SEC
Security Executive Council
A research and advisory firm

KENNESAW STATE UNIVERSITY
INSTITUTE FOR CYBERSECURITY WORKFORCE DEVELOPMENT

Security Optimization

Looking Beyond Traditional Definitions of Convergence

A Security Executive Council's Security Leadership Research Institute Report

Contents

Introduction

In the second half of 2021 the SEC partnered with Kennesaw State University to explore the idea of conducting a research project on the forms of cyber and corporate security collaboration.

The SEC works with many security leaders. In casual conversations we noted there appeared to be successful programs that were officially "converged" organizationally and successful programs that had strong partnerships between cyber and corporate security. At the early stages of this project, we discussed the possibility there is a continuum of convergence that goes beyond the idea that convergence is structured as one unit with one leader within the organization.

As early work progressed, we adopted a concept that better informed our research. For this study we use the term security collaborative optimization (SCO). The research question we were trying to answer was how collaboration influences security optimization, and whether one structure over the other equates to more optimization. We started with definitions of three main structures that occur. In both an online survey and later for a subset of participant interviews we asked security practitioners to identify how cyber and corporate security interacted.

Question options used in survey question:	Descriptions used for interviews:
Option 1: **Merged**	**Merged:** Corporate and Cybersecurity are merged into an organizational unit such as a department or division and collaborate on all or most programs and administration.
Option 2: **Separate with partnerships**	**Partnered:** Corporate and Cybersecurity are separate organizational units but formally collaborate and partner on all or most routine operational issues.
Option 3: **Separate without routine partnerships**	**Ad Hoc:** Corporate and Cybersecurity are separate organization units that do not routinely collaborate or partner on a regular basis but may do so when a situation forces the need.
Option 4: **Other**	**Other:** Some other approach.

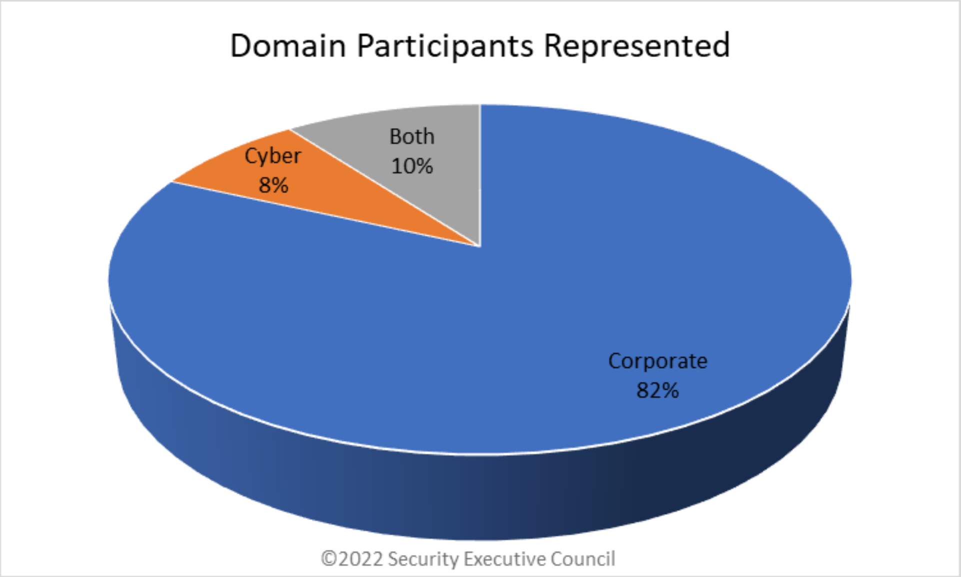
From November 2021 to June 2022, the request for participation for the study was broadcast to security practitioners via the SEC Insight newsletters, SEC social media channels, and direct email invites to SEC clients (approximately 60,000 practitioners in total). Our research partner, KSU, sent it to 255 academic researchers and 273 industry partners from their speakers recruiting list.

This initial phase of the research was broken into two information-collecting efforts: the quantitative and the qualitative. For the quantitative research effort, we sent participants an online survey that captured demographics and some initial questions about security structure in the organization and corporate culture. Then, for the qualitative effort, 21 survey respondents were interviewed to drill deeper into the factors that informed their state of security convergence or SCO. The online survey led us to a list of possible questions to center the interview discussions. Not all questions were covered in all interviews. Participants were asked to select their level of convergence on the online survey and were asked to verify that selection in the interviews. There was only one case were the participant changed their original selection, which was from Merged to Partnered.

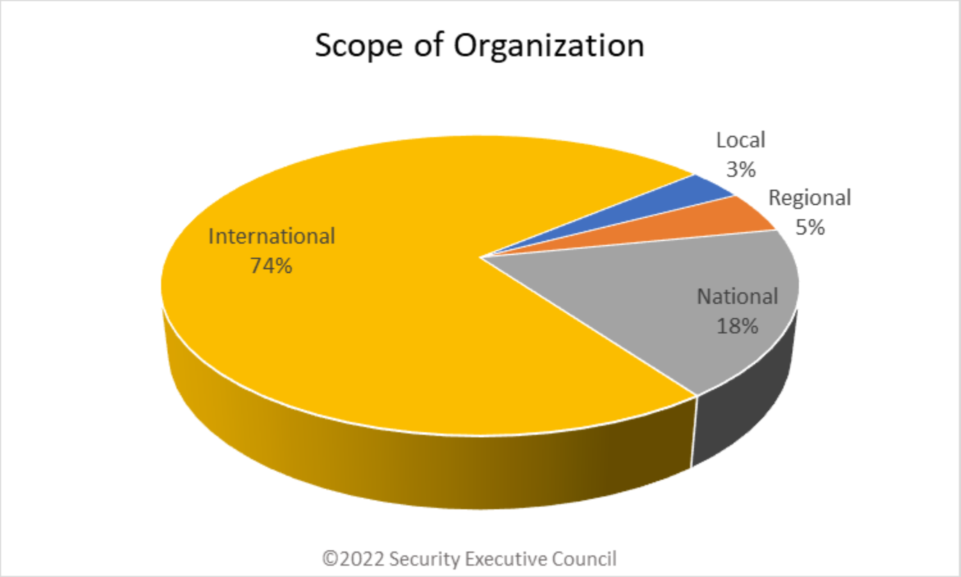
Section I: Online Survey Results

The online survey consisted of 26 questions.

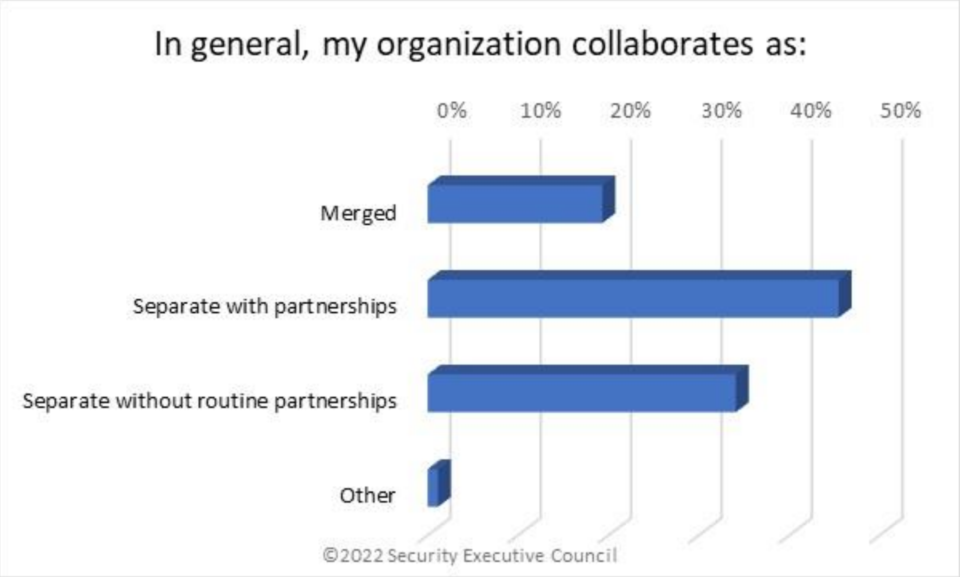
One hundred twenty participants filled out the survey. Of those, 88 were accepted as useable data. (Responses were discarded if the respondent was not a security practitioner or, they filled out the survey more than once or if they answered only a few questions.) Not all participants answered all questions.



