NETWORKWORLD

2016 State of the Network
SURVEY

Exclusive Research from Network World

NETWORKWORLD

EXECUTIVE SUMMARY
2016 State of the Network Study, Network World

Network IT Grows More Challenging—and More Critical to the Business

The network organization is taking on an increasingly important and strategic role within IT and the business, according to Network World's 2016 State of the Network Survey.

The vast majority of IT and business professionals surveyed agreed that the role of the networking professional today is becoming more challenging than ever (85%). In fact, among large enterprises, nearly *all* respondents (91%) noted the increased demands of the position, no doubt due to the size and complexity of their enterprise network environments, the increasing demands on them, and the threats to the network.

As a result, however, a majority of those surveyed also agreed that the networking team is becoming more important to IT's mission (82%), more involved in security initiatives (84%), more successful in driving innovation in collaboration with other IT teams (79%), more integral to shaping IT strategy (74%), and that the role of the networking professional is becoming more rewarding (62%).

Security, Speed, and Reliability Rule the Agenda

More than half (51%) of the IT and business professionals surveyed at enterprise organizations (1,000+ employees) anticipate an increase in their total IT budget over the next year with an additional one-third (38%) saying that it will remain the same. Similarly, nearly half (45%) of SMBs (<1,000 employees) anticipate an increase with 41% expecting it to remain the same. On average, budgets will increase by 8% for enterprise organizations and 6% for SMBs.

Security and speed will be top of mind this year along with the traditional network priorities of ensuring availability and continuity for the business. Protecting against data breaches and leaks continues to be the top network challenge (35%), followed by ensuring availability (27%), ensuring business continuity (25%), and having the right IT talent in place (23%).

Accordingly, respondents said that the primary drivers of networking investments are improving network speed and performance (55%), improving data security (53%), ensuring availability (50%), ensuring business continuity (46%), improving IT process efficiency (43%), and improving business process efficiency (41%). Cost cutting was least likely to be a deciding factor with just 19% of those surveyed saying reducing operating expenses would be a driver and 15% indicating that reducing capital expenses would be.

Being closer to network technologies, it's not surprising that those on the team primarily responsible for networking were more likely to put higher importance behind multiple business drivers of their budget versus those not on the team. For example, more than half of them (52%) said business continuity and business process efficiency were important

(versus 38% and 32% of those not on the team) and 43% said improving agility and flexibility to react to business changes was a significant driver (versus just 26% of those not on the team).

Demand management continues to be the name of the game for those managing corporate WiFi. Keeping up with the proliferation of end user devices remains the top WiFi concern, at 44% again this year, followed by ensuring the WiFi infrastructure is capable of supporting evolving needs like video streaming (38%), and ensuring WiFi coverage throughout the enterprise (37%).

Some of the areas of increasing investment in 2016 will include network security (50%), applications development (42%), data storage (43%), computing hardware (37%), software (35%), data management and analytics (35%), and compliance (38%).

IT network organizations are actively researching, piloting, implementing, or upgrading a variety of technology initiatives. Not surprising, network security monitoring is at the top of this list with nine out of ten organizations in some aspect of actively looking into related projects, piloting, implementing, or upgrading. Network security monitoring and server consolidation have the highest percentages working to upgrade or refine (26% and 19%, respectively) the technology compared to other technology areas. When looking at a specific aspect of the technology adoption process like actively researching a technology initiative, software-defined networking (SDN) rises to the top of the list (43%) followed by infrastructure as a service (37%) for enterprise organizations. These key areas of the technology adoption process present an opportunity for vendors to connect with organizations looking for solutions.

Large enterprises were more likely than their small- to medium-sized counterparts to be managing or researching all categories except for network security, which was equally prevalent in enterprises of all sizes.

Cloud Computing Reaches a Tipping Point

However, the biggest spike in spending this year will be on cloud services. Six out of ten respondents (63%) said that they will increase cloud-related spending this year, compared to 43% in 2015. Perhaps related to the proliferation of cloud implementations, the most popular spot for spending cuts will be the data center (18% will decrease investment).

The expansion of cloud computing will bring both challenges and benefits for Network IT. Seven out of ten surveyed said that cloud will add complexity and difficulty for the networking team, and six out of ten indicated that cloud will alter the structure of the networking team and have an impact on collaboration within IT. At the same time, 67% stated that cloud will allow the networking team to broaden their technology knowledge and become more valuable, and 57% said that the technology will enable the networking team to play a more strategic role within the organization

The short-term impact on security strategy, however, will be contained. About a third (34%) of respondents said cloud will require moderate changes to security strategy and nearly a quarter (24%) said only a few tactical changes will be necessary. Just 14% indicated that cloud would require a complete overhaul of security plans.

A Shifting Security Landscape

When it comes to deploying network security solutions themselves, companies are deploying a mix of hosted and traditional in-house solutions. Just under half (49%) say they will deploy a mix of on-premises and cloud-based security systems, while more than a quarter (27%) will implement on-premises solutions only, and just 7% are comfortable with a full cloud deployment.

Network security automation is a mixed bag. On average, 43% of an organization's network security is automated. Twelve percent are less than 10% automated. The largest portion of respondents, one-fifth, say their network security is 10% to less than 25% automated, and 16% indicated that their security is either 25% to less than 50% automated or 50% to less than 75% automated. Ten percent are 75% to less than 100% automated and just a handful (6%) have full automated network security. Of those who have deployed automated solutions, 34% say they are extremely or very confident in it, while just under half (48%) are somewhat confident.

