IDG

SPONSORED BY

BLUECAT

A HOUSE DIVIDED

The Cost of Dysfunction Between Network & Cybersecurity Teams

Trust issues and lack of network visibility hamper cyber defenses.

"A new study by IDG shows 86% of organizations have suffered repercussions, including increased security breaches and data loss, due to lack of collaboration between Network & Cybersecurity teams."

Organizational tug-of-war adds risk and costs

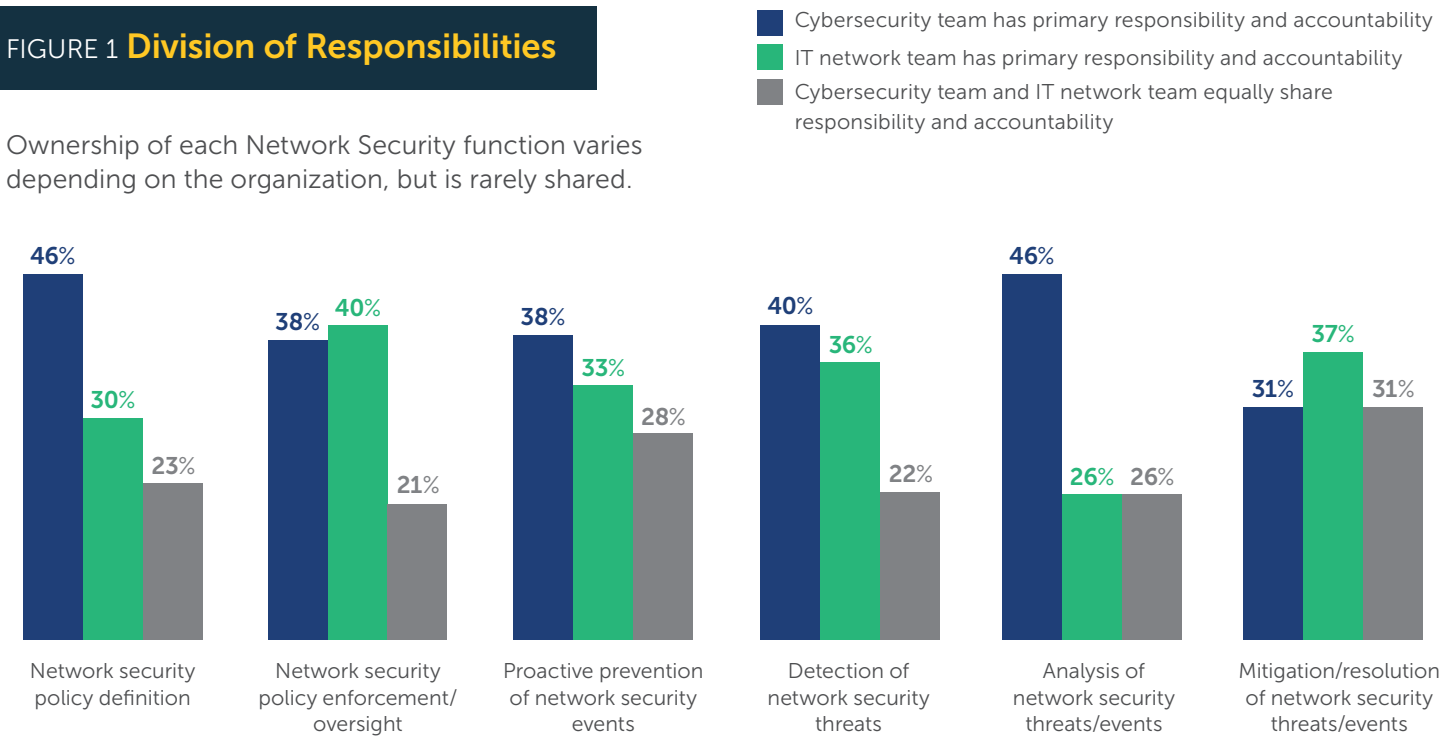
Business investments in network operations and cybersecurity may be shortchanged if the teams responsible for those areas aren't collaborating. A new study by IDG shows 86% of organizations have suffered repercussions, including increased security breaches and data loss, due to lack of collaboration between these teams.

