SOPHOS carahsoft.

SOPHOS

The Impact of Organizational Structure on Cybersecurity Outcomes

Insights from 2,991 IT/cybersecurity leaders working in mid-sized organizations across 14 countries.

Cybersecurity professionals are a core element of an organization's cyber defenses. While much has been written about the shortage of skilled cybersecurity staff, far less focus has been given to how to enable these professionals to make the greatest impact. In short, how best to set them up for success.

This analysis aims to advance this area of understanding by exploring the question: Does organizational structure affect cybersecurity outcomes? The goal is to provide data-based insights to help when considering how to structure your cybersecurity function to achieve the best outcomes, whether you use in-house or external experts, or a combination of the two.

A Sophos Whitepaper. March 2025

The Impact of Organizational Structure on Cybersecurity Outcomes

Thank you for downloading this Sophos resource. Carahsoft is the Public Sector Distributor for Sophos' Cybersecurity solutions available via NASPO, OMNIA, PEPPM PA, and other contract vehicles.

To learn how to take the next step toward acquiring Sophos' solutions, please check out the following resources and information:

For additional resources:
carah.io/SophosResources

For upcoming events:
carah.io/SophosEvents

For additional Sophos solutions:
carah.io/SophosSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Sophos@carahsoft.com
866-436-8778

To purchase, check out the contract vehicles available for procurement:
carah.io/SophosContracts

For more information, contact Carahsoft or our reseller partners:
Sophos@carahsoft.com | 866-436-8778

SOPHOS

The Impact of Organizational Structure on Cybersecurity Outcomes

Insights from 2,991 IT/cybersecurity leaders working in mid-sized organizations across 14 countries.

Cybersecurity professionals are a core element of an organization's cyber defenses. While much has been written about the shortage of skilled cybersecurity staff, far less focus has been given to how to enable these professionals to make the greatest impact. In short, how best to set them up for success.

This analysis aims to advance this area of understanding by exploring the question: Does organizational structure affect cybersecurity outcomes? The goal is to provide data-based insights to help when considering how to structure your cybersecurity function to achieve the best outcomes, whether you use in-house or external experts, or a combination of the two.

A Sophos Whitepaper. March 2024

Research approach

The starting point for this analysis is an independent, vendor-agnostic survey commissioned by Sophos into the experiences of 3,000 IT/cybersecurity professionals working in mid-sized organizations (between 100 and 5,000 employees) across 14 countries. The research was conducted in the first quarter of 2023 and revealed the realities of ransomware, cyber risk, and security operations for security professionals operating at the frontline. The findings formed the basis of the Sophos State of Ransomware 2023 and State of Cybersecurity 2023 reports.

This analysis looked at those cybersecurity experiences through the lens of the organizational structure deployed. The goal was to identify if there is any relationship between structure and outcomes and, if so, which structure reported the best results.

Survey respondents selected one of the following models that best represented the structure of the cybersecurity and IT functions in their organization:

- Model 1: The IT team and the cybersecurity team are separate organizations (n=1,212)
- Model 2: A dedicated cybersecurity team is part of the IT organization (n=1,529)
- Model 3: There is no dedicated cybersecurity team; instead, the IT team manages cybersecurity (n=250)

Nine respondents did not fall into any of these models and so were excluded from the analysis. Organizations that fully outsourced their cybersecurity, for example, to an MSSP, were excluded from the research.

To ensure broad representation, 50% of the survey respondents were from organizations with 100-1,000 employees, and 50% from organizations with 1,001 to 5,000 employees. Overall, there was a strong spread of respondents across each model and organization size band. Perhaps unsurprisingly, the smallest organizations were most likely to not have a dedicated cybersecurity team.

	Organization size											
	100-250 employees		251-500 employees		501-1,000 employees		1,001-3,000 employees		3,001-5,000 employees		Total	
Model 1: IT and cybersecurity are separate teams	90	33%	156	35%	327	43%	430	41%	209	46%	1,212	41%
Model 2: Cybersecurity team is a part of the IT team	149	54%	250	56%	382	50%	539	52%	209	46%	1,529	51%
Model 3: No dedicated cybersecurity team	37	13%	43	10%	60	8%	72	7%	38	8%	250	8%
Total	276	100%	449	100%	769	100%	1041	100%	456	100%	2,991	100%

Executive summary

Organizations with a dedicated cybersecurity team within a wider IT team report the best overall cybersecurity outcomes (model 2) relative to the other two groups. Conversely, organizations where the IT and cybersecurity teams are separate (model 1) reported the poorest overall experiences.