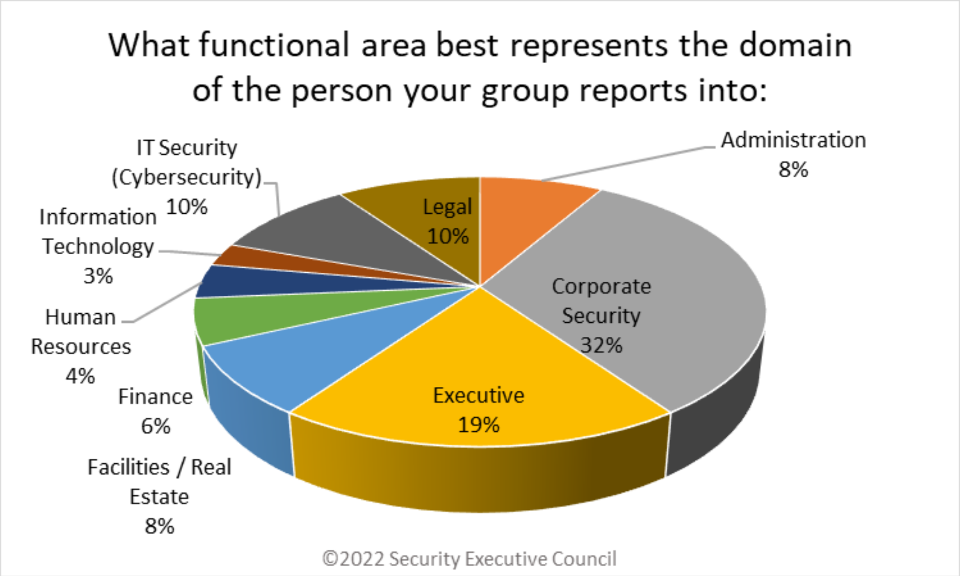
The majority of respondents came from the corporate security realm.



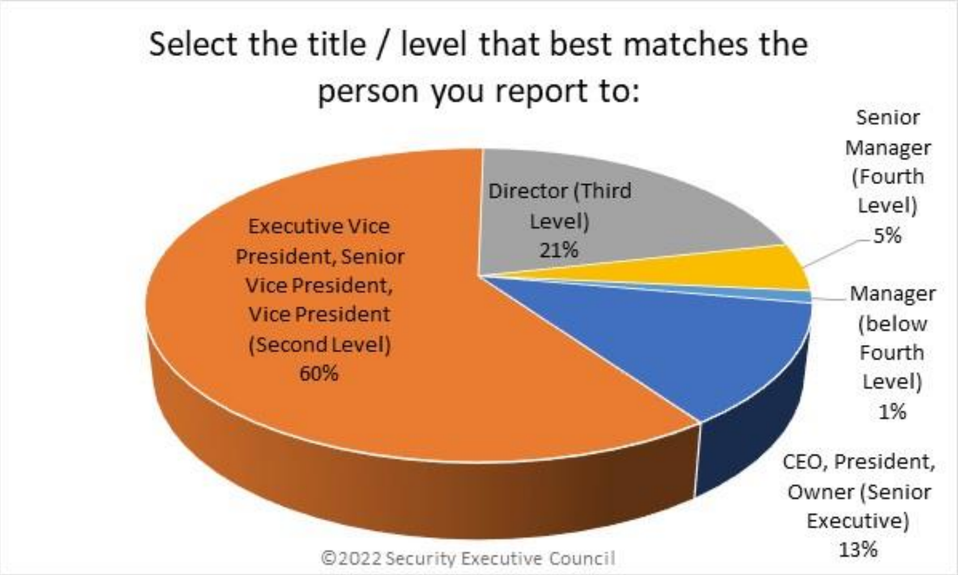
Most respondents (74%) came from organizations with international, rather than national, local, or regional, operations.



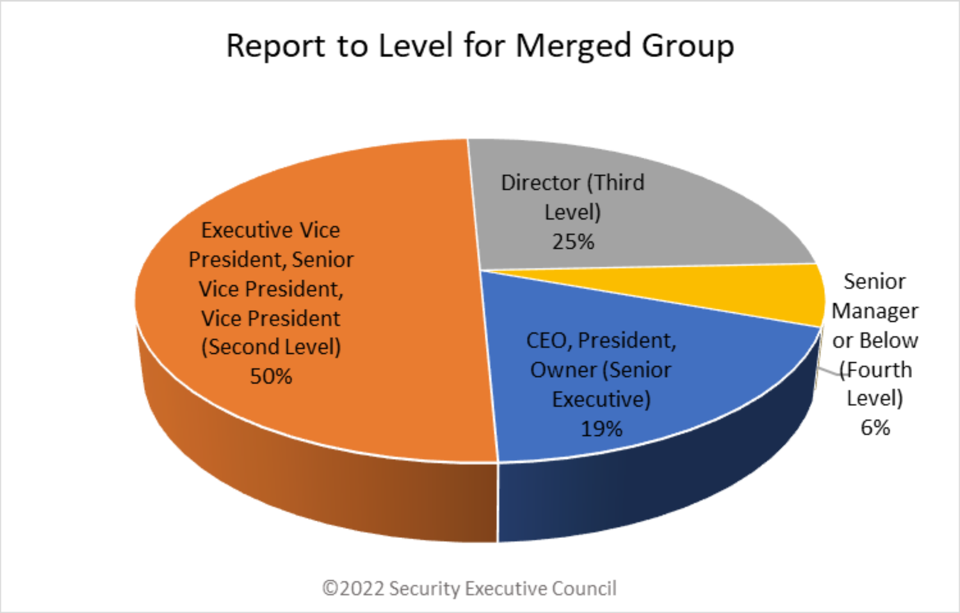
"Separate with partnerships" was the most common collaboration form at 45%, followed by "Separate without routine partnerships"/Ad hoc (34%) and "Merged" (19%)



