EXECUTIVE SUMMARY

2017

State of the Network Survey

NETWORKWORLD
FROM IDG

In Turbulent Times, Organizations Focus on Security, Continuity

The waves of technology-fueled change and revolution have yet to wash over corporate networks, where security and continuity of operations are the hot technology trends.

WE LIVE IN TURBULENT TIMES. All you need to do to prove that thesis is to surf on over to your favorite news website, where the headlines will most certainly be of political and economic shifts, realignments and uneasiness in North America, Europe and in Asia.

This is equally true of the technology sector, which is prone to discussions of digital disruptions and exploration into new solutions. Predictions of huge, technology fueled changes to our lives and workplaces are coming faster and harder than ever before, as technologies like cloud computing, mobility, machine learning and big data analysis are poised to transform the nature of work itself.

How accurate are these predictions? Our annual State of the Network survey found clear evidence that at least some of these waves of technology fueled change are starting to wash across organizations both large and small while balancing ongoing goals.

True: networking professionals tell us that change, in 2017, will be evolutionary rather than revolutionary, with somewhat larger budgets and level investment in things like regulatory compliance, network management and data center technologies. But it is also true that a host of new demands are shaking up the profile of the network team, as security threats loom and technologies like cloud computing, storage and desktop virtualization and automation challenge networking professionals to embrace change without impacting network availability and business continuity.

More money, but more hats for the network team

How does the world look to these network professionals? Considered against many of the factors we use to measure network IT, the coming year will look like the year that preceded it. Responses from the IT professionals we surveyed indicated that the all-important measure of organizational support – the IT budget – is expected to increase in 2017 compared with the year before, and often substantially. Forty-seven percent of IT pros say they expect their budget to increase from the previous year.

Still, increasing budgets aren't ubiquitous. Forty-one percent say their budget will be flat in the next year. It's worth noting that those two numbers are almost identical to responses recorded last year, when 47% of networking professionals said that they expect funding to rise and 40% expect level funds in the year ahead. Also, consistent with the 2016 State of the Network report: IT professionals see their jobs becoming more important and more demanding in the new year. More than three quarters (78%) of those surveyed felt like networking will become a more important component of the information technology group's overall mission in the next year, with 35% strongly agreeing with that notion.

78% AGREE THAT NETWORKING WILL BECOME A MORE IMPORTANT COMPONENT OF IT'S MISSION IN 2017.

More demands go along with that higher profile. Taking the 50,000 foot view of things: a convincing 87% of the networking professionals expect their job to become more challenging in the next year. Forty-two percent strongly agree with the notion that 2017 will be more challenging than 2016 and just 9% disagree with the idea that the job will become tougher in the months ahead. When we asked the same question last year, 85% said the job would be more challenging in the year ahead.

More challenging how? And why? Our respondents' feelings that their job is becoming more challenging may reflect on-the-job realities. Network professionals 10 or 20 years ago may have been content with keeping the network and its users humming along or patching and upgrading server hardware and software. Today's professionals don't have it nearly as simple. Our survey revealed an expanding roster of responsibilities for members of the networking team, who are called on to wear many more hats and to lend their expert opinion to a far wider range of issues.

We delved into the kinds of responsibilities network professionals have. Among the 230 survey respondents who told us they are part of the team that is primarily responsible for networking, we uncovered a wide range of ancillary responsibilities that are also part of the networking job.

For example: pluralities of respondents said that they helped shape the purchase of wide range of technologies for their employer. These ranged from network and systems management products and services, to network security technologies and IT operations tools. Their involvement ranged from determining business needs and technical requirements to recommending vendors or products for purchase, or assisting in the sale of new products or technologies internally.

