A Forrester Consulting
Thought Leadership Spotlight
Commissioned By VMware

May 2020

IT And Security Perspectives: A Spotlight On C-level Vs. VP/Below

Role Results From The May 2020 Thought Leadership Paper "Tension Between IT And Security Professionals Reinforcing Silos And Security Strain"

FORRESTER®

Introduction

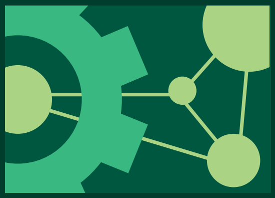
IT and Security teams are tasked with handling major risks and concerns daily. However, in some cases, the gaps between C-level perceptions and practitioners' reality cause teams to work at odds with each other.

In February 2020, VMware commissioned Forrester Consulting to learn how executing against a consolidated IT management and security strategy could help break down silos across the two teams to improve security outcomes. We also explored the relationship between IT and Security teams, including the relationship between C-level and manager/director level employees within those organizations. Forrester conducted a global online survey with 1,451 manager-level and above respondents and interviewed eight CIOs and CISOs to further explore this topic. All respondents have responsibility and decision-making influence over security strategy.

We found that companies are aware of the strained relationships that exist among teams and are focused on attempting to reconcile the divide. Without a unified IT and Security strategy powered by technology-enabled collaboration, companies are unable to advance as they desire.

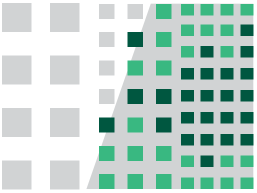
KEY FINDINGS

- **The C-suite faces unique internal challenges that distract from more important issues.** Some of the most important things on the minds of CISOs and CIOs include differences in career advancement opportunities, talent shortages, and pressure from the board.
- **Managers, directors, and VPs are bogged down by strained relationships and unsatisfactory tools.** Strained relationships between IT and Security teams are common in this group. Combined with too many inefficient tools and the constant need to train new employees, this takes workers away from necessary tasks.



- **A unified and consolidated strategy addresses these key relationship concerns.** Companies are aware of these relationship issues and are actively pursuing ways to reconcile them. While only 30% have already implemented a unified and consolidated IT management and security strategy, 41% are planning to implement within the next 12 months.

Gaps Persist Between The Perceived Realities Of C-Suite And VPs/Below

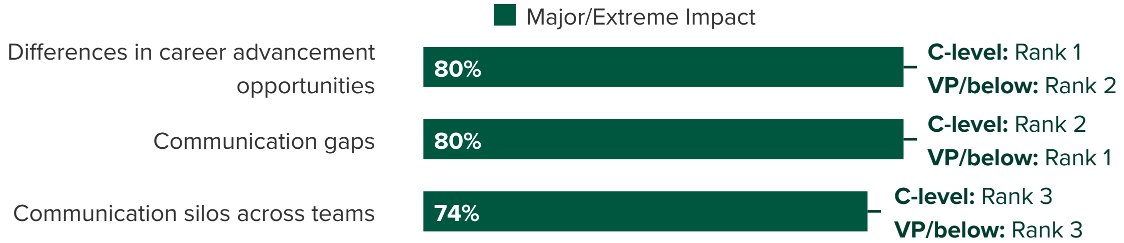


IT and Security tasks are critical in protecting a company's greatest asset: its data. Organizations agree that security is becoming more of a team sport than ever before as more tasks are being shared across teams. However, are these teams united against a common enemy (e.g., risks and breaches)? Or are they at war among themselves? What are the relationships like between C-level executives and the VPs/below within the teams? In surveying global C-level leaders, VPs, directors, and managers of both IT and Security, we found that:

- **C-Suite and VP/below have some different priorities.** Some of these priorities are self-evident. For example, the C-Suite is a top contributor to the development of a security strategy, but the VP/below group is far more involved in its execution. However, these differences can strain the relationship between leaders and those beneath them. For example, when companies have challenges with IT and Security tasks, 6% more of the C-level group experiences the consequence of team misalignment than VP/below, while 5% more in the VP/below group experiences the consequence of a decreased ability to scale. While the C-level is focused more on relationships and processes, the direct reports feel pressure from the top to scale, and they struggle to keep up during challenging times.
- **Communication gaps and silos abound among teams.** When examining gaps between IT and Security teams, both C-level and VP/below agree that communication gaps and silos between teams have a large negative impact on collaboration (see Figure 1). In fact, they rank these two communication issues at the top of a list of 12 gaps, signifying just how common and detrimental these barriers are.