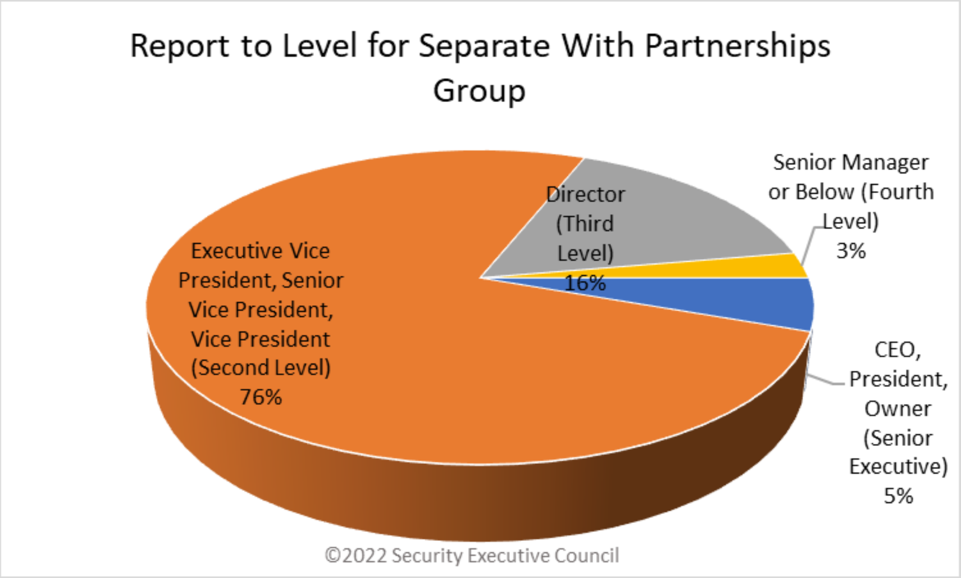
Respondents reported into a variety of functional domains. Corporate security was the most common (32%), followed by Executive (19%), Legal and IT Security (10% each), Administration and Facilities and Real Estate (8% each), Finance (6%), HR (4%) and Information Technology (3%).



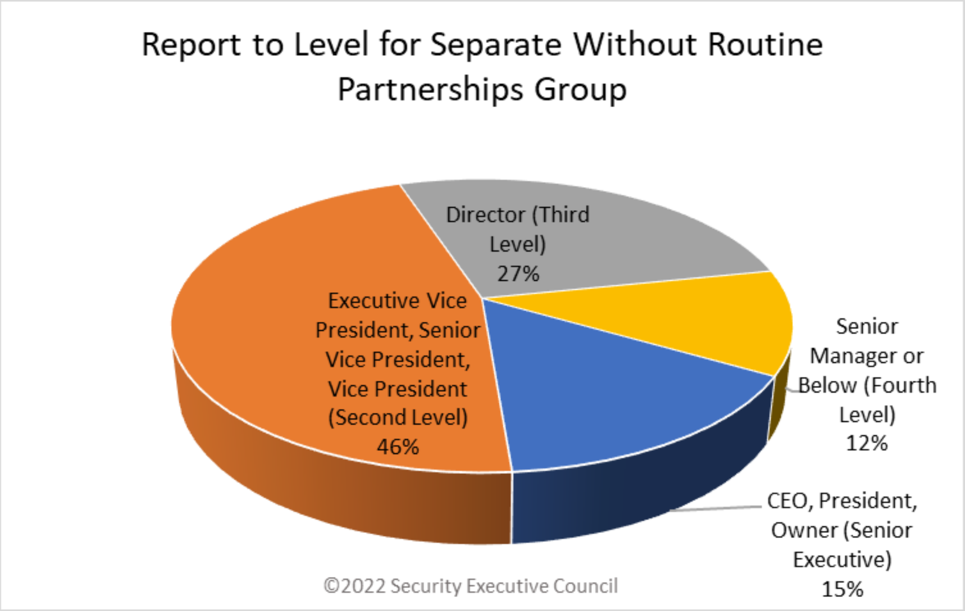
Overall, sixty percent of respondents reported to the EVP/SVP/VP level. Twenty-one percent reported to the Director level, and 13% reported to senior executives.



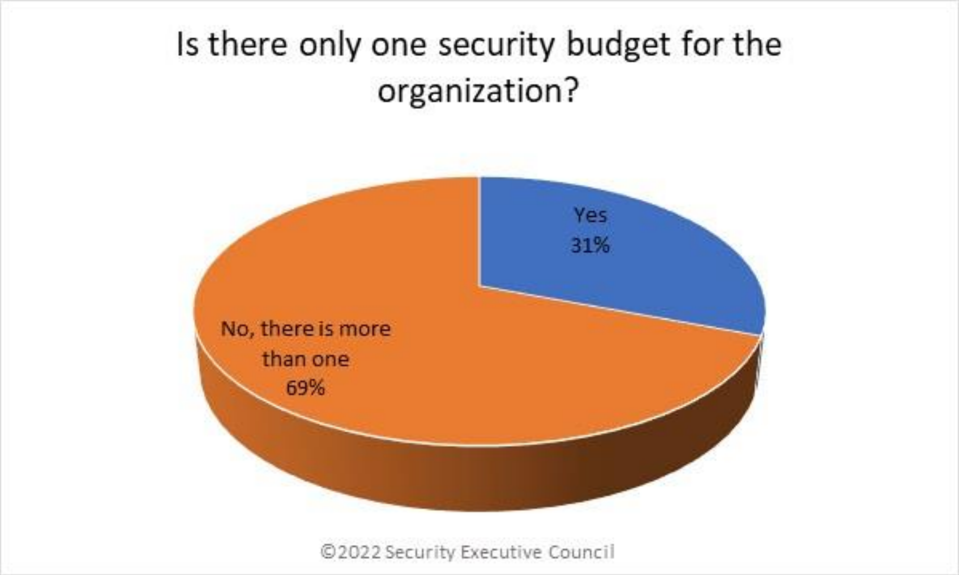
Of the respondents self-identified as Merged, half reported to the EVP/SVP/VP level. Nineteen percent reported to a senior executive, and 25% to the Director level.



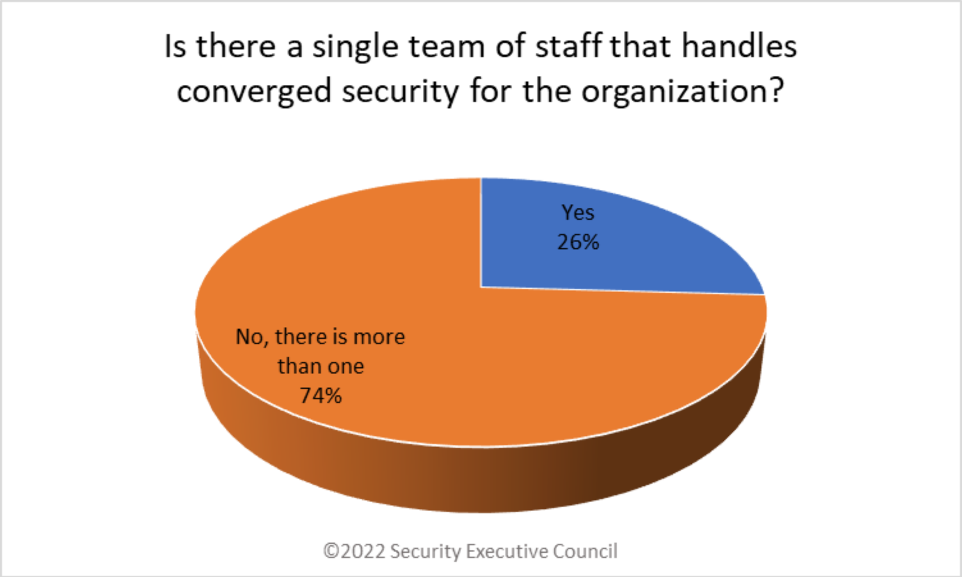
Of the respondents self-identified as Separate with Partnerships, 76% reported to the EVP/SVP/VP level and 16% to the Director level. Only 5% reported to a senior executive.