PURCHASE PROCESS INVOLVEMENT

DETERMINE BUSINESS NEED

64% Network Security

62% Data Storage

DETERMINE TECH REQUIREMENTS

66% Network Security

66% Architecture

EVALUATE PRODUCTS/SERVICES

68% Architecture

67% Systems Engineering

RECOMMEND/SELECT VENDORS

65% Systems Engineering

65% Telecommunications

SELL INTERNALLY

42% Data Mgmt/Analytics

42% Telecommunications

AUTHORIZE/APPROVE

48% Architecture

48% Programming

There are more complex lines of communication into and out of the network group, as well, we found. Eighty-two percent of professionals said that the network team at their organization is more involved with security initiatives than in the past. Further, 71% said that their networking team collaborates with their IT security team on a daily (41%) or weekly basis.

And the collaboration isn't limited to security. Eighty percent of the network and IT professionals agree that greater collaboration between networking and other parts of their organization is driving innovation. Seventy percent of the professionals feel as if the networking management team is more involved in shaping overall IT strategy.

Preparing for change

The truth is that change happens more slowly that we'd expect, even within forward looking and technology friendly firms. Real change, when it happens, is evolutionary rather than revolutionary: building over time in patterns that are clearly visible, not sudden and unexpected. Our survey found evidence of that in the continuity with prior years' surveys when it comes to the kinds of technology investments that companies are making.

Investments in areas like regulatory compliance are mostly expected to stay level (61%) or even decrease (7%) in the next year, while just 30% expect increases in that part of the IT budget – possibly due to these technologies already being in place. Similar results appear with data center investments, as cloud computing technologies hold a presence. Almost three-quarters (72%) of our respondents expect investments there to hold steady in the next year (51%) or decrease (21%), with just a quarter expecting to see an increase in data center spending.

ORGANIZATIONS HAVE PLANS TO INCORPORATE VARIETY OF TECHNOLOGIES INTO IT STRATEGY...

89%	Network securtiy monitoring
82%	Server consolidation
76%	Data management/analytics
75%	Data center storage efficiences
74%	Storage virtualization

Still, change is on the horizon and respondents tipped us off to some of the areas in which their employers are investing and experimenting. Asked what technologies are on the radar or being actively researched, network and IT professionals identify data analysis tools as one area of interest. Three quarters of network team members (76%) say such tools are an area of investment for their organization and more than a quarter of those say data analysis tools are either on the radar or a subject of active research.

Other technologies that our respondents' employers are looking into include desktop and storage virtualization, as well as software defined networking technologies. But new technologies also introduce new and unforeseen risks. That may help explain why concerns about the security and the integrity of network environment emerged as a top concern and point of anxiety.

For example, strong market forces are pushing more and more applications and data to the cloud. At the same time, news reports have highlighted the risks of crippling denial of service attacks against web sites and core Internet ecosystem players. Perhaps reflecting the uncertainties that go along with operating a hybrid or cloud reliant business, network professionals are very concerned about network availability. Thirty-five percent rated it as their top concern while a quarter said that ensuring business continuity was the top concern at their firm.

NETWORK/DATA CENTER CHALLENGES

38%	Protecting against data breaches/leaks
35%	Ensuring availability
25%	Ensuring business continuity

It is worth noting that such concerns took a back seat to data protection, highlighting the widespread awareness of the epidemic hacks and data theft that have affected all industries. Protecting against data breaches and leaks was the top challenge identified with 38% rating it as a top concern. In addition, improving data security is a top driver of networking investments (55%), just behind improving network performance, which 61% rated as a primary driver.

Our respondents' fixation on security isn't about boxing shadows. It is an understandable reaction to a real increase in the risks facing organizations, which are besieged by a wide range of online foes. These threats range from cyber-criminal groups pushing ransomware onto corporate networks to crippling denial of service attacks to rampant theft of data from organizations in the healthcare and government sectors.

The stakes in these attacks – measured on both the balance sheet and in terms of reputation – are also rising. In November 2016, San Francisco public transit agency was forced to give free rides after a stubborn ransomware attack froze critical systems and displayed the message "You Hacked" on terminals in Muni subway stations. Yahoo Inc. reported in December 2016 that information on one billion (with a "B") customers had been stolen in an attack dating back to 2013. This after revealing in September that some 500 million user accounts were exposed in a 2014 incident. In the wake of those revelations, the company's pending acquisition by Verizon is in jeopardy.