Figure 1: Impact Of Team Gaps

"As security and IT teams work together, what impact do the following gaps have on that collaboration?" (Showing top 3 of 12.)



Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

According to one CIO:

> "[Most issues within teams are] 100% communication. [It's] people not communicating, not documenting, or not telling somebody what they're doing. That is 100% the problem. You can put meetings together. You can do ticket reviews. It's just so difficult because people fundamentally just don't think about communicating. That's really where [the problem is] at."
>
> *CIO of energy corporation in the US*

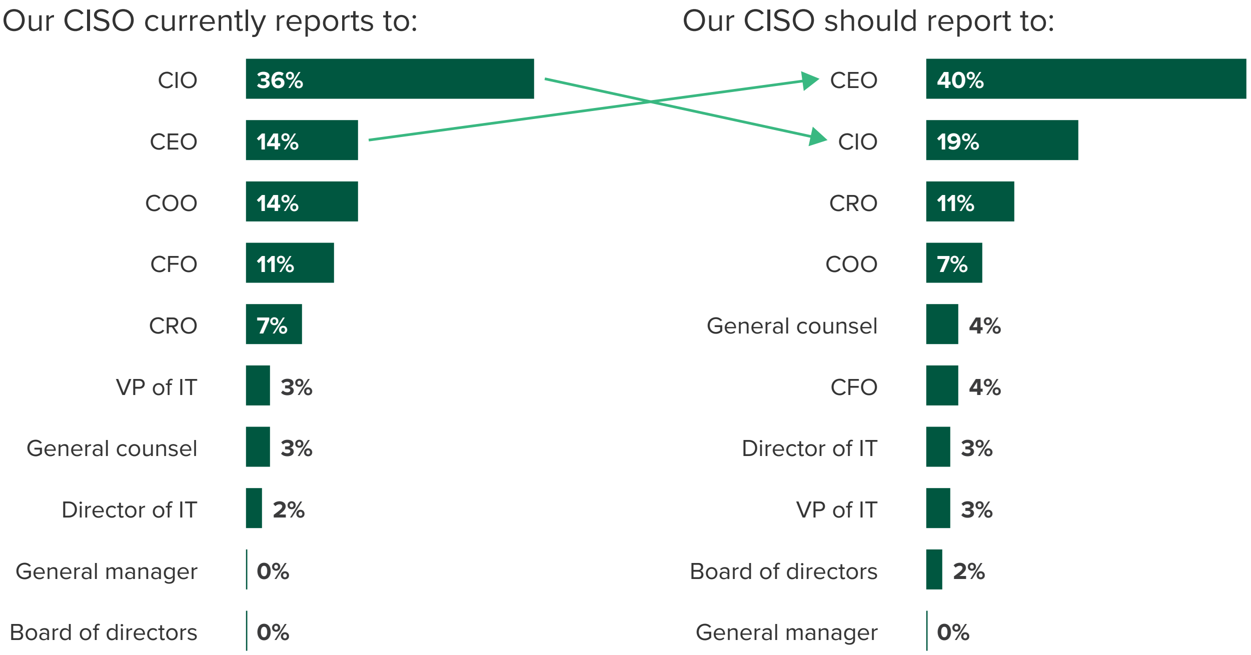
Regardless of role level, IT and Security teams are feeling the harsh consequences of communication silos — whether through lack of communication/collaboration tools shared across teams or lack of effort.