Employee awareness and cooperation took over as the top security-related concern (35%); moving up from the 3rd biggest concern in 2015. This correlates to the 2016 Global State of Information Security Survey that showed current employees and former employees topping the list of likely sources causing security incidents. Employee education can help to stem the problem of private or sensitive information being exposed unintentionally. In terms of outside the organization, protecting against threats such as advanced persistent threats and distributed denial-of-service attacks (33%) remains a top concern. Executive level IT see this as more of a concern (38%) than their mid-level (24%) and IT professional (33%) counterparts. Budgetary constraints rose as a top challenge with 29% saying it is of concern compared to 25% last year. Additionally, managing the security and risk surrounding mobile devices remains a high security challenge with 28% citing it as a concern. Just 17% of respondents were worried about protecting against malicious insider threats, despite the increased damage that an employee can do.

Respondents are considering a number of new security initiatives, particularly around new and expanding capabilities like mobility and social media along with persistent or increasing threats. Respondents are actively researching or have on their radar enterprise mobility management such as mobile device management (MDM), mobile application management (MAM), and mobile information management (MIM) (57%), ID management solutions (54%), securing access for mobility programs (54%), securing access to social media (52%), data loss prevention (52%), next generation firewalls (52%), and corporate data encryption (50%).

Respondents aren't entirely sure about handing these new (or existing) security programs over to emerging vendors. Nearly three out of ten (29%) said their perception of risk increases with new vendors versus established players while 40% said they're equally risky. Fourteen percent said new vendors would be less risky.

Software-Defined Networking and Internet of Things: In Limited Release

Companies continue to show interest in software-defined networking (SDN), with similar levels of respondents (41%) as a year ago indicating that they are actively researching the approach or have it on their radar. However, just 16% of companies have SDN installed or in production, 5% are piloting it, and 4% are upgrading or refining it. When looking by company size, enterprise organizations are ahead of SMBs with regards to piloting it or having it installed or in production today (27% vs. 16%). Over one-third of overall respondents (35%) say they have no plans for SDN this year; however, when looking at company size, we see that 41% of SMBs say they have no plans today versus just 25% of enterprise organizations.

Looking ahead a year from now, it's apparent that both enterprise and SMB organizations plan to be farther down the adoption curve. Enterprise organizations will move from 12% piloting today to 22% planning to be in the piloting stage 12 months from now. Similarly, 4% of SMBs are piloting today versus 12% planning to a year from now. This illustrates the opportunity for SDN vendors to connect with companies still in the researching phase that have active plans to move their organizations into piloting and installation within the next year.

Several challenges inherent in emerging technologies have led to the delay in more widespread adoption, chief among them a lack of necessary IT skills cited by 41% of respondents. Other issues include integration with legacy technology (34%), staff resource constraints (28%), and lack of trustworthy and reliable support from vendors due to the immaturity of the technology (23%).

Internet of Things (IoT) technologies are getting somewhat more traction with 20% of enterprise respondents and 15% of SMBs noting that IoT efforts are underway today. Another 43% of enterprises and 32% of SMBs are planning implementations within the next three years. However, a little more than a third (37%) of enterprise companies and the majority of SMBs (52%) say they have no plans for IoT at all.

While business leaders like CEOs, COOs, and presidents are taking charge of IoT efforts at one in five SMB companies, IoT looks to be largely an IT-driven business innovation, especially for enterprise companies. Roughly four out of ten enterprise respondents said their CIO is leading IoT efforts followed by 21% executive VP, SVP, VP IT leading, and 19% IT architects.

Out of the Data Center

With networking capabilities increasingly critical to digital-enabled business innovation, the networking organization must continue to operate in collaboration with other areas of the business. Networking executives, managers and leaders are working closely with other groups within the technology organization as well as across multiple business functions.

Network IT works in collaboration on a daily basis with IT services/help desk and IT operations at 44% of organizations, with systems administration (41%), and IT security (40%). Cross-departmental collaboration in the form of adopting the DevOps approach to software development, has been or is being adopted at some level at nearly half (46%) of large enterprises (down from 54% last year) and at 25% of small- to mid-size companies. Enterprise respondents said the top drawback to not adopting DevOps would be slower time to market (30%). As many companies are continuing to transform their business into digital-centric, non-adoption of DevOps means slower time to market with their products and services and places a hindrance on that transformation. Other common drawbacks of not adopting DevOps would be less collaboration between development, IT operations and business (29%), and lack of visibility into IT operations requirements early in the development lifecycle (27%).

Looking beyond the walls of IT, the networking group works hand in hand with corporate operations on at least a weekly basis, according to 44% of respondents and collaborates at a similar frequency with top business executives (39%), technical consultants (35%), the cloud infrastructure team (33%), corporate finance (29%), and sales and marketing (26%, both).

When seeking to join forces with those outside of IT, however, the networking group is traditionally the initiator. Six out of ten networking team respondents said that their team either always or usually has to initiate such collaboration efforts with the business.

Methodology

Network World's 2016 State of the Network Survey was conducted among members of Network World's Tech Connections Panel and among visitors to NetworkWorld.com. The survey fielded online with the goal to help tech marketers inform their product development, marketing and messaging strategies, specifically relating to emerging technologies that impact the network. This was a targeted research effort, to be considered qualified respondents must have indicated that they are primarily responsible for at least one of the following technology areas: Application development, Cloud services, Compliance, Computing hardware, Data center, Data management/analytics, Data storage, Database, Intranet, IT governance, IT operations, Network security, Network/Systems management, Programming/Sys Analyst/Architect, Software, Systems engineering, or Telecommunications.

Results are based on 301 completed surveys. The margin of error on a sample size of 301 is +/- 5.7 percentage points. For the purposes of this report, enterprise organizations refer to those respondents at companies with 1,000 or more employees. SMBs refer to those respondents at organizations with less than 1,000 employees. Percentages on single-select questions may not sum to 100 percent due to rounding.