NETSCOUT®

| WHITE PAPER |

Why Can't We Be Friends?

Enterprises Need Renewed Focus on Aligning IT and Cybersecurity

SECURITY

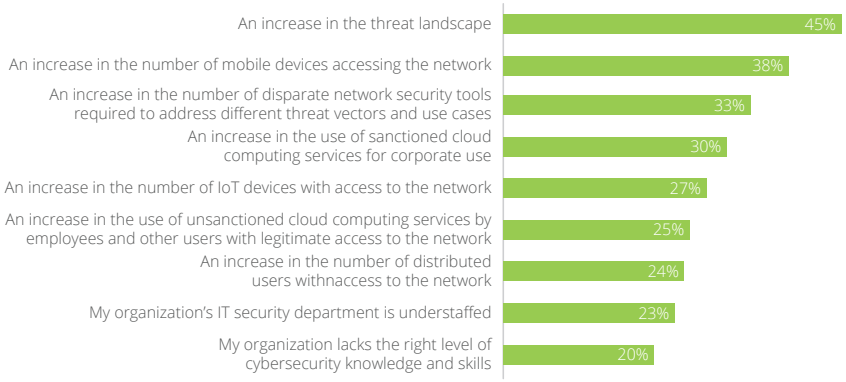
TABLE OF CONTENTS

Increasing Threat Landscape Drives Need for NetSecOps Collaboration

Cybercriminals increasingly are finding new ways to infiltrate enterprise networks by weaponizing new attack vectors, leveraging mobile hotspots, and targeting compromised Internet of Things (IoT) devices. And there's no question that attackers are succeeding in their efforts, considering that more than 5.4 million distributed denial-of-service (DDoS) attacks were launched in 1H 2021—representing an 11 percent increase in attacks over the same period just a year ago.

Meanwhile, ensuring network security is increasingly difficult, thanks to the ever-expanding threat landscape, as well as confusion over the network security tools on the market, what they do and don't do, and what's needed to ensure enterprise network security. This is evidenced by a recent survey of 226 network security and IT professionals, who were asked why network security has become more difficult over the past two years According to the Enterprise Strategy Group (ESG) survey, 45 percent attributed it to an increase in the threat landscape, and 33 percent blamed an increase in the number of disparate network security tools needed to address different threat vectors.

You indicated that network security has become more difficult over the last two years. In your opinion, which of the following factors have been the most responsible for making network security management and operartions more difficult?
(Percent of respondants, N=226, three responses accepted)



Yet even as enterprises grapple with the increases in cyberattacks against their networks, they're increasingly doing so with IT and cybersecurity teams that are at odds with one another. The primary mission of IT teams is to deliver efficient, engaging employee experience and to ensure an agile, frictionless customer experience. Meanwhile, security teams are focused on protecting assets, while ensuring that employees, customers, and others on the network don't make mistakes or forget things that create security issues.

As such, it's imperative for these two vital teams to work well together. Yet according to ESG, 44 percent of cybersecurity and IT professionals say the relationship doesn't work well at times, citing several factors that contribute to the friction, including:

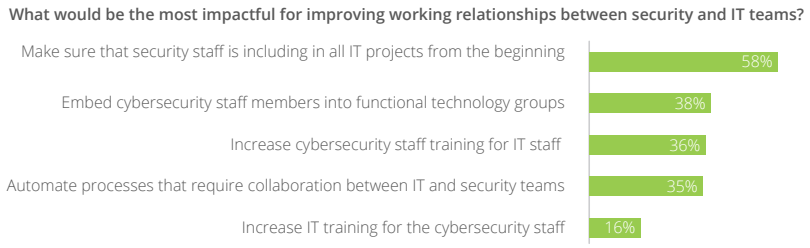
- **Issues with reporting structures:** Many chief information security officers (CISOs) now report directly to chief executive officers (CEOs) and boards of directors rather than to the chief information officer (CIO), creating conflicting agendas between CIOs and CISOs. This also can lead to CISOs having a lack of insight into the CIO's technology strategy, potentially delaying organizational enterprise goals and creating unexpected vulnerabilities.
- **Budgetary conflicts:** CIOs and CISOs often compete for the same budget resources, pitting their respective interests against each other for finite funds.
- **Compliance issues:** A lack of good communication and poor working relationships between the CIO and the CISO can lead to noncompliance and create network vulnerabilities. In many cases, this comes down to a struggle over who has ownership over the policies and procedures in place to ensure compliance requirements are met.
- **Lack of skilled workers on both teams:** The technology worker skills gap isn't new, with 95 percent of cybersecurity and IT professionals saying it hasn't improved over the past few years, and 44 percent saying it's gotten worse—resulting in increased workloads (62 percent), unfilled open job requisitions (38 percent), and high burnout among staff (38 percent).

In fact, cybersecurity professionals say the most stressful aspects of their jobs often stem from these very issues. Almost a third say their greatest stress stems from IT initiatives or projects that were started by other teams with no security oversight, and 31 percent point to working with disinterested business managers.

What are the most stressful aspects of your job as a cybersecurity professional?
(Percent of respondants, N=489, three respnses accepted)

Fostering Collaboration Between Network and Security Teams

Apple co-founder Steve Jobs once famously said, "Great things in business are never done by one person. They're done by a team of people." That kind of thinking is what is needed—and is often lacking—in terms of IT and security teams working as one unit.



In many cases, this begins with frustration over roles—who does what, when, and how. For instance, cybersecurity professionals generally want to participate in IT planning, but they're frustrated when relegated to technology administration roles. Likewise, security teams want to participate with business management in strategic planning, but they are often shut out of meetings and not considered in the development of strategic plans.