C-LEVEL PERSPECTIVES ON KEY CHALLENGES

While many challenges are shared, the C-suite faces unique hurdles. When looking at C-suite challenges we found that:

- **Differing career advancement opportunities are top of mind for all levels, but particularly for the C-level due to reporting structures.** In fact, C-level executives cite differences in career advancement opportunities as the top negative impact on collaboration between IT and Security counterparts (see Figure 1). For the C-level, much of this struggle lies in their reporting structure. While most CIOs report directly to CEOs, more than twice as many companies say that their CISOs report to the CIOs (36%) rather than the CEOs (14%) (see Figure 2). Even though CISOs are given a chief officer title, they are one step more removed from the CEO than CIOs typically are, and this might contribute to more dissatisfaction. Despite the current organizational structure, many CIOs (44%) and CEOs (44%) agree that CISOs should report to CEOs. Many see this as a win-win situation as CISOs would have better career prospects and CIOs would no longer have to shoulder the responsibility (and liability) of having Security roll up to them.

Figure 2: CISO Reporting Structure



Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

When asking C-suite professionals about their opinions on this, they said it often comes down to the person in the role and the person they will report into. For example, if the CEO is not security-minded, then a CIO would likely be a better boss for a CISO. If a CIO and CISO are at odds, then a separate structure could be better.

"Who should the CISO report to?"

"It doesn't matter as long as who they report to enables them to do their job. . . . And that doesn't mean a blank checkbook and things like that, but it means that the CISO can be effective at mitigating risk and protecting their company and their enterprise."

CIO of energy corporation in the US

"As a CISO, does it work out well that you report to your CIO rather than the CEO?"

"I would say it's working out well in this instance, but that's only because I have a CIO who is very concerned about security and therefore allocates a significant portion of his budget to security. I've talked to peers who have been in relationships where the CIO was not so forward-thinking, and they got starved on the budget side and there was little they could do about it. So, it kind of depends on who sits in that seat."

CISO of a tech solutions organization in the US

"How do you see reporting structures changing in the future?" (Asked to CISO who reports to CIO.)

"[I see] either a direct-reporting relationship to the CEO or to another member of the C-suite. Interestingly even my CIO — my boss — suggested that the CEO might be a better reporting relationship for me for that very reason. Because on the accountability side, he feels like he's got to make these decisions in terms of resource allocations, and he doesn't necessarily want to make that choice. If he lowers Security's budget, then he's concerned that if there's an issue, it's going to come back on him. If he increases it, he may not be able to deliver. And his primary objectives are delivering innovation, the new product, and so on. So he feels, I think at times, uncomfortable making those kinds of decisions and would rather see me report either directly to the CEO or another member of the C-suite so he can be focused solely on his objective."

CISO of a tech solutions organization in the US

Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

- **Board visibility is a source of tension for CIOs and CISOs.** The inherent nature of C-level executives means that they face additional pressures of ultimately being held accountable to their boards for all corporate actions and events. Based on their interactions with their boards, CIOs and CISOs report that the top three most important items to their boards are:
  - Brand protection (81%)
  - Security threats and risks to the business (78%)
  - Reducing risk and exposure (77%)

  While the VP/below group is rarely or never present in these board meetings, the CIO and CISO shoulder the overwhelming responsibility for company protection. In the words of one CIO:

> “The board trusts that I’ve got a plan and that I’m handling it, which is good and bad. My biggest fear in my role as CIO is that the leadership says, ‘Oh, he is taking care of it. We trust him.’ And I’m like, ‘Look, it’s not if we’re going to get compromised. It’s when. Okay?’”
>
> *CIO of energy corporation in the US*

Additionally, CIOs report getting slightly more time with their boards than CISOs during the course of a year (CIOs average 8.1 hours per year and CISOs average 6.8 hours). Furthermore, CIOs are usually present with CISOs when they address the board. That creates a large conflict of interest, particularly for those CISOs who report to their CIO. When asked if there was a conflict of interest in a CIO’s presence during a CISO’s board presentation, one CISO noted:

> “I don’t think you’ll find a single CISO who doesn’t say that there’s some kind of conflict of interest.”
>
> *CISO of a tech solutions organization in the US*

While some CISOs have additional checks and balances in place (i.e., a dotted line to an audit committee) to report any discrepancies, one CISO reported that it would be a risky career move unless the situation were dire:

The presence of the CIO at CISO board presentations often creates a conflict of interest.

