Research Report

FREEFORM DYNAMICS

in association with

JUNIPER NETWORKS

Network security in the spotlight

Understanding why it can go wrong is key to making the right investment decisions

Freeform Dynamics, 2020

Introduction

The first half of 2020 saw dramatic shifts in network usage as much of the world shifted to remote and home working, and as businesses went through years-worth of digital transformation seemingly overnight. This has made network security more important than ever, yet the main trigger for deciding to upgrade network security remains "Shutting the stable door after the horse has bolted." In other words, wait until something goes wrong before you act to prevent it happening again.

This approach can result in significant pain both for the business and for its operational staff. Where and why is this pain most severe, and how are network security staff and others working to change this? How are buying decisions made – and how can administrators avoid being unfairly blamed for security failures – in an area where new threats and defensive technologies appear with amazing frequency? And do the advantages of single-sourcing your network security outweigh the advantages of being able to choose and combine the best technology from a range of suppliers?

Those were just a few of the big questions we recently asked in an online survey. In this report, we summarize the answers of 223 respondents working in a range of business and technology roles, all of them involved in networking and/or security. Our conclusions confirm that many challenges are shared ones, but we also highlight key factors that differentiate top performers from the mainstream, and we suggest new and better ways for everyone to improve network security.

Making the right decisions is key for business success

It's of little surprise that more than 80% of our respondents agree future business success depends on making the right network security decisions, with only 3% disagreeing (Figure 1). The risks of getting it wrong are just too numerous and varied, from data losses due to user error or criminal action, to new network threats breaking through your defenses. It could even be something as simple as the organization losing business because its users' needs changed faster than its ability to move to meet them.

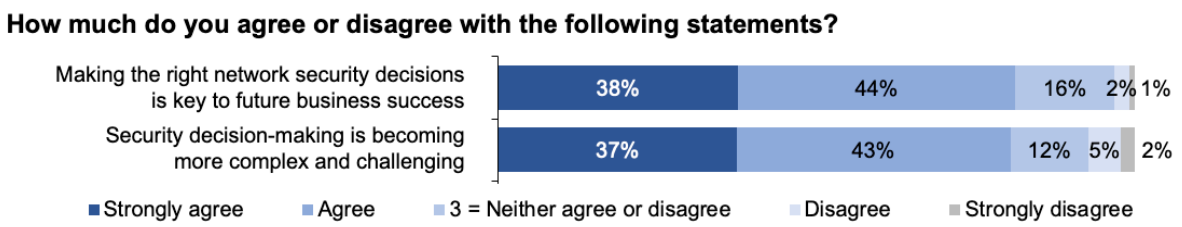

Figure 1

But those decisions are becoming harder to make

As if the range of network security technology on the market wasn't already broad and confusing enough, we now have cloud and software-as-a-service options to choose from as well. Add in evolving user expectations, as a new and allegedly tech-savvy generation joins the workforce, and it's clear there are no easy decisions. Indeed, 80% of our respondents said that security decision-making is becoming more complex and challenging.

And they are too often driven by failures

When we asked what sort of events would prompt improvements in network security, the answers were clear: the strongest triggers were reactive, not proactive – change frequently does not happen until after something has already gone wrong (Figure 2).

How likely would the following events be to prompt you to upgrade your network security?