Of the respondents self-identified as Separate Without Routine Partnerships, 46% reported to the EVP/SVP/VP level. Fifteen percent reported to a senior executive, and 27% to the Director level.

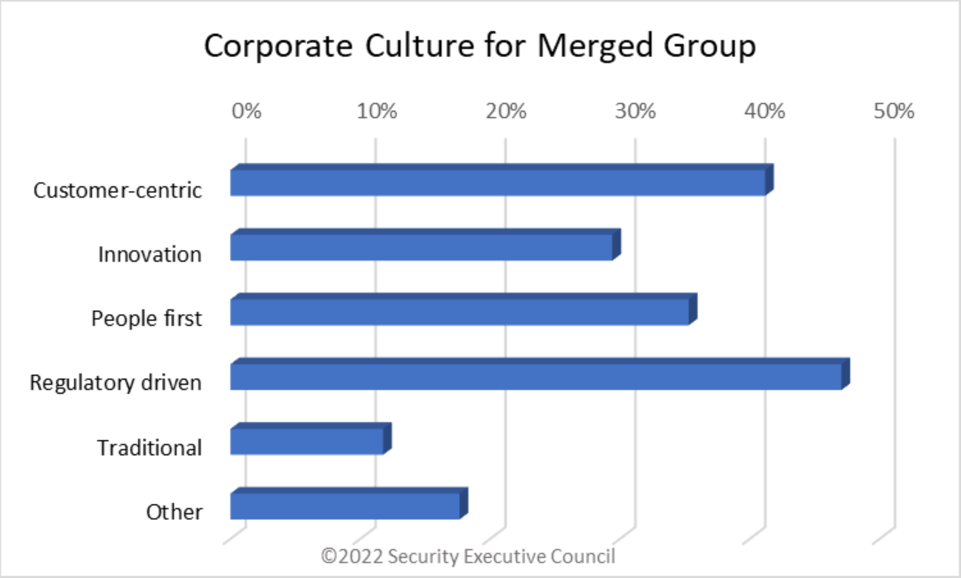


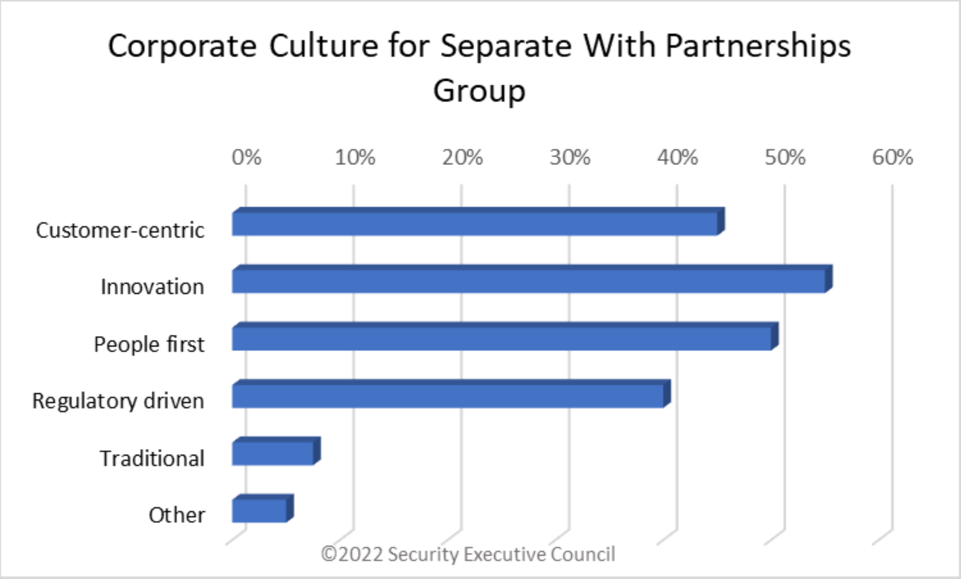
Nearly 70% of respondents reported that their organizations maintain separate budgets for different security functions.

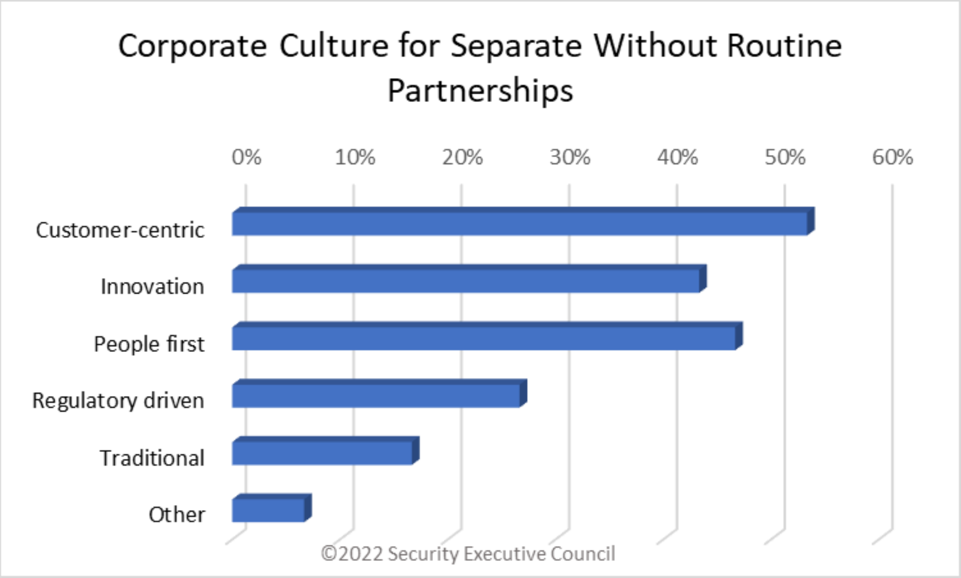


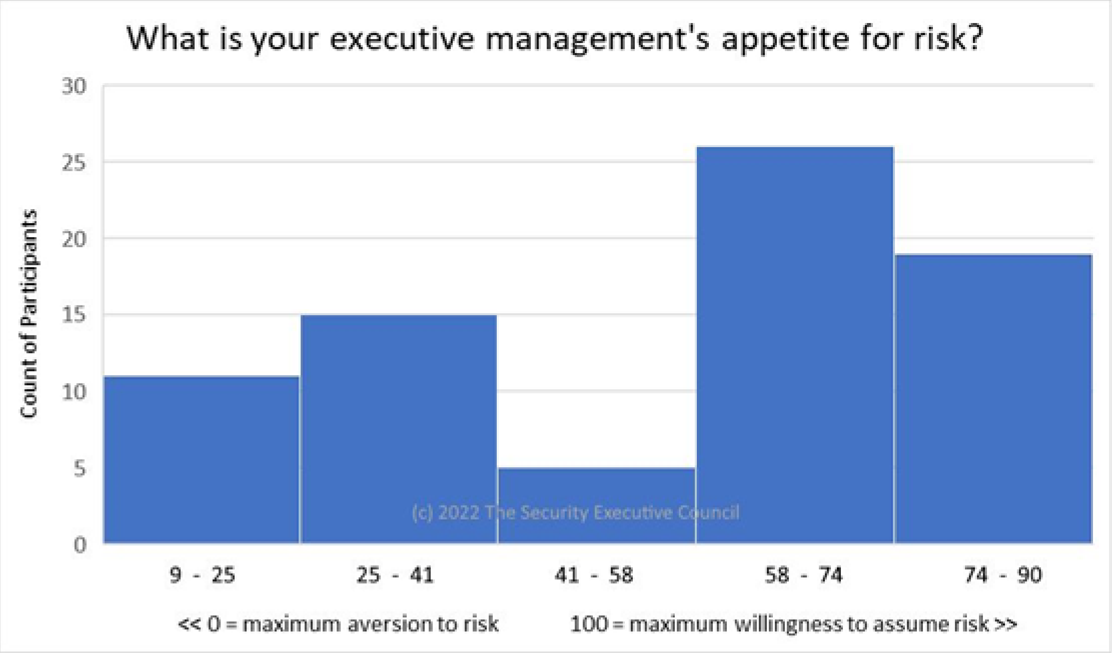
Seventy-four percent said more than one team handles security for the organization.