> “I have a lever that I can pull. I can go to the head of the audit committee of the board and say, ‘Hey there’s a problem.’ Now, would I actually pull that lever? I would have to be pretty fed up with the situation to do so because, politically, that would probably not be good for me from a career perspective.”
>
> *CISO of a tech solutions organization in the US*

The board pressure to reduce risks and maintain uptime, compounded by potential conflicts of interest in board meetings (particularly for CISOs), creates a tension that is unique to the C-suite.

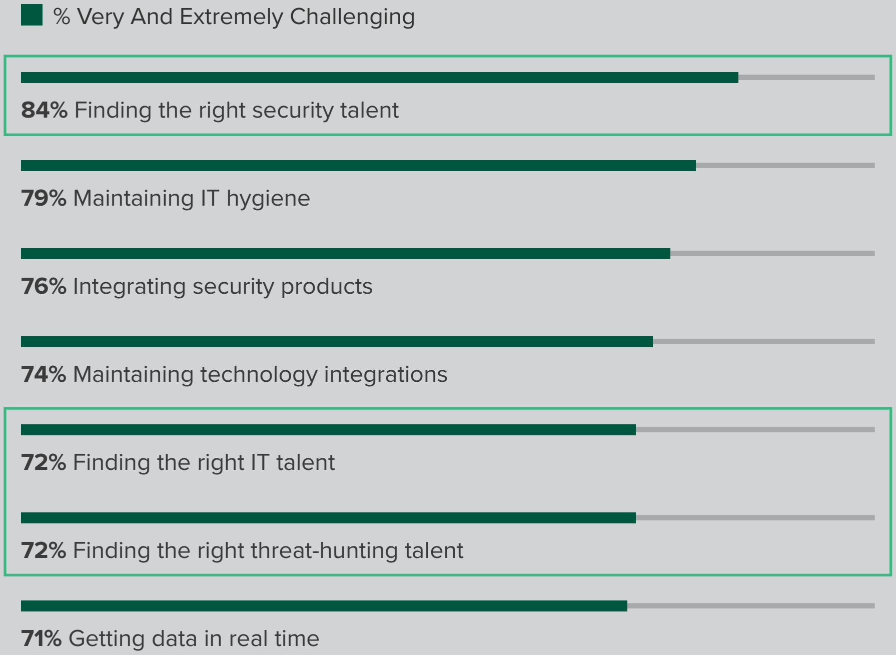
- **C-level executives struggle to find skilled employees due to talent shortages.** In the current workforce, there is a shortage of skilled IT and security professionals, and this serves as a major challenge for C-level executives looking to fill critical roles on their teams. This issue is a global challenge, particularly in the security space as expressed in this quote:

  > "There's a massive shortage. There's no doubt that there's a shortage of resources and expertise in the security domain. I think it's getting better, but very slowly. In the Canadian market, there are now universities that are focusing on dedicated programs around security. In Ontario, they're actually building a dedicated university or college around cyber, which is fantastic. The US has an improving space, but it's still very challenging to hire the right resources. In Australia, it's almost impossible. . . . And in the UK, [experts are] very difficult to find. So, there's definitely a global shortage of expertise in the security domain."
  >
  > *CIO of a tech solutions organization in the US*

  In fact, finding the right security talent is the top challenge of C-level executives, with 84% citing it as very or extremely challenging (see Figure 3). It is no surprise that finding the right talent represents three of their top seven challenges.

Figure 3: Challenges Of Talent Gaps

Top 7 Most-Challenging IT And Security Tasks For C-Level Professionals



Base: 480 IT and security C-level professionals (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

Despite the hiring challenges, the C-suite still has a stronger focus on finding skilled talent to fit evolving needs (70%) rather than focusing on reskilling current employees to do so (64%). As a result, C-level executives are taking measures to attract talent and retain or hire, and that includes increasing salaries and benefits in order to attract better talent (76%) and hire entry-level talent to train. One CISO noted that the talent shortage has led to a change in hiring tactics:

> "We hired a lot more entry-level folks and then just trained them up, and we hired a lot of people who are not cybersecurity professionals and then we added cybersecurity skills after we brought them over. We still hire experienced cybersecurity people, but it's a lot less as a proportion of the overall hires than [it used to be]."
>
> *CISO of a tech solutions organization in the US*