Among the repercussions survey respondents attribute to lack of collaboration are: slow response to security events (34%), finger-pointing (33%), increase in security breaches/data loss (32%), loss of productivity (28%), service downtime (27%), inability to determine the root cause of security events (26%), and increased costs (26%). *See figure 2.* Adding insult to injury, nearly two-thirds of respondents reported experiencing two or more of those repercussions.

"Network and Cybersecurity teams are often battling the wrong adversary: each other," says Mathew Chase, a seasoned Information Technology executive who was consulted about the findings of this research. "Their strained relationship results in additional challenges and angst when they should be defending the organization as a cohesive team."

FIGURE 1 **Division of Responsibilities**

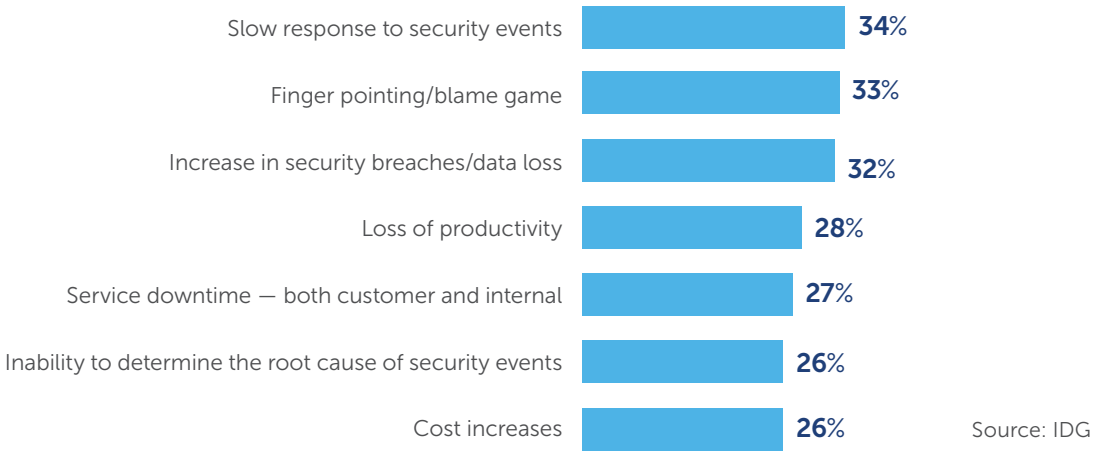
Ownership of each Network Security function varies depending on the organization, but is rarely shared.



NOTE: Due to rounding, numbers do not always equal 100.

SOURCE: IDG

FIGURE 2 **Repercussions from a Lack of Close Collaboration Between Cybersecurity and Network Teams**



Source: IDG

Just ***38%*** *of surveyed organizations feel "very well-equipped" to protect the network from future cybersecurity attacks.*

With network security incidents continuing to rise, it's increasingly important that the two teams collaborate to keep the network operating and secure. Yet, just 38% of surveyed organizations feel "very well-equipped" to protect the network from future cybersecurity attacks. When there are issues, finding the root cause is essential to resolve an incident quickly and completely. These teams can't afford to be working at cross-purposes, or duplicating efforts.

Dysfunction stems from a lack of trust & understanding

The clash is caused by a tug-of-war over responsibility for several aspects of network security, which creates gaps that endanger organizations. While network policy definition and threat analysis most often fall within the purview of cybersecurity teams, ownership over other aspects like threat detection is a more contentious issue and very infrequently shared. *See figure 1.*

Half of those surveyed by IDG indicated that conflicting objectives are the greatest obstacle to making that trust between teams happen. Only a small percentage of survey respondents say the two teams share primary responsibility in the areas of policy enforcement, event prevention, threat detection, and event mitigation. The lack of clarity on ownership likely contributes to why 55% of survey respondents don't believe there is a high level of trust between cybersecurity and network teams. It also may be a reason why the research found 43% of network and 58% of cybersecurity professionals think their counterparts lack a fundamental understanding of their role.