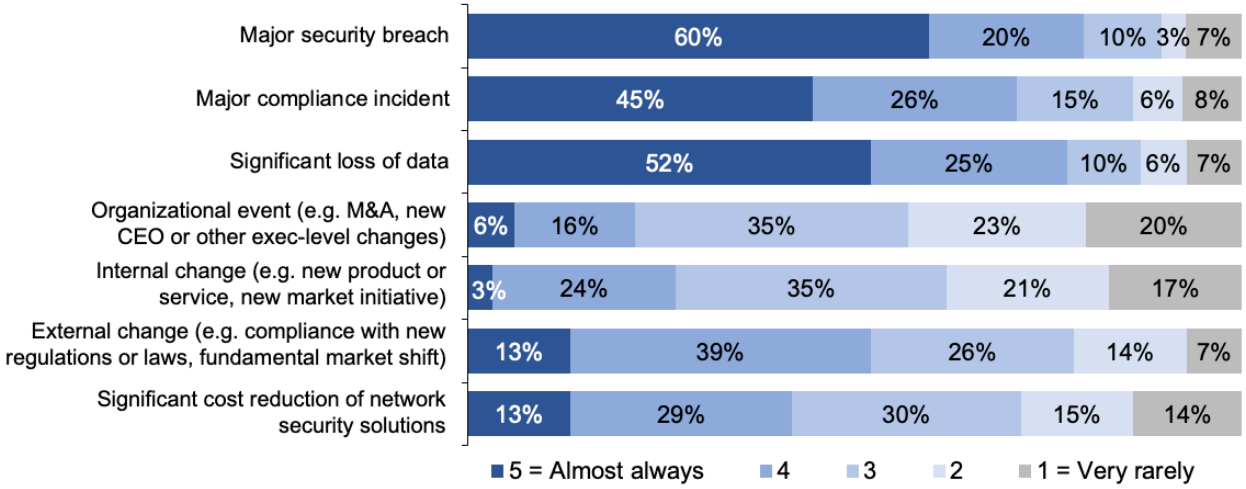

Figure 2

This was corroborated when we asked respondents to say, in their own words, what has in the past persuaded management to invest in network security. Among their comments were the following:

"A big breach or data loss has been the best way to get buy-in."

"Breaches combined with prior documentation that leadership was informed of dangers but refused to act."

"Issues being highlighted through demonstrable incidents, either in the organization or related organizations. It is very difficult to make the case through risk management and pro-active security management processes."

"Internal buy-in is always easier after a major breach or loss."

"The only thing that motivates senior management is when they're under threat in some way – loss of their job, bonus, etc. Otherwise it's business as usual."

All of this should be extremely concerning because regulations such as GDPR typically require that personal data be protected using appropriate technical and organizational measures. As an organization, if you wait until a breach or loss occurs before upgrading your network security, then it could be argued that you were negligent and that your protections were not appropriate. In such a case, it would be well within the regulator's powers to increase the severity of both the fine and any other sanctions applied to the organization and its directors.

Network security works, but isn't easy to manage

So how well – or badly – are organizations doing on network security today? And where is the decision-making complexity that we mentioned above causing the most pain or trouble? To better understand these issues, we asked our respondents to rate their organizations' current performance on a number of key areas around network security.

It is worrying that only around half of our respondents felt confident enough to say their organization's performance was good or excellent. Worse, almost a quarter expressed particular concerns over data security (Figure 3).

Most interestingly though, the two areas in which the largest proportion reported substandard performance related not to security per se, but to the (lack of) ease of network and security management. The dissatisfaction ran to 35% in the case of security management.

How well would you say your organization is performing today in the following areas?