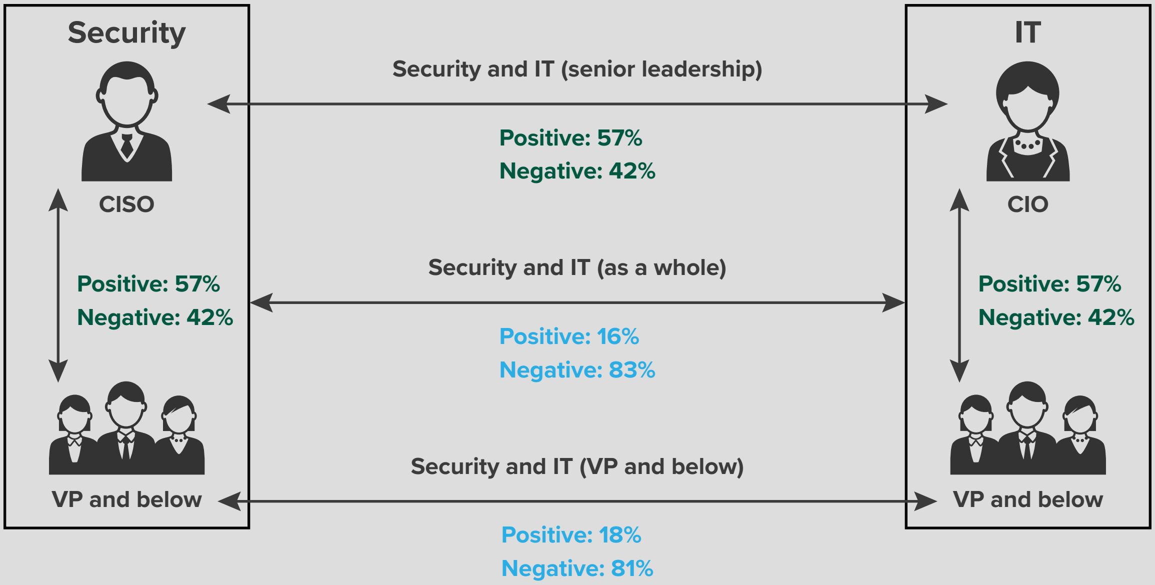
The C-suite can be distracted by internal challenges such as board pressures, career advancement hinderances, and talent shortages, shifting its focus away from critical issues such as security risks and IT threats.

VP/BELOW PERSPECTIVES ON KEY CHALLENGES

It is no surprise that the VPs, directors, and managers who report to the C-Suite face unique challenges as well. In a look at VP/below challenges, found that:

- **Negative relationships impact the VP/below groups to a significant degree.** Even though relationships between the C-level and the VP/below groups are not great, they tend to be significantly better than the relationships between the VP/below group in Security and their peer group in IT. When C-level peers work at odds with each other, the practitioners under them feel the conflicting goals and communication gaps the most, adding a major strain on their relationships amidst competing objectives.

Figure 4: Nature Of IT And Security Relationships



Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

- **Understaffed teams and talents gaps bog down employees.** The talents gaps and staffing challenges lead to employees spending a lot of time training. Although the C-level prefers to hire skilled employees, the talent shortage often leads them to hire entry-level candidates to train or to reskill internal employees. However, the C-suite rarely shoulders the responsibility of educating and training these new employees. This often leaves the VP/below group in a constant cycle of educating and reskilling employees, and that distracts them from other critical operational tasks.

  A significant number of teams (64% of Security teams and 53% of IT teams) also report being understaffed. However, C-level executives are out of touch with staffing needs, further exacerbating the issue. While 65% of the VP/below group report having understaffed IT or Security teams, only 49% of C-level employees report the same for those teams. The VP/below group feels a much greater stress from being understaffed, as those employees tend to be executers of tasks, and they can see just how difficult execution is with limited resources. The C-suite is also constantly fielding requests from the bottom-up for more tools, staff, and dollars. Perhaps they are not taking staffing requests as seriously, but instead focusing on bigger picture goals.

C-level executives are out of touch with staffing needs.