Visibility lights the path to recovery

The good news is that the majority of network (82%) and cybersecurity (92%) professionals realize they should be collaborating more, and those that already do so are reaping benefits. About two-thirds believe that cybersecurity and network operations functions are likely to further converge organizationally over the next 12 to 24 months.

Organizations that structure the two functions under one management team report a variety of benefits, including better network visibility for the cybersecurity team and a higher level of mutual trust. The number one benefit is faster response to security events.

55% *of survey respondents don't believe there is a high level of trust between cybersecurity and network teams.*

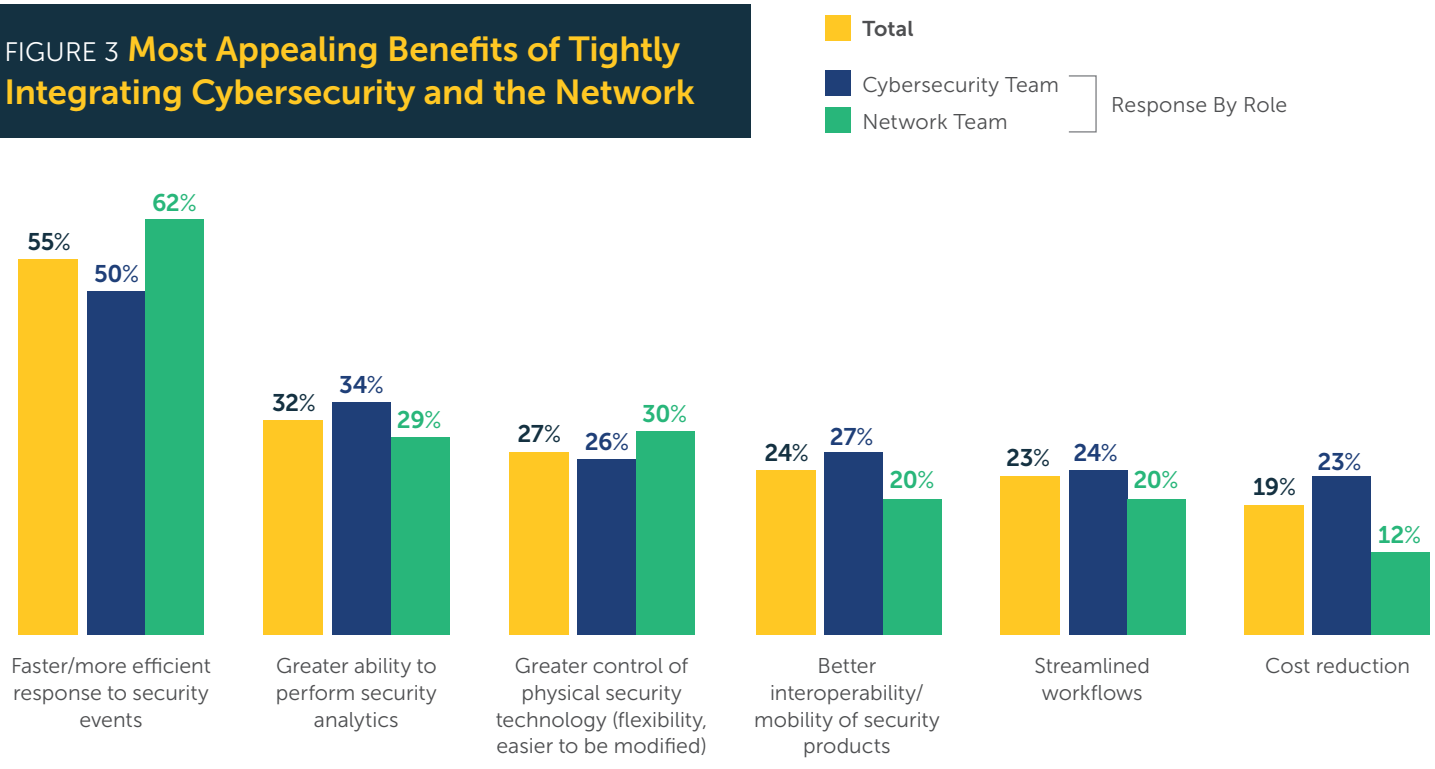
That shared visibility into the network goes hand-in-hand with high levels of collaboration. The percent reporting a high level of trust between teams more than doubles at those organizations providing complete visibility to cybersecurity staff. Similarly, when the cybersecurity team has complete visibility, organizations have a higher level of confidence that they are very well-equipped to protect the network from future cybersecurity attacks. But only 37% of cybersecurity respondents say they currently have that level of visibility.