While cybersecurity and wider IT operations are separate specializations, the relative success of model 2 may be because the disciplines are also intrinsically linked: cybersecurity controls often have a direct impact on IT solutions while implementing good cyber hygiene, for example, patching and locking down RDP is often executed by the IT team.

The analysis reveals greater correlation between an organizational structure that facilitates specialization under a shared, connected umbrella and cybersecurity success, relative to other approaches.

The study also made clear that **if you lack essential cybersecurity skills and capacity, how you structure the team makes little difference to many of your security outcomes.** Organizations looking to supplement and extend their in-house capabilities with specialist third-party cybersecurity experts (for example, MDR providers or MSSPs) should look for flexible partners who demonstrate the ability to work as an extension of the wider in-house team.

Important note

While this analysis provides insights into the correlation between IT/cybersecurity structure and reported outcomes, it does not explore the reasons behind these results i.e., causation. Every organization is different, and the structure of the IT/cybersecurity function is one of many variables that can impact propensity to achieve good security outcomes, including industry sector, the skill level of team members, staffing levels, the age of the organization, and more.

Our goal with this analysis is to shine light on an under-reported topic, and provide data-based insights which we hope will help anyone exploring how best to structure their IT/cybersecurity function. While the large audience for this analysis (2,991 respondents across 14 countries) ensures the findings have strong statistical significance, the learnings should be used alongside other considerations to identify the best approach for an individual organization.

Data display

The study analyzed respondents' experiences across multiple aspects of cybersecurity. In the data tables, we have used a Red-Amber-Green traffic light approach to reflect which structure reported the best outcomes (green) and which had the poorest (red). While lacking nuance, this approach has the advantage of enabling readers to quickly see how the different approaches compare. Please look at the individual data points to see the exact response for each group.

Ransomware impact

Every step that helps reduce the impact of ransomware is a positive one, including optimizing the internal structure of the organization. Our analysis of the impact of ransomware is split into three main areas: propensity to experience an attack, recovery operations, and business impact. Respondents in organizations following model 1 report the poorest outcomes in all three areas, with those adopting model 2 reporting the best overall ransomware experiences (and never report the worst).

Propensity to experience an attack

Model 1 organizations (where IT and cybersecurity are separate teams) reported the highest rate of ransomware attacks, with 72% of respondents saying that their organization was hit in the last year. Conversely, model 3 organizations with no dedicated cybersecurity team reported the lowest rate of attack, with just over half (56%) being hit by ransomware. Model 2 organizations are between the two, with 63% reporting an attack in the last year. Interestingly, the root cause of attack varied by organization structure:

- Model 1: Almost half of attacks (47%) started with an exploited vulnerability, while 24% were the result of compromised credentials.
- Model 2: Exploited vulnerabilities (30%) and compromised credentials (32%) were almost equally likely to be the root cause of the attack.
- Model 3: Almost half of attacks (44%) started with compromised credentials, and just 16% with an exploited vulnerability.

Organizational structure had little impact on propensity to have data encrypted, with all groups reporting encryption rates in the 70s (79% for model 1, 73% for model 2, 76% for model 3). However, model 1 was considerably less likely to have experienced data exfiltration (theft) as well as encryption: just 17% of model 1 victims whose data was encrypted said it was also stolen compared to 38% of those following model 2 and half (50%) of those following model 3.

	Model 1 IT and cybersecurity are separate teams	**Model 2** Cybersecurity team is part of the IT team	**Model 3** No dedicated cybersecurity team
Organization was hit by ransomware in the last year	72%	63%	56%
Data was encrypted in the attack	79%	73%	76%
Percentage of encryption events where data was also stolen	17%	38%	50%

Ransomware recovery operations

There are two main methods to restore encrypted data following a ransomware attack: using backups and paying the ransom to get the decryption key. The study revealed a marked difference in backup use and propensity to pay the ransom between model 1 and models 2 and 3, with model 1 organizations far more likely to pay the ransom than the other groups. (In all groups, some organizations used both methods of recovery.)

80% of organizations where the cybersecurity team is part of the wider IT team (model 2) were able to use backups to recover encrypted data, closely followed by 76% of those who do not have a dedicated cybersecurity team (model 3). These organizations also reported the lowest rates of ransom payment (37% and 35% respectively).