- **Practitioners are dealing with disjointed and unsatisfactory tools.** On average, companies have 27.4 different security products. Members of the VP/below group are the primary executers and operators of IT and security tools within organizations. However, only 34% are working with mostly or completely integrated security solutions. This leaves two out of three professionals struggling with nonintegrated solutions that can't, for instance, seamlessly share data. Even those who claim to have a unified strategy have not consolidated critical items across teams. Reported areas of consolidation include:
  - Technology based on SIEM tools (65%)
  - User interfaces (58%)
  - Data products/tools (54%)
  - Compliance based on audit (49%)
  - Operational processes based on SOCs (37%)

  Ideally, all of these things would be consolidated (near 100%) across teams to truly signify unification. However, teams are willing to settle for much less than across-the-board consolidation while still considering it a unified strategy. Based on these findings, it appears that having just a few of these things integrated makes respondents feel as though they are unified, although this may only be minimally true.

  Dissatisfaction with this disparate toolset is high. In fact, only 52% report being satisfied with the performance and security coming from their existing enterprise firewalls. That's a major concern since those are some of the most established and long-standing security solutions in their toolsets.

Only 34% are working with mostly or completely integrated security solutions

Staffing challenges, negative relationships, and disjointed tools plague the day-to-day performance of managers, directors, and VPs of IT and Security teams.

Consolidated Strategies Help Address Relationship Woes

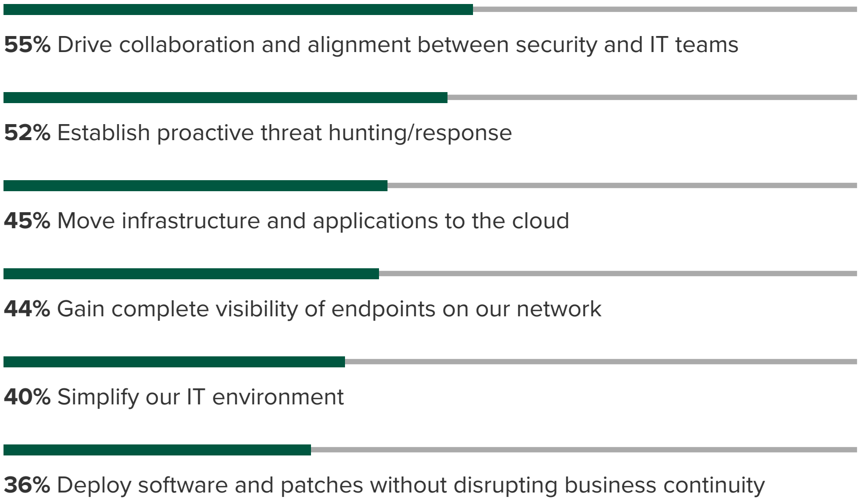
Strained relationships and diverse challenges between the C-suite and VP/below level teams can place major hurdles in the way of collaboration. However, when looking at how companies attempt to overcome these issues, we found that:

- **Companies are focused on turning around strained relationships.** Despite the strained relationships that persist, companies are aware of their issues and are actively focused on trying to drive collaboration and alignment. In fact, when given a list of 14 priorities for their IT organizations, both the C-level group and the VP/below group ranked driving collaboration and alignment between IT and Security teams as the top priority (55%). That's above other critical tasks such as establishing a proactive threat-hunting response, moving to the cloud, and gaining visibility into endpoints (see Figure 5). It is apparent that these teams understand that the collaboration must be in place for all other critical tasks to be effective within their organizations. In fact, 65% agree that their organization has taken measures to strengthen the relationship between IT and Security.

Both C-level executives and the VP/below group rank driving collaboration and alignment between IT and security teams as their top priority.

Figure 5: Top Priorities Of IT Organizations

"Which of the following initiatives are likely to be your IT organization's top priorities over the next 12 months?" (Top 6 shown.)



