



**Breaking Down
Exposure Management Silos:**

Confronting the Network-Security Disconnect

A Letter from Mordecai Rosen, Skybox Security CEO

Cybersecurity today has become a game of connecting the dots. You know you have a vast number of vulnerabilities and where many of those lie throughout your network, but do you know which are likely to cause the most damage to your organization? Do your security and network teams agree on where to prioritize their efforts? And if so, do you have the right tools and processes to address these exposures quickly enough regardless of the team responsible?

This is the challenge most organizations today face. The high rate at which new exposures and vulnerabilities are identified and malicious actors exploit them makes it incredibly difficult for network and security teams to keep up. This is complicated even further when the teams rely on incompatible systems separated by their own operational silos. Without an agreed-upon and shared view of your environment, related exposures, and their priority to the business, there is a disconnect within the organization—and a gaping hole that malicious actors can exploit.

In conversations with hundreds of security and networking leaders like yourself, one thing is clear: Lockstep collaboration and communication are a high priority, but siloed systems and processes leave leaders with doubts. We are hearing that this top priority is why many organizations are turning to Continuous Exposure Management, a proactive and comprehensive approach to cybersecurity that continuously identifies, evaluates, and mitigates potential cyber threats and vulnerabilities.

Faced with millions of potential threats, continued operation in silos is overwhelming and highly risky. Only by working together using a common approach and tools can network and security teams focus on the most critical risks, allowing for more effective resource allocation and overall improved security.

Within the next 12 months, even the most sophisticated security measures could be overwhelmed by AI-powered attacks. That is why the convergence of approaches for security and network operations is no longer a strategic advantage; it's an existential imperative.

At Skybox Security, we're committed to facilitating this crucial collaboration. We surveyed 500 cybersecurity and IT leaders across various industries to uncover the barriers organizations face in integrating security and networking teams' approach and its impact on their overall security.

We hope these findings spark a conversation that ushers in a new era of cybersecurity—one where security and networking teams work in unison.

Sincerely,
Mordecai Rosen



Executive Summary

The modern enterprise runs on a vast network of technologies, often operating invisibly in the background. Network teams face the daunting task of ensuring this intricate web functions seamlessly and is kept up to date. Working nearby, the security teams have an equally challenging role: maintaining robust security across all systems to keep their critical data and assets secure. These challenges have grown exponentially with the rise of public and private clouds, the proliferation of OT and IoT devices, the continued support of remote work, and the lingering presence of legacy on-prem assets.

On top of this, security and network teams often report to different management chains with different budgets, goals, and priorities. As cyberattacks escalate in frequency, sophistication, and cost, this siloed nature between the groups creates critical blind spots for attackers to exploit.

To explore this pressing issue, Skybox Security partnered with Sapio Research to survey 500 security professionals and executives across North America and the UK. We wanted to learn more about the obstacles organizations face in harmonizing security and networking teams and the impact this has on their overall cybersecurity posture.

The survey results show organizations actively striving for better collaboration between their network and security teams to bolster their defenses against cyber threats. However, a deeper look into the confidence of these processes reveals a discrepancy between perceived effectiveness and actual outcomes.

As a result, many organizations are looking to implement an integrated approach and tools for vulnerability/network security management, such as Continuous Threat and Exposure Management (CTEM), to improve collaboration between network and security teams

This report highlights key findings from the survey and provides insights into the challenges and opportunities for organizations seeking to bridge the gap between security and networking.

Collaboration on the Rise

When computers first became a fixture in organizations, they were typically managed by internal IT teams. They managed everything from hardware and software to users and support. As technology progressed, networking ramped up productivity and became a natural extension of the IT team's responsibility. With the IT team focused on managing an increasingly complicated infrastructure, the rapid adoption of the internet, and associated exposures to breaches and ransomware, a separate team focused on cyber security was spawned. Network teams managed the infrastructure, and security focused on protecting critical data and assets from outside cyber threats.

As these functions expanded, teams were formed with different responsibilities and priorities, different budgets, and frequently, different management chains. These silos have created an environment where teams often work in parallel instead of cohesively working together towards a common goal. Unfortunately, this creates gaps that provide opportunities for cybercriminals to enter networks and cause significant damage.

Clearly, as executive leadership and IT decision-makers facilitate collaboration and communication between teams, they will better secure their organization. Today, they are making great strides towards improved communication and collaborative systems, bridging/closing the gaps that leave them vulnerable to cybercriminals.

In fact, of the 500 respondents surveyed, most organizations (90%) stated they have formal processes in place for network and security teams to collaborate on vulnerability and exposure management. With 81% of decision-makers perceiving their current collaboration levels as effective and a similar percentage (82%) reporting successful information-sharing practices, organizations seem to be well in control and protected from most potential attacks.

However, this seemingly good news is covering a great deal of concern and anxiety just under the surface.

Let's take a closer look at the trends we see in today's global organizations.

A False Sense of Security

The survey found that **more than half of these respondents (55%) were concerned about a security risk due to a lack of communication between network and security teams**. This apprehension is significantly heightened among C-level executives (67%), suggesting they feel a greater sense of responsibility and understand that as the ultimate stewards of the organization's success and security, they bear the heaviest burden of potential fallout from a security breach caused by poor collaboration.

Concern over risk of security incidents due to a lack of collaboration:



The concerns of these organizations are not unfounded. In the last 12 months, almost half (45%) said they experienced miscommunications that resulted in delays in reporting or addressing security incidents, validating the fears of those highly concerned about the risks associated with collaboration breakdowns. Furthermore, three quarters (75%) believe that their organization's security posture has been negatively impacted by miscommunication between network and security teams to some extent.