It's apparent that visibility goes a long way to resolving trust issues and promoting collaboration. It allows both teams to have greater confidence in what is happening on the network, and subsequently how their actions stand to complement, overlap, or create gaps with their counterparts' activity. And, according to 55% of survey respondents, the most appealing benefit of tightly integrating the cybersecurity and network teams is a faster, more efficient response to security events. *See figure 3.*

Finding common ground in DNS data

In many organizations, the cybersecurity team is focused on protecting applications, data centers, endpoints and firewalls. The network operation is often a missing link. Until they have shared visibility into the network, there is going to be potential for security gaps, duplicated effort, outages, and a damaging lack of trust.

FIGURE 3 **Most Appealing Benefits of Tightly Integrating Cybersecurity and the Network**



SOURCE: IDG

"There is a lot of eye-opening on both sides of the fence," says Michael Harris, CEO of BlueCat. "Organizations need both visibility into critical network infrastructure and a controlled, real-time view for cybersecurity."

Respondents identified the following advantages to modernizing DNS: better network management and controls, ability to mine DNS data for threats, increased agility, and increased automation.

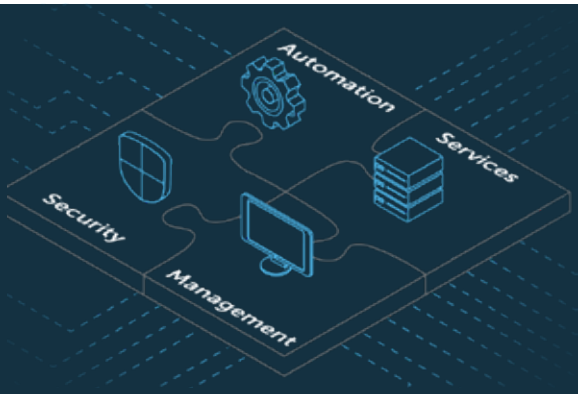
One often-overlooked area that can be shared by teams to enable network control and visibility is DNS. When set up in a unified way, DNS represents a rich data source that provides much-needed shared visibility; it is also pervasive across the network, which allows it to exact control over activity.

Survey respondents see many advantages to modernizing DNS to reach such a state, including better network management and controls (37%), ability to mine DNS data for threats (35%), increased agility (29%), and increased automation (22%), among others. Capturing and analyzing DNS queries and responses tied to other contextual data makes it possible to audit user activity, find anomalies, and establish role-based access controls.

But many enterprises rely on homegrown DNS management solutions that are difficult to build and maintain, let alone share access to. Every solution in the infrastructure requires a separate set of servers, configurations, backups, patches, and upgrades. Systems like this are vulnerable to human error, difficult to automate, and require serious effort to maintain. Moreover, wrangling each disparate part of these systems together for comprehensive visibility and shared administrative access is exhausting. The results are weak security, inflexible architecture, downtime, skewed management approaches, and impaired and under-utilized visibility.