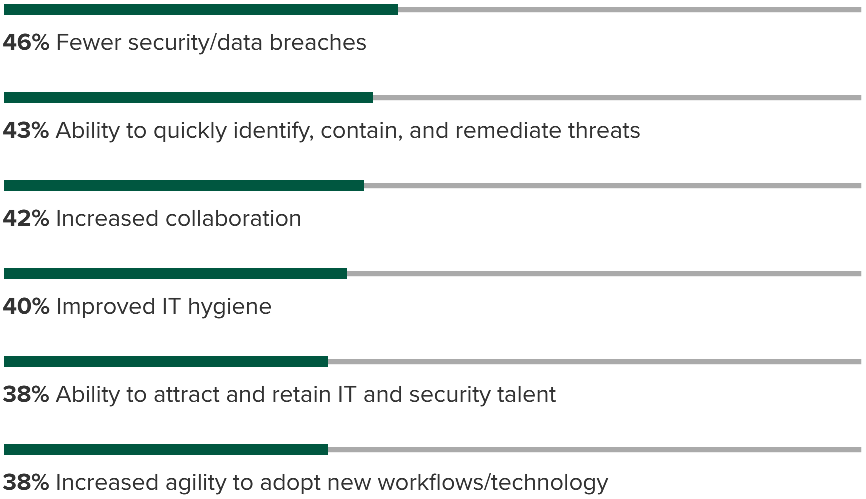
Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

- **Organizations are moving to a unified and consolidated strategy to address critical issues.** While only 30% have already implemented a unified and consolidated IT management and Security strategy, 41% of organizations are planning to implement one within the next 12 months and another 23% are interested in doing so. The move towards this approach is a clear acceptance of the profound perceived benefits that can come from such a move (see Figure 6). In addition to reducing data breaches and threats (which are top priorities of boards), a consolidated strategy helps increase collaboration to reduce internal tensions and attract IT and Security talent in a tight hiring market.

64% are interested in or planning to implement a unified and consolidated IT management security strategy in the next 12 months.

Figure 6: Benefits Of A Consolidated Strategy

"What are the benefits of a unified, consolidated IT management and security strategy?"



Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

As companies work to address internal tensions between IT and Security, they are increasingly looking to unified strategies to help address key challenges, both internal and external.

Key Recommendations

IT and Security have both evolved into fields that require multiple skillsets to successfully engage with an ever-expanding set of internal and external stakeholders and enable the business. Years of hyper-growth and teams with skillsets in high demand and vital roles within enterprises have resulted in strained relationships, which can prevent organizations from achieving desired goals.

Forrester's in-depth survey of IT and Security professionals yielded several important recommendations:

Emphasize collaboration and communication to help overcome the legacy of past problems. C-level executives, along with personnel at the VP/below level agree that breaking out of communication silos and bridging communication gaps are necessary prerequisites for IT and Security to work together to accomplish their common strategic objectives.

Unify the strategy between IT and Security to reduce the tension between practitioner teams. Developing a clear forward path for IT and Security that reinforces their shared mutual goals will help make both parties successful and will also smooth out any perceived tensions that may come from career concerns. A unified strategy helps prove the objectives and targets to confirm that a rising tide lifts all boats.

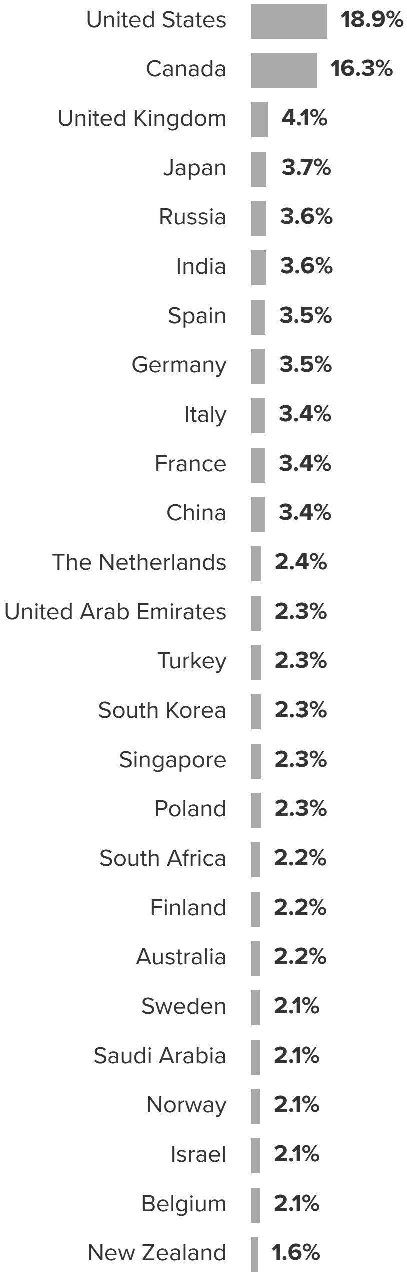
Fragmented tools and technologies exacerbate tensions between shareholder teams. Data and communication silos along with the sheer number of tools and technologies prevent IT and security professionals from aligning. Others may perceive them as slow, apathetic, or hostile. But, in reality, it is the need to bounce back and forth between infrastructure, databases, and user interfaces that is a key part of the problem. Having a consolidated toolset that serves both the IT and Security teams allows them to operate from a single source of truth. That enables collaboration, faster response times, and fewer data discrepancies. A unified strategy must also focus on eliminating the tool sprawl and address the attention drain that it causes.