75% believe security posture was negatively impacted by miscommunication between network and security teams

This begs the question: is the confidence in collaboration and communication misplaced?


The Potential for Human Error Remains High

Miscommunication and human error persist, even with established processes. While teams are willing to collaborate, incompatible technologies that lead to fragmented information hinder their efforts. This lack of a unified source of truth can lead to critical oversights, leaving gaping holes in the security fabric.

The findings expose a fundamental challenge: **there is ineffective communication and collaboration between these two critical teams.** When network teams operate without a clear understanding of the security implications of the changes they are making, unnecessary risks or vulnerabilities can be introduced. Similarly, if the security team fails to share the highest priority vulnerabilities with the network team before patching, they could significantly delay mitigating the risks. The resulting communication gaps can be costly for organizations.

The survey results further underscored this challenge, which revealed that incompatible systems and siloed organizational structures are the most significant obstacles to effective collaboration between network and security teams (cited by 50% of respondents).

Sometimes, organizations try to solve this problem by buying additional point solutions to address specific pain points. However, piling these solutions together usually results in competing data, conflicting recommendations, and more confusion. For larger organizations, it's common to have multiple security tools in place – sometimes even multiple for the same area, like vulnerability management. Since each tool has its own way of filtering and prioritizing data, it's hard for teams to determine their true risks and find the most effective mitigation and remediation actions. Often, teams outside of security don't even have visibility into these tools.



The challenge of siloed structures is particularly pronounced in larger organizations (65% for 10,000+ employees versus 41% for 1,000-4,999 employees). As teams grow and management begins to focus on narrower areas, there is a tendency for network and security teams to operate independently, which becomes more entrenched, hindering effective communication and collaboration. In contrast, smaller organizations appear to navigate these silos more effectively, perhaps due to closer proximity and flatter hierarchies. But unfortunately, this doesn't leave them exempt from these risks.

This research clearly shows that **organizations need to foster a culture of open communication** and a shared approach that facilitates seamless interaction between network and security teams to better secure their critical data and assets.

Siloed structures are the top barrier to team collaboration

Change is Coming

The survey results reveal a strong desire for change. A significant majority, 3 in 5 respondents (61%), said they would be somewhat or very likely to implement an integrated solution for vulnerability and network security management to improve collaboration between the two teams.

This desire is particularly pronounced among those who harbor deep concerns about security incidents stemming from collaboration breakdowns, with a staggering 92% expressing a likelihood to implement such integrated solutions.

This overwhelming response underscores a crucial realization: **while effective communication is vital, it's not enough**. Even with open dialogue and well-intentioned processes, the inherent limitations of siloed systems and disparate tools will create vulnerabilities. The human element, prone to error even in the best of circumstances, further amplifies these risks.

61% likely to implement an integrated vulnerability and network security management solution

This desire is particularly pronounced among those who harbor deep concerns about security incidents stemming from collaboration breakdowns, with a staggering 92% expressing a likelihood to implement such integrated solutions.

This overwhelming response underscores a crucial realization: while effective communication is vital, it's not enough

Even with open dialogue and well-intentioned processes, the inherent limitations of siloed systems and disparate tools will create vulnerabilities. The human element, prone to error even in the best of circumstances, further amplifies these risks.

Organizations recognize that true collaboration requires more than conversation – it demands a unified approach to network and security management. This can be done through exposure management tools that fully visualize the network and continuously assess, prioritize, and remediate the most critical cyber threats. Integrated solutions will bridge the gap between teams, streamline processes, and minimize the potential for human error via defined processes and automation. By breaking down silos and providing a shared source of truth, these solutions can help organizations move beyond mere communication and build a stronger, more resilient security posture.

Looking Ahead

While eliminating silos entirely may not be feasible, fostering better synchronization between teams is essential for proactive security.

Organizations must adopt a unified solution that serves as a centralized repository for security data, accessible to all relevant teams. This approach streamlines workflows, provides a single source of truth, and enables budget consolidation. A continuous exposure management (CEM) solution provides multi-source aggregation, enabling disparate network and security teams to work in the same tool and communicate more effectively.

By building a map of your hybrid attack surface, you can more accurately visualize your networks and understand your risks. Using a CEM solution allows you to prioritize vulnerabilities using the aggregate data from your point solutions while also considering severity, importance, exploitability, and network exposure. To further bolster your security, these solutions offer alternative mitigation and remediation options – to keep your networks protected before you can patch.



Ideally, this solution should also help teams assess the security risk associated with each network security policy change. Visualizing end-to-end access routes allows you to safely test and plan network changes without impacting traffic.

An integrated solution empowers network teams to make informed decisions that consider security implications, while security teams gain the ability to proactively manage risk when patching delays are unavoidable.

Cybersecurity is a shared responsibility across the entire organization. However, the network and security teams are crucial in establishing a strong foundation for the entire company. By collaborating effectively as a united front against cyber threats, these teams will improve efficiency with their own tasks while simultaneously enhancing the organization's overall security posture.

Methodology

This survey targeted IT/security decision-makers responsible for network, vulnerability, and infrastructure management within their organizations. A total of 500 participants from the UK and USA were surveyed. Respondents needed to be employed by organizations with at least 1,000 employees to qualify.

Data collection took place in July 2024 using an online survey platform. Sapio Research facilitated the survey process, inviting participants via email and providing an online link to complete the questionnaire.

Want to learn more? Get a demo or talk to an expert:

skyboxsecurity.com/request-demo 

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics, and automation to quickly map, prioritize, and remediate vulnerabilities across your organization.