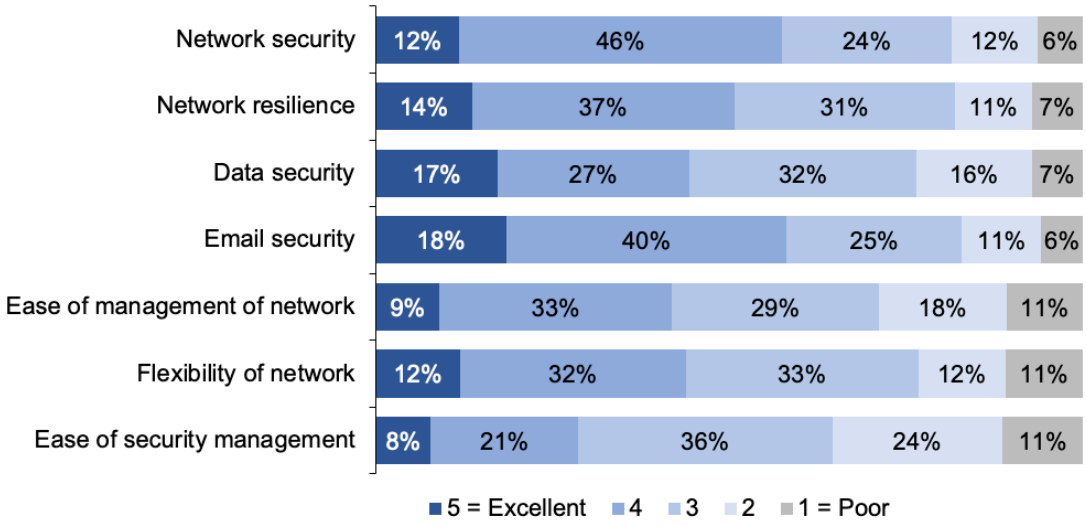

Figure 3

Clearly, there is still plenty that could be done to improve the usability and interoperability of network and security systems and tools. However, as we will see later in this report, the ease of management challenges here are as much symptoms of other problems or failings as they are problems in their own right.

Identifying the Top Performers

We also used the self-assessments in Fig 3 to calculate overall network security performance metrics for our Performance Scorecard. From this, we identified two groupings: a 'Top Performers' group comprising the 40% of respondents with the highest performance metrics, and the rest as the 'Mainstream'. In turn, this gave insight into how preferences, awareness, resourcing and so on correlate with an organization's network security capabilities.

This is useful because we see a lot of variation in some of our survey responses, but the variation calms down considerably when we regroup the answers according to our Performance Scorecard.

The attitude of senior management

A good example of this is when we asked about the attitudes of senior management. Taken as a whole, we saw a relatively even split between what one might regard as generally positive and generally negative answers.

However, once we brought the Performance Scorecard to bear, the difference was clear: Top Performers were far more likely to have senior managers who saw network security as a strategic enabler of competitive advantage, while the Mainstream were much more likely to have managers who were, at best, only minimally interested in the topic (Figure 4).

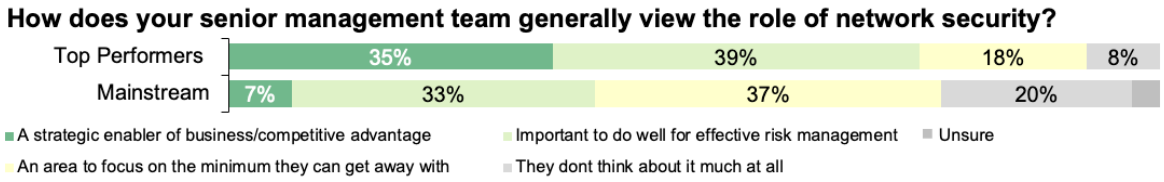

Figure 4

How up-to-date is your infrastructure?

We might expect these attitudes to carry through into how network security is actually implemented, in terms of the infrastructure available and in use, and sure enough, we see similar differences there too. When asked about the age and type of infrastructure in use, the Top Performers were much more likely to report having a significant proportion of modern and future-proof equipment, while the Mainstream were more likely to be working with older systems, approaching end of life (Figure 5).

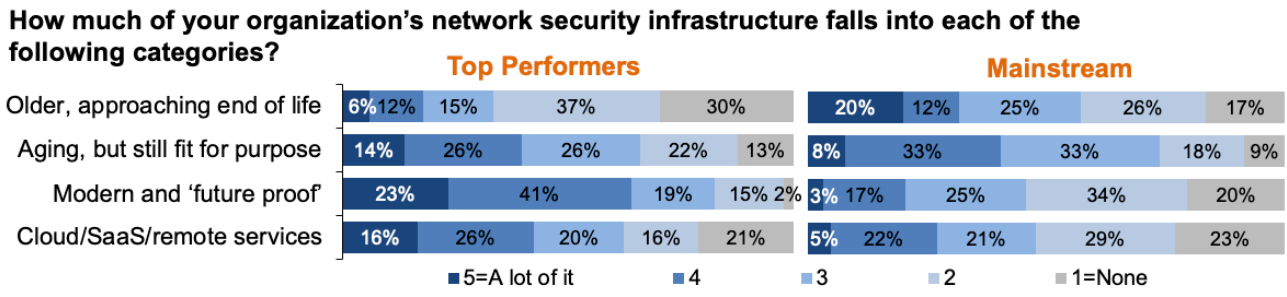

Figure 5

Similarly, while most respondents reported having at least some remote network security infrastructure, whether that be cloud, SaaS or managed services, it was the Top Performers who were more likely to employ remote services.