The survey reveals that those leveraging DNS data in their security strategies are more confident that their network is protected from DNS exploitations, which according to industry research are used in 91% of attacks. For instance, of those who reported feeling extremely confident their company's infrastructure is protected from DNS-leveraged security threats, 94% were leveraging DNS data.

"DNS has always been in the hacker's toolbox for mapping and disrupting organizations," notes Chase. "Organizations need to make the shift towards using DNS as skillfully as their adversaries in order to protect against and respond to threats across the enterprise."



About BlueCat

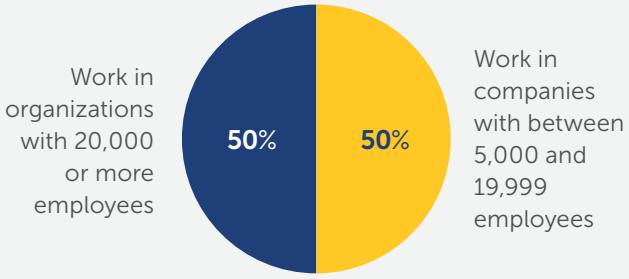
BlueCat is the Enterprise DNS Company™. The largest global enterprises trust BlueCat to provide the foundation for digital transformation strategies such as cloud migration, virtualization and cybersecurity. Our Enterprise DNS platform makes shared network visibility possible for cybersecurity and network teams, and improves control and compliance across entire networks. This allows organizations to centralize and automate DNS services for security and operational efficiency. For more information, please visit www.bluecatnetworks.com.

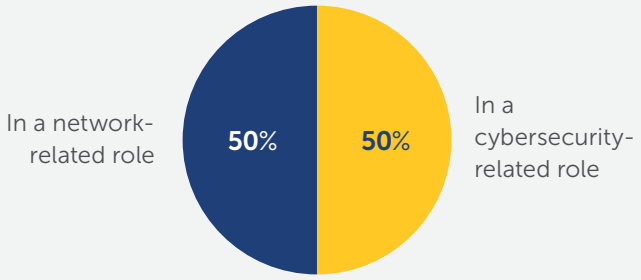
Appendix A: Methodology & Respondent Profile

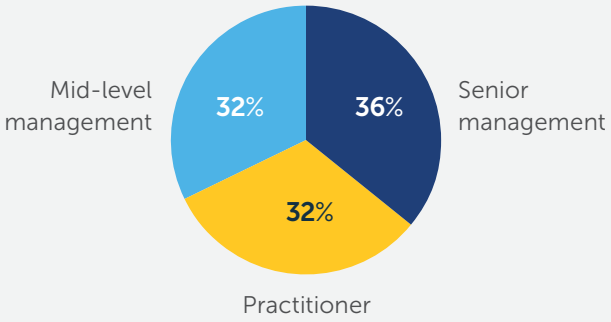
This report is based on a research survey conducted by IDG communications Inc. on behalf of BlueCat between May 16, 2018 and June 1, 2018. The objective of the survey was to understand the accelerating convergence and collaboration of traditional network and cybersecurity teams, and its effect in causing disruption and/or opportunities.

A total of 200 qualified North American respondents participated in the survey, which was conducted via email invitation. Respondents were required to be employed in a network (data wired, wireless, voice, etc.) or a cybersecurity (IT/network security/cybersecurity) role at a company with 5,000 or more employees. Senior management, mid-management, and analyst level roles are equally represented. All qualified respondents are involved in the purchase and integration of cybersecurity technology.

A broad range of industries are represented including:







The margin of error for a sample size of 200 is +/– 6.9 percentage points. For questions requiring respondents to select a single answer, percentages may not sum to 100% due to rounding.

For more information about this research, please contact Jen Garofalo, Research Director at IDG (jen_garofalo@idg.com).