Those incidents and a long list of others like them have increased pressure on network and IT professionals to formulate security and continuity strategies that go far beyond keeping viruses off corporate desktops and hackers on the other side of the firewall. More connected infrastructure means the possibility of cyber-physical attacks. At the same time, security initiatives increasingly span corporate networks, mobile devices and the cloud. Increasingly, they encompass both second- and third party relationships, as well.

More security budget...but for what?

Most of the respondents expect budgets for network security to increase in the next year. A strong majority (55%) expect more money for addressing network security in 2017 and 38% say the levels will stay the same. Only investments in cloud services were earmarked for a greater increase in investment.

44%
REPORT EMPLOYEE AWARENESS & COOPERATION TO BE TOP SECURITY CHALLENGE

What will that money be spent on? In theory, spending should track closely with threats and attacks. But in the security space, coupling spending with actual risk can be difficult. Asked what the top security challenges and obstacles their organization faced, employee awareness and cooperation ranked as the top challenge (44%) – and one without any easy, technology fix. The next highest ranked threat – protecting against threats from outside the organization like DDoS attacks and so-called advanced persistent threat actors – is another big, scary and very real concern without an easy remedy. The risks there were on display in September and October of 2016, when firms such as Twitter, CNN, PayPal and Amazon.com saw their operations hampered by a massive denial of service attack on a provider of managed Domain Name System (DNS) services.

To figure out where security spend is likely to happen, we surveyed our network professionals on their plans for a wide range of security technologies. No clear candidate emerged as a hot new security product, but the responses did give us a good sense of the technologies that are well established on networks and those that are gaining wider adoption.

Endpoint protection products, for example, are already in use on 65% of the networks managed – a good example of a mature security product. Thirty-four percent said that data loss prevention (DLP) tools are installed or in production, and 11% are in the process of upgrading these tools as their organization. Coupled with the 26% who are piloting or actively researching the technology, that suggests that DLP – once a niche security product – is gaining widespread acceptance in an era of massive, headline grabbing breaches. So too corporate data encryption technology, with 43% saying their company has deployed it or is in the process of upgrading or refining their corporate data encryption technology. Another 21% said they are piloting or actively researching the technology.

INSTALLED SECURITY TECHNOLOGIES

56%	Network security
52%	Endpoint security
35%	Corporate data encryption
34%	Data loss prevention tools
31%	Next generation firewalls

As security technologies and business models evolve, however, the way that even those established security technologies are deployed is changing. Just 27% of those we surveyed said that network security solutions will be deployed solely on premise in 2017. A strong majority, 58%, said that their networking security products will be a mix of on premise and cloud services, while just 3% expect to embrace wholly cloud-based security services in the next year.

Changes are afoot on the network

The business press may be agog with the possibilities of The Internet of Things (IoT), software defined networking and machine learning and automation. But when it comes to investing in the future, respondents revealed cooler heads and a more pragmatic approach to the future: embracing new technologies and approaches where they stood to gain the most benefit, and putting money behind the technologies that will help their organization best transition to the future.

There was broad interest in faster wireless technologies like 802.11ac "gigabit" WiFi. Twenty-two percent of network/IT professionals said they already adopted the standard and close to a third said they will be doing so in the next two years. Only a quarter (25%) said they have no plans to adopt faster wi-fi technology in their organization.

Security automation technology is another example. There has been much written about the potential of automation to replace low-level IT workers of all stripes. In the information security field, security analysts and security operations center (SOC) workers spend their days combing through event logs and the output of various security tools. There's strong evidence that this kind of automation is taking amid our surveyed professionals. They reported that about 40% of network security is automated at their organization. More than a quarter (27%) said they are extremely or very confident in the technology while more than half (54%) said they are somewhat confident in the results they got from security automation tools.