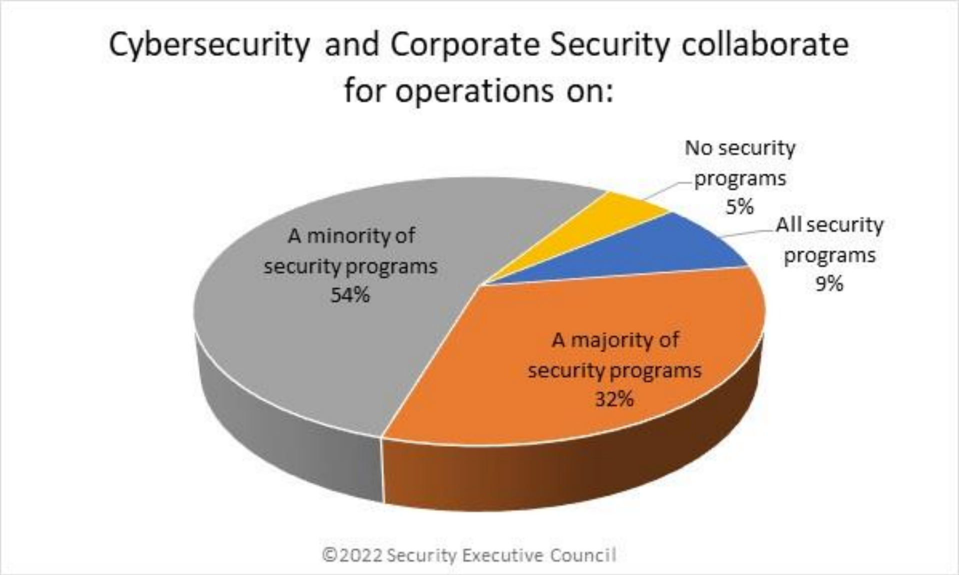
The following charts show how the three groups characterized their corporate culture. The Merged group's top two descriptions for their culture were Regulatory Driven (which fell into fourth place in the other two groups) and Customer Centric. In the Separate with Partnerships group, the culture was most characterized as Innovative, with People First and Customer Centric close behind. The Separate Without Partnerships group identified their culture as Customer Centric, closely followed by People First and Innovative.


Corporate Culture for Merged Group
0%
10%
20%
30%
40%
50%
Customer-centric
Innovation
People first
Regulatory driven
Traditional
Other
©2022 Security Executive Council

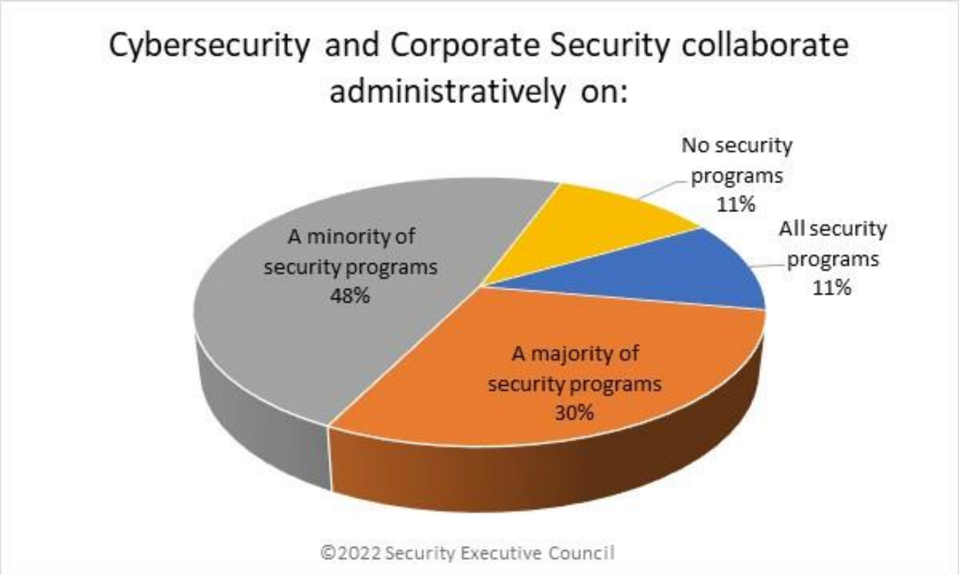

Corporate Culture for Separate With Partnerships Group
0%
10%
20%
30%
40%
50%
60%
Customer-centric
Innovation
People first
Regulatory driven
Traditional
Other
©2022 Security Executive Council


Corporate Culture for Separate Without Routine Partnerships
0%
10%
20%
30%
40%
50%
60%
Customer-centric
Innovation
People first
Regulatory driven
Traditional
Other
©2022 Security Executive Council

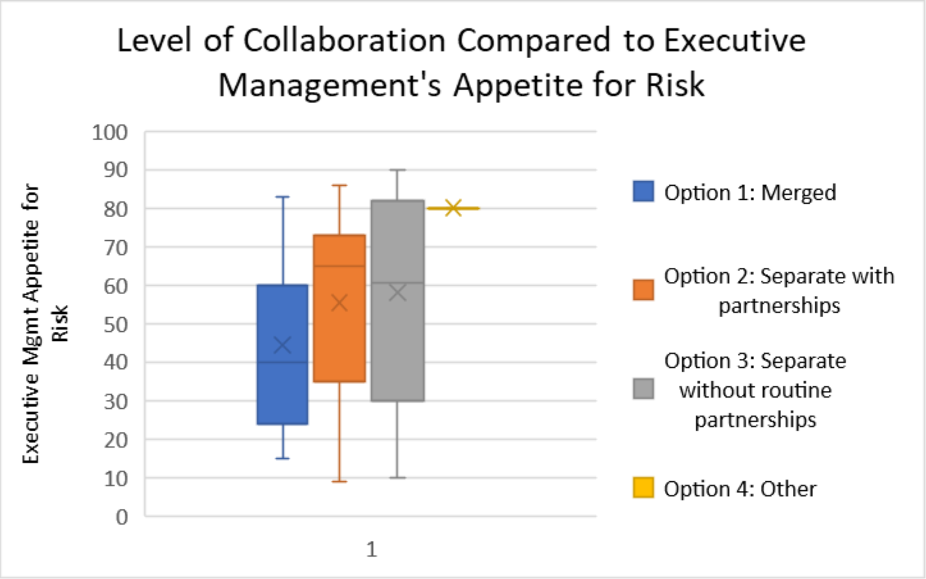

What is your executive management's appetite for risk?
Count of Participants
30
25
20
15
10
5
0
9 - 25
25 - 41
41 - 58
58 - 74
74 - 90
<< 0 = maximum aversion to risk
100 = maximum willingness to assume risk >>
(c) 2022 The Security Executive Council



