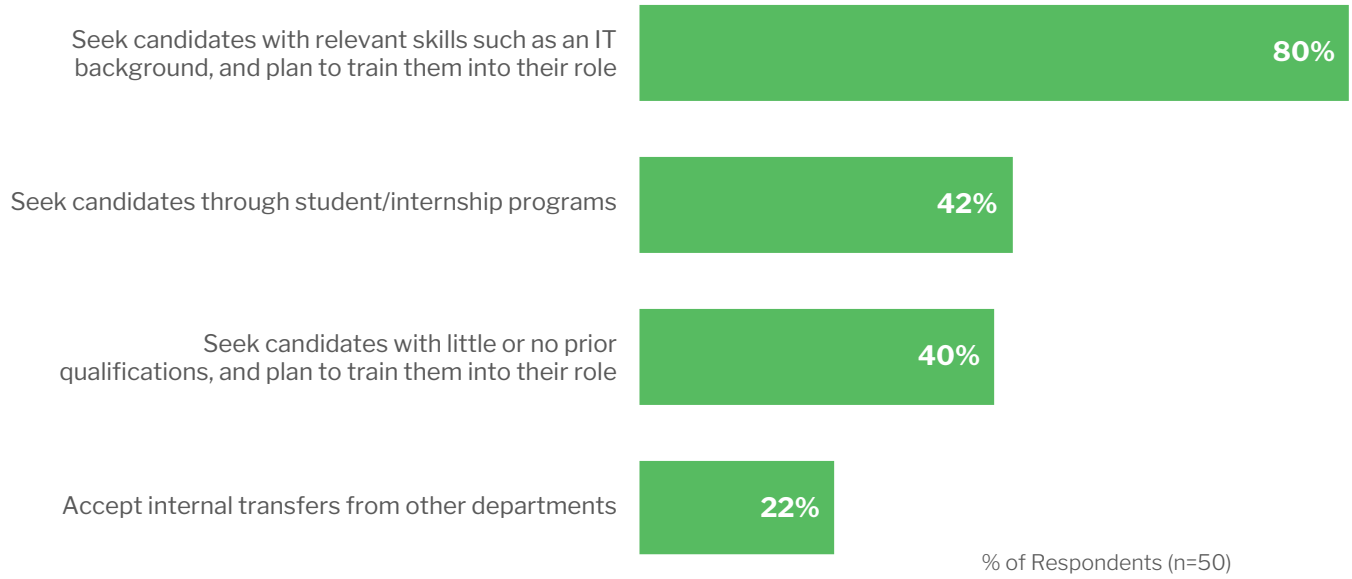
From here, the options begin to broaden. Hiring personnel with a general IT background, but no specific security experience, follows next at 51%, with contractors rated below that. But only 28% of respondents consider hiring those with little or no qualifications an option. Also, few survey respondents (12%) mention internship programs or cooperation with colleges and universities – but these efforts do get a positive mention in personal respondent interviews, indicating that those who pursue such options view them favorably.

Recruiting and Retaining Women

As organizations weigh their alternatives for bringing new candidates into the workforce, expanding their efforts to reach out to those underrepresented in cybersecurity, such as women, may offer opportunities to help close the expertise gap. While 63% of study respondents say they seek fully qualified candidates only, without regard to gender, nearly half (45%) say women are underrepresented in their security organization relative to the workforce as a whole. Among those who say that women are underrepresented, only 37% have, or are planning, a formal program that specifically targets women.

Figure 9: Respondents Having a Formal Recruitment Program Targeting Women: What Does It Consist Of?

Source: 451 Research Security Leadership Survey, 2019



Among these organizations with a formal program, 80% seek candidates with relevant skills such as a general IT background, and plan to train them into the role. This approach is mentioned nearly twice as often as internship (42%) or outreach to candidates with little or no prior qualifications (40%), and nearly four times more often than accepting internal transfers from other departments (22%).

While it may seem paradoxical that 42% of those with or planning a formal outreach to women plan to employ student or internship programs, compared with only 12% of organizations reporting difficulty sourcing security personnel generally, these numbers may not be as disconnected as they appear, since the actual number of respondents in each case is nearly the same.

Conclusions

The perspectives of the cybersecurity leader are a direct reflection of the security interests and concerns of the enterprise. Security has become far more strategic to the business, requiring expertise in domains ranging from technical knowledge to business acumen and maturity in key focal disciplines such as cyber risk management. Together, these attributes have increasingly brought security executives to the attention of leadership at the highest levels of the enterprise, signaling the growing importance of cybersecurity to the business as a whole.

But there are still battles to be won. The importance of security must be assured in the face of contention such as competition for resources, or losing the priority given to security spending when it is categorized simply as part of spending on IT overall. Without this assurance, businesses may make decisions that appear sound and supportive of strategic priorities, but which can place those very priorities at higher risk.

Businesses and security leaders alike must also get more creative about how they address problems like the high demand for security expertise in the face of limited supply. Making the most of opportunities to include those underrepresented in the security workforce, such as women, can bring new perspectives as well as bringing new talents and skills to bear on the security challenge. Such efforts can broaden the variety of experience within an organization, where new ideas may be key to anticipating what an intelligent adversary may do next.

All these factors reflect how cybersecurity, a priority that has already become strategic to the business, may become even more so in the future. As organizations see the business potential that new approaches to information technology offer, they will also have to reckon with the new ways they introduce risk. It will be the cybersecurity leader at the center of this reckoning, looked to as both a voice of objective credibility as well as a focus of decisive action, to guide businesses in successfully navigating these uncharted waters. Because of this privileged position, it will also be the cybersecurity leader who continues to provide the perspective that only those with responsibility can, around how cybersecurity has developed thus far, and how it will evolve in the future.

Methodology

In July 2019, 451 Research surveyed the 305 Chief Information Security Officers and senior enterprise cybersecurity leaders qualified and described in the 'Demographics' section above. We asked a wide range of questions aimed at evaluating and measuring the following key themes:

- Dynamics describing the nature of the cybersecurity leadership role.
- Factors that have influenced changes in the role in recent years.
- Interactions across the business, including the groups within the business these leaders interact with most, and would seek to interact with more.
- Issues and challenges in sourcing cybersecurity expertise, with specific questions regarding the recruitment and retention of women in cybersecurity.
- Pressures of the security leadership role, and leaders' most significant concerns.
- Trends shaping the future of information security.

Respondents were screened for qualification as described earlier and asked to provide responses to a web-based questionnaire. For questions where the sum of respondent percentages for all responses exceeded 100%, respondents could provide more than one response, or were asked to rank responses as described in specific questions. The survey was further supplemented by interactions with 10 discussion-board participants screened for their role in cybersecurity leadership similar to the screenings applied to the survey, as well as six in-depth interviews with additional cybersecurity leaders similarly qualified.

Content Provided By

kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at *www.kaspersky.com*.

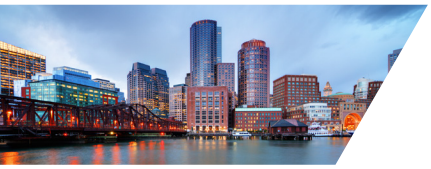
About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 1,000 client organizations globally through a combination of syndicated research and data, advisory and go-to-market services, and live events. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
Chrysler Building
405 Lexington Avenue, 9th Floor
New York, NY 10174
+1 212 505 3030

SAN FRANCISCO
505 Montgomery Street,
Suite 1052
San Francisco, CA 94111
+1 212 505 3030

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700



BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®