For the fifth consecutive year, the Information Systems Security Association (ISSA) conducted a survey in 2021 to determine how such frustrations might best be addressed. Respondents provided a number of suggestions that could improve the relationship between security and IT, including:

- Ensuring security personnel are included on IT projects from the start (58 percent)
- Embedding security personnel into functional technology groups (38 percent)
- Automating processes that promote collaboration between IT and security (35 percent)

In fact, cross-silo collaboration is considered imperative for effectively identifying and troubleshooting service performance issues, as evidenced by a 2021 survey from EMA in which 35 percent of network operations teams said security system problems such as bad policies and device failures had led to such issues. With growing enterprise adoption of public and private cloud architecture, cross-silo collaboration becomes even more important.

NetSecOps collaboration also is key to improving network performance, reducing security risk, and accelerating security incident detection and response. Security teams should detect, validate, investigate, and respond to threats on an ongoing basis, while also recognizing that security also is a strategic priority for network teams. In fact, a reduction in security risk is among the key measurements of success for network teams—even before service quality, network visibility, and end-user experience.

Moreover, today's complex digital infrastructure demands collaboration between network and security teams to gain better clarity on whether an IT service event is a performance issue or a security incident. Cross-team collaboration drives cost and operational efficiencies, reduces overall risks, and quickens the pace for resolving security incidents. The more converged network and security teams are—and the more integrated the tools and processes used between them—the more successful they are at achieving these objectives.

Important Steps for Ensuring Collaboration

- **Start with a clear picture**. IT leaders need to create a transformational security view across operations and infrastructure, including a data store built for use by both security and network teams; a toolset that enables collaborative workflow; and documented policies, controls, and best practices that formalize cross-team collaboration. Doing so provides a strong foundation for configuring and implementing a robust cybersecurity strategy.
- **Begin at both the design and deployment stage**. According to a McKinsey & Company survey the COVID-19 pandemic has forced enterprises to accelerate digital transformation timelines by three to four years, increasing their dependence on and use of the cloud, software-defined solutions, virtualization, and the IoT. But even as those technologies have increased mobility, the security perimeter has become increasingly vulnerable. NetSecOps collaboration at the infrastructure design and deployment stages firmly places security as a first priority.
- **Start with a single source of truth**. A single source of truth ensures that network and security teams share consistent, up-to-date information, eliminating blind spots and data control conflicts. NetSecOps should look for opportunities to unify data collection and the tools used for analysis wherever possible.
- **Choose the right tools**. ISSA also found that network performance monitoring and network automation/orchestration are considered the two most essential tools for collaboration. Network performance and security incidents often are interrelated, and performance management tools are vital in identifying potential security incidents. Likewise, network automation tools empower enterprises to make quick network changes in response to security events.
- **Formalize the collaboration**. Documenting the processes established for collaboration serves to formalize collaboration between network and security teams. Documentation should incorporate change controls where necessary and leverage industry best practices where relevant, thus establishing a roadmap for effective collaboration between network and security teams.

Building a Common Network Security Technology Stack

Another important step for ensuring that security and network operations teams work collaboratively is adopting a common network security technology stack that includes the following:

- **Stateless protection devices in front of stateful firewalls:** Implementing stateless protection devices in front of stateful firewalls helps to block threats such as command-and-control (C2) traffic, state-exhaustion distributed denial-of-service (DDoS) attacks, and known bad DNS domains. To be effective, these devices need timely and accurate threat intelligence that continually updates blocking lists in real time, enabling them to protect stateful network infrastructure, filter out known cyberattack traffic, and enable IT operations teams to maintain peak network performance for business requirements.
- **Examine all east/west traffic:** Security experts have come to rely on next-generation firewalls for security at network perimeters. Although such firewalls cover network ingress/egress, they leave internal networks open to attacks. To close this gap, network security needs to look at all east/west traffic in their legacy networks and hybrid cloud environments, enabling security teams to quickly and easily identify and filter out known threats moving laterally inside their environments.
- **A common source for network and cloud visibility:** It's not unusual for network and security teams to find that they're using a multitude of disparate tools to collect the same network data. But what's necessary to achieve holistic network and cloud visibility is a common source of network truth that's derived from network metadata. The right tool should have real-time packet analytics that create a robust set of locally stored, highly indexed metadata that can be quickly accessed and analyzed for more efficient incident detection, investigation, and mitigation—all of which are crucial for maintaining strong performance and detecting and responding to security incidents.
- **Network traffic analysis capabilities:** To ensure network performance and security, teams need to understand network traffic patterns, as well as the disposition of every device connected to the network before an incident occurs. Doing so helps them identify and remediate rogue devices, misconfigurations, and vulnerable systems, while maintaining application performance for business operations. Network traffic analysis capabilities deliver end-to-end visibility that allows teams to monitor normal network behavior to identify anomalies that might impact network security or performance.
- **Network detection and response systems:** Modern-day cyberattackers increasingly deploy anti-detection and forensics techniques to avoid being detected by endpoint detection and response (EDR) solutions. In addition to traffic analysis, teams need a way to analyze network data and threat intelligence in order to detect and investigate anomalous, suspicious, and malicious network activities that are hidden from other cybersecurity tools. Network detection and response systems can detect threats that EDR and log-based system miss—while also providing access to a comprehensive source of metadata and network packets. Such data is crucial for triage and investigations.

LEARN MORE

To learn more about fostering collaboration between IT and security teams, as well as developing a strong security technology stack, get in touch today.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECWP_024_EN-2101 10/2021