The one area where the Top Performers' answer might at first seem perplexing is the proportion with infrastructure that is aging, but still fit for purpose. One way to interpret this, though, is that for these respondents it is the 'fit for purpose' element that is important. In other words, it is infrastructure that does its job just as well as newer and flashier systems and will has the benefit of familiarity. As we note in the next section, newer infrastructure is typically also easier to manage and use, although of course with anything new there are still learning curves to climb.

Some pains are universal

Anyone who has worked as a network security practitioner knows that there are many pains and frustrations involved. They do vary though, from role to role, from time to time, and from organization to organization, so we assembled a list covering four notable areas and asked our respondents to rate them.

One of the most interesting things we saw once we compared the answers of our Top Performers and the Mainstream was that while there was considerable variance in some areas, others turned out to be remarkably consistent across the spectrum (Figure 6).

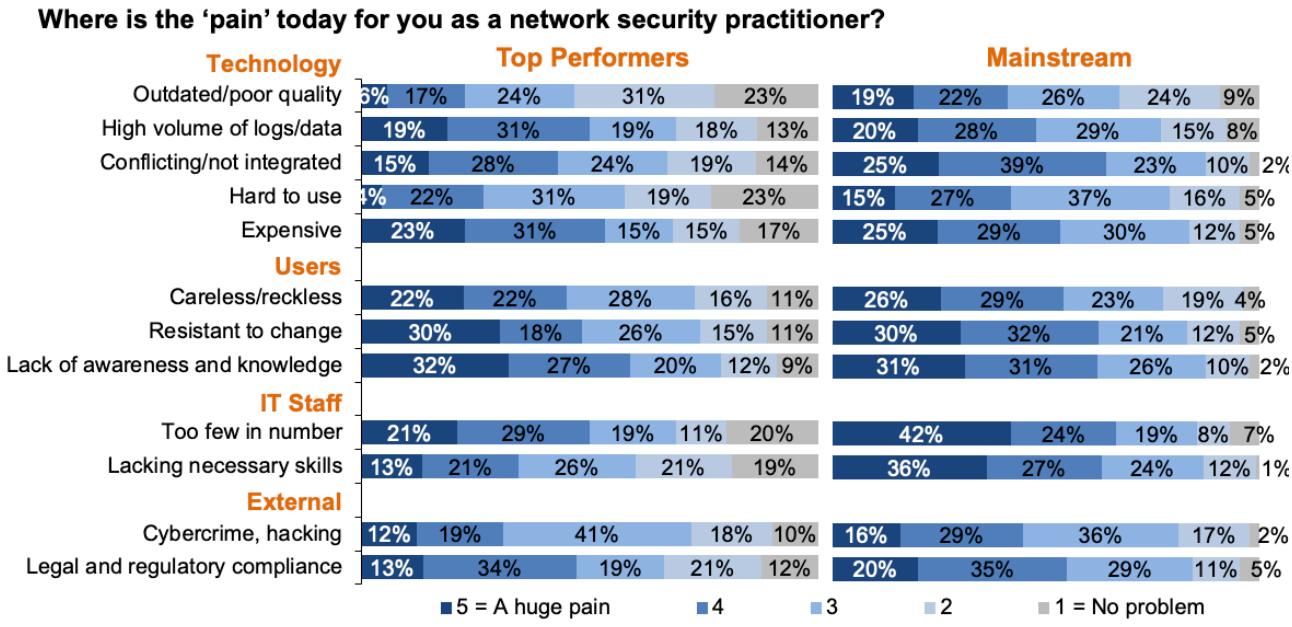

Figure 6

Of course, everyone has problems with users. For example, they often don't understand the need for network security well enough, many are resistant to change, and if they lack awareness of risk, they can be careless or even reckless. However, there are ways that security practices can make the user problem better or worse, which we will touch on later in this paper.