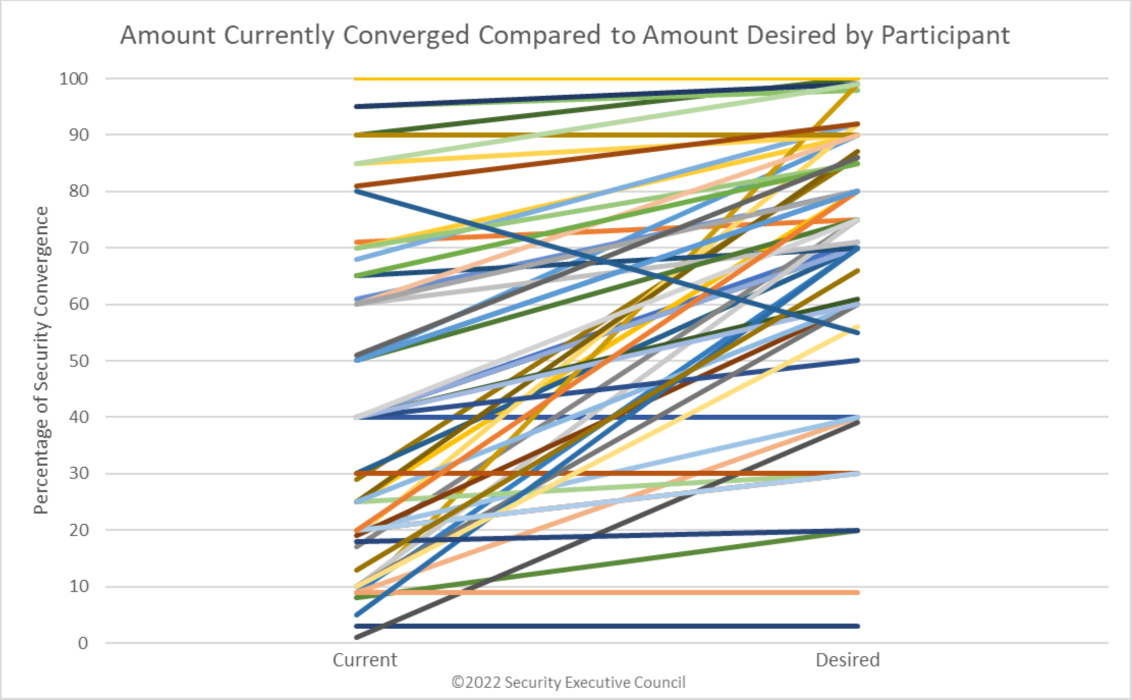
Eighty-six percent of respondents collaborate on operation for some security programs – 54% on a minority, and 32% on a majority. Only 9% collaborate on all security programs, and 5% collaborate on none.

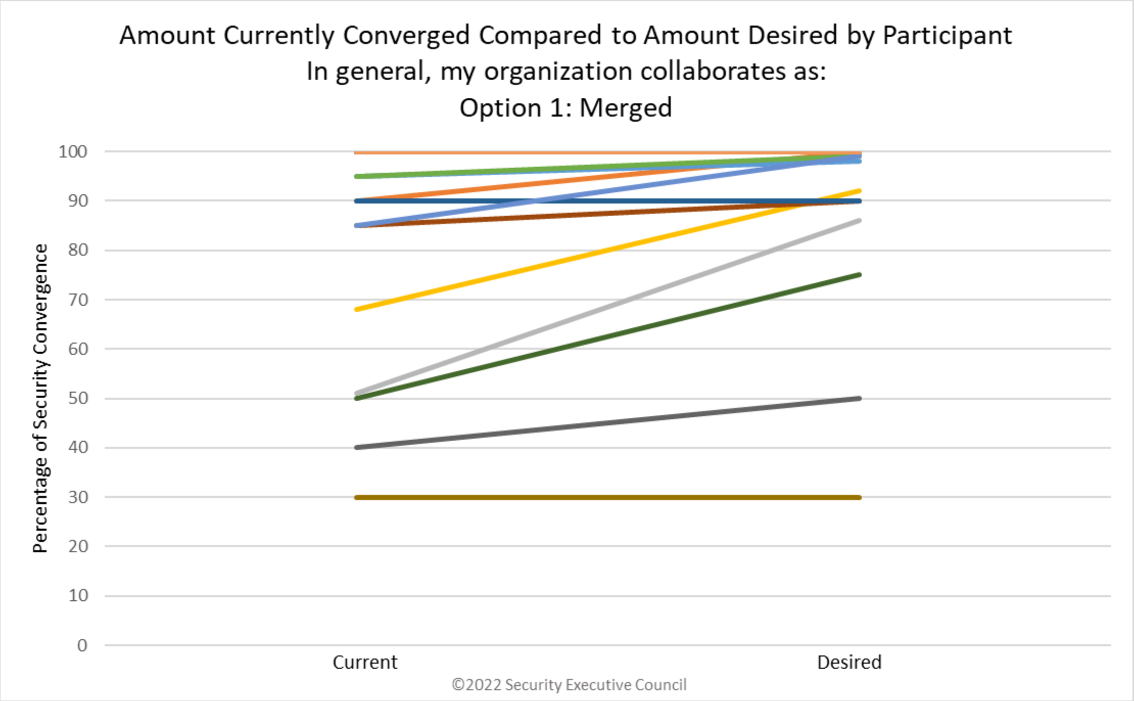


Administratively, the trend is similar. Seventy-eight percent collaborate administratively on some security programs, while 11% collaborate on all and 11% on none.

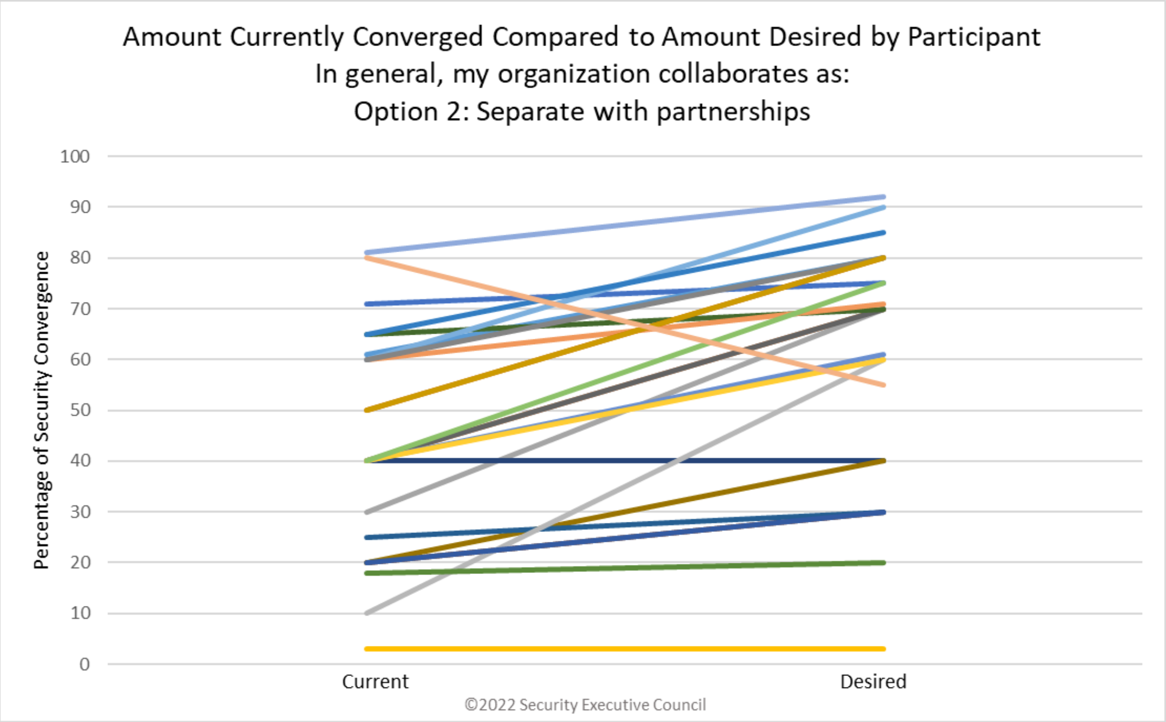


Merged appears more risk adverse, which may be a reason the organization has a merged structure.