Appendix A: Methodology

In this study, Forrester conducted an online survey with 1,451 manager level and above IT and Security respondents at global organizations across industries to evaluate the relationship between IT and Security teams, as well as the challenges and benefits of having a unified, consolidated IT management and Security strategy. Forrester also conducted 8 qualitative interviews with CIOs and CISOs about this topic. The study was completed in February 2020.

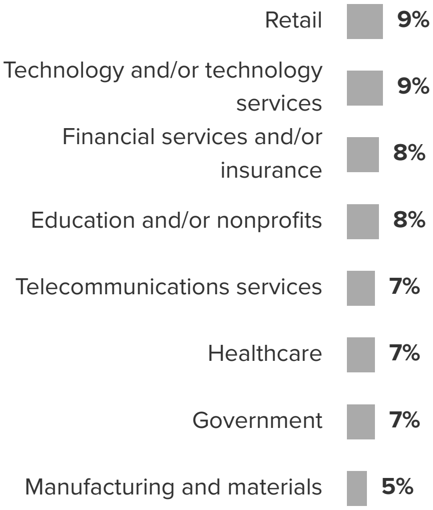
Appendix B: Demographics/Data

COUNTRY/REGION

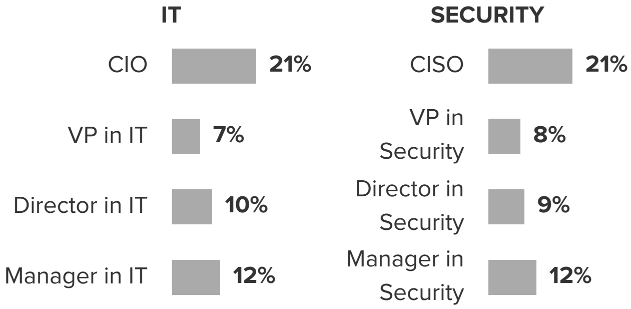


EMEA: 46%
North America: 35%
APAC: 19%

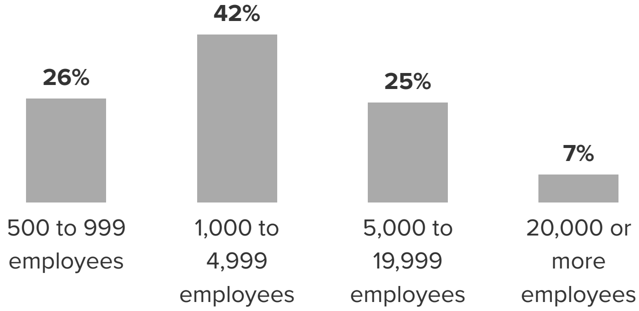
TOP INDUSTRIES



RESPONDENT ROLES



COMPANY SIZE (BY EMPLOYEES)



Base: 1,451 IT and security managers and above (including CIOs and CISOs) with responsibility for security strategy and decision making
Source: A commissioned study conducted by Forrester Consulting on behalf of VMware, February 2020

To read the full results of this study, please refer to the Thought Leadership Paper commissioned by VMware titled "Tension Between IT And Security Professionals Reinforcing Silos And Security Strain"

Project Director:
Emily Drinkwater,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk
research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.