On IoT, respondents see great potential when it comes to improving the way their company operates. Applications for IoT technologies in areas like customer service and support (44%), improving operational efficiency (38%) and data management and analytics (36%) all rated highly. Almost a third see the potential for new products and services based on IoT technologies like remote sensing and cloud based data analysis.

BENEFITS OF IoT

44%	Customer service and support
38%	Operational efficiency
36%	Data management/analytics
29%	Creating new products and services

Asked to describe their company's IoT efforts, eight in ten respondents said that their company still has no IoT efforts underway, with 40% saying their employer has no immediate plans for IoT based products and services at all.

A quarter expect some IoT initiatives to be underway within the next two years, while 13% said plans for IoT initiatives are further out in the 2 to 3 year timeframe.

Still, it's important to note that larger companies appear more game to try their hand with IoT. Just 29% of enterprises said they have no IoT deployments underway and no plans for them, compared with 51% of SMBs. And 31% of enterprises said they do have IoT projects in the work – compared with just 10% of SMBs.

If companies are dipping a toe in IoT, they're ready to submerge a whole foot – or even a leg – in areas like virtualization, where there are clear benefits to be realized in cost, performance and agility.

For example, hyperconverged networking is a 'virtualization first' approach to deploying IT assets with applications in areas like data center consolidation, disaster recovery and desktop virtualization. It promises huge cost savings and efficiencies for companies that can find a way to migrate critical systems and data to hyperconverged IT architectures.

We asked our survey respondents about their plans for hyperconverged networks. Close to half (48%) said that hyperconverged networks were on their radar, or that they were actively researching or piloting the technologies.

We got a similar response when we asked about software defined networking (SDN), a more flexible and dynamic approach to networking and promises firms both greater control over networks and lower costs. While adoption of SDN technologies has been gradual, almost half of our respondents (49%) said they were either considering or actively piloting SDN technologies. Another 18% said they had already deployed SDN technology or were upgrading it within their organization.

Here again, larger companies are more likely to experiment with technologies like hyperconverged networks and software defined networking technology than small organizations. Enterprise organizations are three times as likely to be piloting such technologies (13%) than are SMB organizations (4%).

Looking to the future: some big questions

Looking ahead to the future, our networking professionals tell us that change will be steady and inexorable. From security to advanced analytics to cloud based computing, organizations are moving ahead in a deliberate fashion and with an eye to making their organizations more efficient.

But challenges loom. Technologies like cloud computing and software defined networking offer huge opportunities to organizations to reduce costs and improve their agility. But they also require new talent and skills that can be hard to come by. It's worth noting, for example, that IT skills gap is the top cited challenge to deploying SDN technologies (46%), ahead of even integration concerns (40%).

Such environmental challenges – finding skilled workers, avoiding wasteful spending or non-productive investments, steering clear of known risks like crime and extortion – are familiar to brick and mortar companies as well as high tech firms. The challenge for companies across the spectrum will be finding creative solutions to those endemic problems so that they can reap the maximum benefits that technology offers their firm. Doing this, while also navigating a business, regulatory and political environment at home and abroad that may go topsy-turvy, is sure to keep networking professionals occupied in 2017!

About our survey

We surveyed 294 professionals with exposure to network IT at their place of employment for the 2017 State of the Network survey. More than three quarters of our respondents (78%) said they were primarily responsible for networking at their organization. Respondents are nicely balanced between enterprise organizations (51%) with more than 1,000 employees and small and mid-sized firms (49%) with fewer than 1,000 employees. The average company size was 13,386 employees. There is a variance in respondents IT budget as well – 31% said they worked for companies with IT budgets less than $1 million, and 8% of respondents said they worked for companies with IT budgets ranging from $250 million to $1.5 billion annually. The average IT budget was $125 million annually.

Methodology

Network World's 2017 State of the Network survey was conducted online among members of Network World's Tech Connections Panel and among visitors to NetworkWorld.com between August 29, 2016 and September 26, 2016. The goal of the study was to help tech marketers inform their product development, marketing and messaging strategies, specifically relating to emerging technologies that impact the network.