Conversely, just 60% of those where IT and cybersecurity are separate teams (model 1) were able to use backups to recover encrypted data. In fact, this group was almost equally likely to pay the ransom (58%) to get data back. This may be due to a lack of available backups, inexperience in recovering from backups, or a combination of the two. Whatever the cause, **low ransomware resilience is one of the most notable differentiators for model 1 organizations.**

In addition to being the group most likely to pay the ransom, model 1 organizations also reported paying much higher ransoms, with their median payment more than double that of models 2 and 3. For organizations following model 1, the median ransom payment came in at $935,600. Conversely, model 2 and 3 organizations reported average ransoms of $320,167 and $350,000 respectively. (Model 3 ransom payment data is based on just 13 respondents so should be considered indicative only).

The faster an organization can recover from a ransomware attack, the better. Over half (54%) of the model 2 organizations fully recovered within a week, compared with 37% of those following model 1 and 35% of those following model 3.

	Model 1 IT and cybersecurity are separate teams	**Model 2** Cybersecurity team is part of the IT team	**Model 3** No dedicated cybersecurity team
Paid the ransom to get encrypted data back	58%	37%	35%
Used backups to get encrypted data back	60%	80%	76%
Median ransom payment	$935,600	$320,167	$350,000 (13 respondents)
Fully recovered within one week	37%	54%	35%

Business impact of ransomware

The ransom is, of course, just one element of the financial cost of recovering from a ransomware attack. Excluding any ransom payment made, organizations following model 1 report a mean average ransomware recovery cost that is more than $1M higher than those in companies following model 2 ($2.41M vs. $1.29M). For completeness, model 3 organizations reported a mean remediation cost of $1.75M. Model 2 organizations also report a median recovery cost ($375,000) that is half that of the other two groups ($750,000).

Within the private sector, model 1 organizations were more than twice as likely to report having lost a lot of business/revenue due to the attack (57%) than those following model 2 (31%).

	Model 1 IT and cybersecurity are separate team	**Model 2** Cybersecurity team is part of the IT team	**Model 3** No dedicated cybersecurity team
Cost to remediate the ransomware attack (excluding any ransom payment)	$2.41M mean $750,000 median	$1.29M mean $375,000 median	$1.75M mean $750,000 median
Lost a lot of business/ revenue due to the ransomware attack	57%	31%	37%

Security operations

Human-led attacks are complex and multi-stage. Detecting, investigating, and neutralizing them in a timely manner requires advanced security operations skills. The biggest takeaway from this area of analysis is that while model 2 organizations fare best in security operations delivery, most organizations find it challenging to deliver effective security operations on their own. Essentially, how you structure the team makes little difference if you lack essential capacity and skills, which indicates that all types of organizations could benefit from outsourced expertise in security operations.

Percentage of organizations that find delivery of core security operations tasks challenging

	Model 1 IT and cyber security are separate teams	**Model 2** Cybersecurity team is part of the IT team	**Model 3** No dedicated cybersecurity
Identifying signals from noise (i.e., what to investigate)	74%	69%	73%
Prioritizing which signals/alerts to investigate	72%	68%	76%
Getting sufficient data to identify if a signal is malicious or benign	74%	68%	76%
Remediating malicious activity in timely way	73%	69%	72%
Identifying the root cause of the incident i.e., how the adversary entered the organization	75%	74%	80%

Day-to-day cybersecurity management

Looking at the day-to-day impact of cybersecurity, there is a lot of common ground across all three groups, and all experience similar challenges. However model 2, again, reported the best relative outcomes.

Across all three models, more than half of respondents report that cyberthreats are now too advanced for their organization to deal with on their own (60% model 1, 51% model 2, 54% model 3). This finding highlights both the widespread need to supplement in-house resources with external security support and the importance of selecting third-party experts who meet you where you are and are able to adapt to your particular IT/cybersecurity functional set-up.

All models also share similar worries around cyberthreats and risks. Data exfiltration and phishing (including spear phishing) feature in the top three cyber concerns for all three groups, and security tool misconfiguration is the most common perceived risk across the board. Essentially, everyone has the same top concerns, independent of organizational structure.

Cybersecurity takes a lot of time and effort, with most respondents reporting that dealing with threats gets in the way of key initiatives. Respondents also indicated that they would like to spend less time firefighting threats and instead focus more on strategic issues. While all groups report challenges in these areas, model 2 organizations appear to be better placed to deal with the day-to-day impact than those following models 1 or 3.