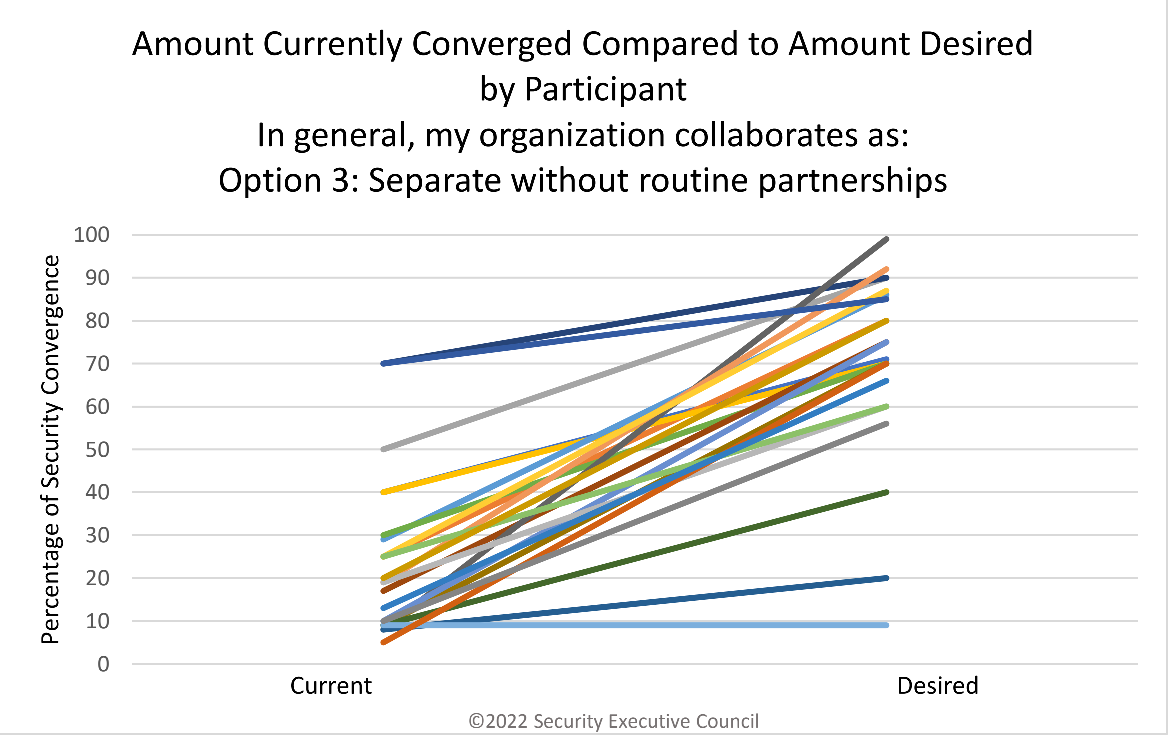




Respondents identifying as Merged desired similar or slightly more “convergence” than they currently have.



Respondents identifying as Separate with partnerships generally desired more “convergence” than they currently have, though some desire no change and one desired less.



Nearly all respondents without routine partnerships desired more formal convergence than they currently have.

Section II: Interview Results

Thirty-one people were invited for an interview after the survey results were complete. We interviewed 21 of those.

Level	**Invited**	**Participated**
Merged	8	7
Partnered	14	11
Ad Hoc	9	3

Definitions of the collaboration structures are listed again in the sidebar. For brevity in this section of the report, we called these groups Merged, Partnered, Ad Hoc Partnerships and Other.

Because we only had three interviews with participants identifying as Ad Hoc Partnerships, the data was not rolled up, but suffice it to say, none seemed to think their current structure was a good one, and two are no longer with the company they were with when we interviewed them. Merged and Partnered categories also included one participant each that was not happy with the current structure.

Common Themes

At a very high level we heard some common themes across Merged and Partnered participants that likely have an impact on SCO.

- Good relationships are key to the structure working.
    - Partnered: “I think it all comes down to relationships, too. Having that trust between the two organizations is huge ... The more you meet, I think the closer you become and the more you trust each other… And getting their buy in and support will help us sell what we're trying to do and vice versa.”
    - Partnered: “When I was offered this position as the global head of security, I told my boss that it is essential that global security has a relationship with our cybersecurity elements within business technology. And that if I couldn't be that person, you need to find somebody else that could collaborate in that space… That's how strongly I feel about the topic.”
    - Merged: “I [reported] previously to CISO [who] worked in a vertical, he wouldn't share horizontally. And it wasn't working. It created so many problems that he left [and we got] a new CISO in and it just all went away. So, it is tremendously important that they all have a mutual respect and appreciation for each other's program.”

- Transparency between groups is vital to make it work.
    - Merged: “It's always constructive communication. It's a lot about the personalities as well. Nobody's actually tanking on each other's. It's generally about, well, let's fix this. If there is a problem, let's fix it. And that approach helps a lot. Nobody is playing politics here.”

Collaboration Structures Defined

Merged
Corporate and Cybersecurity are merged into an organizational unit such as a department or division and collaborate on all or most programs and administration.

Partnered
Corporate and Cybersecurity are separate organizational units but formally collaborate and partner on all or most routine operational issues.

Ad Hoc
Corporate and Cybersecurity are separate organization units that do not routinely collaborate or partner on a regular basis but may do so when a situation forces the need.

Other
Some other approach.

  - Partnered: “There's no point in hiding anything we're doing. It just wouldn't make sense… There's an expectation that we're talking where we need to talk and we're sharing where we need to share.”

- Communication is important, but some talked of “two different languages” and a need to work on understanding each other’s language and viewpoint.

  - Merged: “My team does not have a deep knowledge of cyber, but they do have a deep knowledge. And they joke sometimes about when the cyber people talk, like, ‘I didn't bring my decoder ring today. I don't know what they're saying. They say hello, and then I get lost.’ We're spending a lot of time trying to help them understand cyber a bit more.”
  - Partnered: “We can speak pretty frankly, the way most security professionals like to, and they can speak to us as well. [We call each other out on our] jargon. So that we can understand each other. We've got to figure this out. I think the company deserves that. …we're working at it.”

- Most often the move evolution to a better security structure, either Merged or Partnered, was due to unplanned or unforeseen opportunities, for example, a spin off/acquisition, new security leadership, a negative security incident - versus a management decision or formal plan to change or enhance the security structure. The one exception was regulatory requirement.