	Model 1 IT and cybersecurity are separate teams	**Model 2** Cybersecurity team is part of the IT team	**Model 3** No dedicated cyber-security team
Say that cyberthreats are too advanced for the organization to deal with on their own	60%	51%	54%
Top cyber threat concerns for 2023	Data exfiltration (theft by external attacker) 39% Phishing (including spear phishing) 36% Cyber extortion 34%	Data exfiltration (theft by external attacker) 44% Phishing (including spear phishing) 43% Ransomware 41%	Phishing (including spear phishing) 44% Ransomware 37% Data exfiltration (theft by external attacker) 36%
Would like to do less firefighting of cyberthreats and focus more on strategic issues	69%	64%	63%
Say that dealing with cyber incidents has negatively impacts IT team's work on other projects	61%	55%	63%
Top perceived security risks	Security tool misconfiguration 26% Zero-day threats 25%	Security tool misconfiguration 29% Zero-day threats 28%	Security tool misconfiguration 26% Internal users (accidental) 24%

Final analysis

The analysis makes clear that organizations where the cybersecurity team is embedded within the wider IT team report the best cybersecurity outcomes relative to the other structures considered.

It may be that model 2's connected approach facilitates collaboration and shared outcomes, and makes it easier to leverage respective expertise to achieve improved protection, reduced risk, and more effective and efficient delivery of services. It may also be that organizations that adopt this approach are more willing and/or able to engage specialist third-party expertise to support their cybersecurity needs, which helps them achieve superior outcomes. At the same time, working together within a larger group may help prevent the operational silos that can reduce the impact of cybersecurity efforts.

As stated, this report focuses on correlation rather than causation, and further research is needed to understand the reasons behind these outcomes. In the face of today's cybersecurity challenges, any gain for defenders is important and we hope this analysis will spur further study into how organizations can leverage their internal structure to help optimize their defenses.

Sophos security operations services

Sophos MDR provides best-in-class 24/7 security operations services that support organizations of all sizes, including many thousands of small and medium-sized businesses. Customers choose the level of support and involvement they need to best support their business and internal team structure.

Popular models include:

- The Sophos MDR team works in partnership with the in-house team.
- The in-house team takes the lead during working hours, passing to Sophos MDR for evenings, weekends and holidays.
- The Sophos MDR team fully manages security operations on behalf of the customer.

Sophos MDR is consistently top-rated by customers, with the highest rating and most reviews of any MDR provider on Gartner Peer Insights and G2. To learn more and discuss how Sophos MDR can support your organization, visit www.sophos.com/mdr and speak with an adviser today.

Appendix A: Consolidated table of results

	Model 1 **IT and cybersecurity are separate teams**	**Model 2** **Cybersecurity team is part of the IT team**	**Model 3** **No dedicated cybersecurity team**
RANSOMWARE IMPACT			
Organization was hit by ransomware in the last year	72%	63%	56%
Data was encrypted in the attack	79%	73%	76%
Percentage of encryption events where data was also stolen	17%	38%	50%
Paid the ransom to get encrypted data back	58%	37%	35%
Used backups to get encrypted data back	60%	80%	76%
Median ransom payment	$935,600	$320,167	$350,000 (13 respondents)
Fully recovered within one week	37%	54%	35%
Average cost to remediate the ransomware attack (excluding any ransom payment)	$2.41M mean	$1.29M mean	$1.75M mean
Lost a lot of business/revenue due to the ransomware attack	57%	31%	37%
SECURITY OPERATIONS (Percentage of respondents that find delivery of core security operations tasks challenging)			
Identifying signals from noise (i.e., what to investigate)	74%	69%	73%
Prioritizing which signals/alerts to investigate	72%	68%	76%
Getting sufficient data to identify if a signal is malicious or benign	74%	68%	76%
Remediating malicious activity in timely way	73%	69%	72%
Identifying the root cause of the incident i.e., how the adversary entered the organization	75%	74%	80%
DAY-TO-DAY CYBERSECURITY MANAGEMENT			
Say that cyberthreats are too advanced for the organization to deal with on their own	Data exfiltration 39% Phishing (including spear phishing) 36% Cyber extortion 34%	Data exfiltration 44% Phishing (including spear phishing) 43% Ransomware 41%	Phishing (including spear phishing) 44% Ransomware 37% Data exfiltration 36%
Top cyber threat concerns for 2023	69%	64%	63%
Would like to do less firefighting of cyberthreats and focus more on strategic issues	61%	55%	63%
Say that dealing with cyber incidents has negatively impacts IT team's work on other projects	Security tool misconfiguration 26% Zero-day threats 25%	Security tool misconfiguration 29% Zero-day threats 28%	Security tool misconfiguration 26% Internal users (accidental) 24%

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, MAGIC QUADRANT and PEER INSIGHTS are registered trademarks of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved.

Gartner Peer Insights content consists of the opinions of individual end users based on their own experiences with the vendors listed on the platform, should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

SOPHOS