- Participants expressed difficulty in measuring or detailing the cost or savings of the structure. They focused instead on the ability to identify issues sooner and mitigate faster because the two areas of expertise make a more holistic service. Participants feel like they are less likely to miss threats by working together.
  - Partnered: “Measuring this is hard. We're very weak on KPIs. It's always a nagging level. How do you measure impact in security? So, we have a lot of qualitative things.”
  - Merged: “…it's been hard for us to say, look, because we made this change, now we have this and this saves money or we've got lower risk. We can certainly point to wins along the way. But it's hard to quantify that we saved X number of dollars or anything like that.”

Comparing Lesser Similarities

Beyond the most common themes, a few other similarities stood out.

- Structure benefits:
  Transparency, efficiency, and speed of response were mentioned by participants in both levels. Centralization and single point of contact were mentioned by a few in Merged.

- Level of satisfaction with structure:
  Merged and Partnered participants were satisfied (mostly on the high side) with the structure save for one participant from each level.

- Challenges with structure:
  "People" issues; language barriers. They needed to work on communication with the other side and building trust.

- Key facilitating factors:
  Participants from both levels mentioned executive support and the strength of the relationships between cyber and corporate security leaders and staff.

Differences

There were also some notable differences.

- Which do you think has a larger influence on convergence and optimization – culture or strategy?
  Almost all of Partnered said culture. Most of the Merged participants said it was a blend or that culture and strategy intersect.

- Governance:
  Merged overall was more formal than Partnered. However, Partnered participants talked about keeping each other informed on issues that may impact the other. Several have reoccurring meetings or touchpoint conversations. Most Partnered participants stated they have separate policies, but several said they are familiar with the other side's policies and/or they review each other's policies.

- Do both sides understand each other's risks?
  Many Merged participants had or are still working on it. There was discussion of the two areas of expertise; that they look at things differently and have different languages/jargon. A majority of Partnered said yes, there was an understanding.

- Optimization Objectives:
  This varied widely between the two Levels. There was some commonality in Merged in the area of AI/automation.

Note regarding the question on how participants measure the impact of collaboration:
This question may have been unclear. Merged and Partnered Participants that answered it focused on metrics for certain elements of cyber or corporate security, rather than joint metrics that show the value or impact of the collaborative structure, which was our intended target.

Additional Thoughts from Participants

The last question we asked was: Anything else you would like to add? Following are some quotes of interest.

Merged:

- “If you’re not working for a decision maker or an advisor, you’re not working for the right people.”
- “The Efficiencies and the cost savings is enormous and I don’t think anybody can really argue back on that. Having a security leader being a direct report to the CEO is another way to help with that culture and help drive that.”
- (When asked what would happen if someone came in and started to pull apart the structure): “We continue to work with each other. But as soon as you had people change roles, that would be gone, I think."
- "All of this could have worked as separate organizations if we were just really good at collaborating together, which we did work well. But being in the same organization just takes [it to] another level."
- "So I tried for years to do this [in] another place and due to various changes in the organization over time, interest would increase and then wane. I look at what's been accomplished here and I would love to take credit for it… [but] it takes, I think, the right timing, right opportunity, the right personality match with management."

Partnered:

- “Even when "converged," [we] never had converged budgets. Trust between the two orgs is critical; we have to think about one another and not throw one another under the bus. Meeting together as teams more often is helpful with this. It all comes [down] to relationships.”
- “I think it brings what I would call a calming effect on the business that they realize that regardless of what vector, if there is a security threat to the company, we're going to be dealing with the best way that we possibly can, bringing the best minds to the table and hashing it out, regardless of what titles are out there – VP, CIO, CSO, Head of Security - it doesn't really matter.”
- “Trust is critically important because it helps execs trust that you're bringing unbiased objective analysis and good judgment. Hire for collaboration in your teams. Be willing to speak frankly and negotiate.”
- “We have a lot of trust in our cyber staff and they in us. They know the boundaries. They know when it's something outside of their purview, they're quick to call us and [say] you guys take the lead. We [have] a great process."
- "I am a firm believer that the two disciplines are different enough. They need to be focused on by [the] experts in them, and we shouldn't try and make these experts holistic. There's enough divergence in what we do that the singular focus and expertise we each bring to our job needs to be recognized and appreciated as standalone. "

Section III: Phase 2

We believe that SCO may take several forms. From Phase 1 of this research, we have some themes on what seems to facilitate collaboration optimization, but not much on the outcomes in tangible measures. This will be something we will explore in Phase 2.

For our next step, we will bring practitioners – some that we originally interviewed and others we have not - together in panels for discussions. Clearly we had fewer cyber security participants than corporate security. Some of that is due to the SEC's audience, which is mostly corporate security. We would like to find more cyber practitioners to participate in Phase 2 of the research.

Based on the work in Phase 1, we have many questions yet to be answered, such as:

- How do security leaders measure success via joint metrics to provide ROI on security collaboration optimization (SCO)?
- Are there benefits to having two organizationally distinct security groups?
- If Merged, are there still two distinct staff groups (or more) based on skills?
- Specifically, how much time do cyber and corporate security spend working in partnership? Do both sides need to contact one another or are they already interacting on a formal basis?
- Does their current structure cost more? Cost less? Amount of money saved?
- Are they using or exploring using AI/automation?
- What are the specific drawbacks of their current structure?
- What impact does industry have on their structure (e.g., some utilities require interrelated cyber and physical security plans)?

Future Phases

The research plan includes the creation of an online industry tool security practitioners can use to assess SCO in their organization.

Acknowledgements

Research Team

Greg Kane, Senior Analyst, Security Leadership Research Institute

Kathleen Kotwica, PhD, EVP and Chief Knowledge Strategist, SEC; Principal Analyst, Security Leadership Research Institute

Herb Mattord, PhD, CISM, CISSP, Director of Undergraduate Education and Outreach, KSU Institute for Cybersecurity Workforce Development

Mike Whitman, PhD, CISM, CISSP, Executive Director of the Institute for Cybersecurity Workforce Development and Professor of Information Security at Kennesaw State University

Editorial Assistance

Marleah Blades, Senior Editor, SEC

Interview Meeting Assistance

Deborah Baldwin, Tier 1 Leader Services & Projects Specialist, SEC

Concept

Bob Hayes, Managing Director, SEC

We thank all of the security practitioners that participated in this research for their time and willingness to share.

About the Security Executive Council

The Security Executive Council is the leading research and advisory firm focused on corporate security risk mitigation strategies and plans. We work with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video for a quick overview or visit us at www.securityexecutivecouncil.com

About the Security Leadership Research Institute

The Security Leadership Research Institute (SLRI) provides independent and actionable research to the security and risk community. The SLRI was formed because of the need by the security industry to document the entire spectrum of corporate security risk mitigation through research. The SLRI conducts many forms of research, including benchmarks, practitioner quick polls, state of the industry and trend reports, and custom research for individual companies and security leaders. Learn more: www.securityexecutivecouncil.com/about/research_institute.html.

About Kennesaw State University
Kennesaw State is a comprehensive university located on two suburban campuses in Kennesaw and Marietta, northwest of metro Atlanta. We are making an impact across the region, the nation and around the world. As the third largest university in Georgia, Kennesaw State has nearly 43,000 students enrolled in over 180 undergraduate, master's, doctoral degree and certificate programs.
https://www.kennesaw.edu/