Perhaps the most striking thing, though, was that there were two other pain-points shared equally by all, regardless of which performance group they fell into and of their differing budgets and levels of management attention. The first complaint was that the infrastructure remains expensive, and the second was the high volume of log data that must be dealt with.

The latter is something that the industry has been aware of, and working on, for many years now – as witnessed by the number of log data management tools and technologies on the market. However, it seems clear from our survey that more work still needs to be done both here, and in terms of bringing costs down.

Other pains can be reduced

On the variance side, Top Performers were considerably less likely to report suffering the pain of outdated, conflicting or hard to use technology. In part, this ties back to the earlier questions regarding modern versus aging or end-of-life infrastructure – newer equipment is typically easier to manage, use and integrate.

They were also less likely to complain about having too few staff and inadequate skills. Again, this very probably reflects the greater respect paid to network security in many of these organizations. The greater availability of staff and skills will also help reduce the problems of integration and ease of use.

It is useful to note though that, even among the Top Performers, there were still complaints about staff numbers and skills, with barely one in five respondents able to say they had no problems here. The skills deficit is real and continues to demand attention from vendors and senior management alike.

Cloud, on-prem or hybrid?

Other areas of business have been swift to adopt services delivered remotely, whether via SaaS or a public or private cloud, but network security has not been quite as keen. Just fewer than half of Top Performers agreed that cloud services and SaaS were important parts of their security strategy (Figure 7).

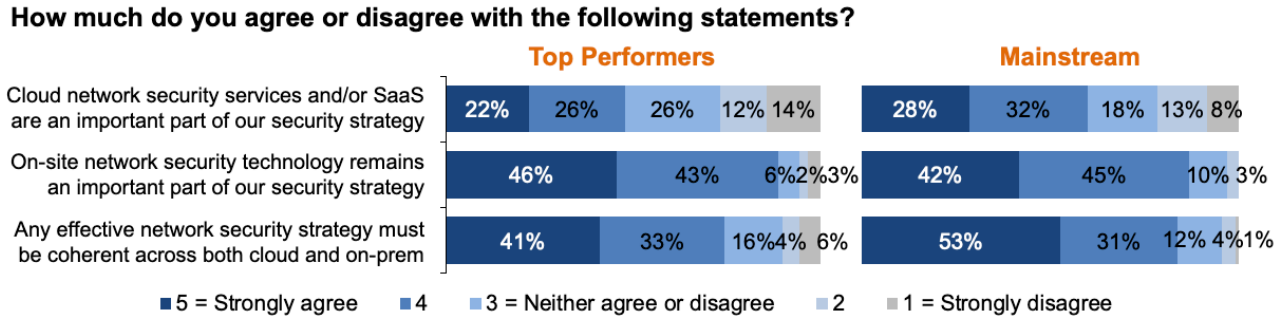

Figure 7

The proportion of the Mainstream keen on cloud was slightly higher at 60%, which may reflect their greater problems with on-site staff and skills shortages. And whatever the usage of cloud/SaaS solutions for network security, there is no doubt that the vast majority of respondents still consider on-site technology to be key to their strategy.

Not surprisingly, with the majority using a hybrid of cloud/SaaS and on-site network security technologies, we saw general agreement on the need for coherency across the various delivery mechanisms. Taking all the respondents together, 80% saw this as important for effective network security, with just 7% disagreeing – presumably because they exclusively use either on-prem or cloud, but not both.

The question then is, with so much complexity and so many challenges, what's holding people back from working to improve things?

Why is it hard to improve network security?

When we asked about factors that inhibit better network security, the answers fell into three main groups. The biggest issues for all were lack of budget and time, though compared with the Mainstream, fewer of the Top Performers had major worries here (Figure 8).

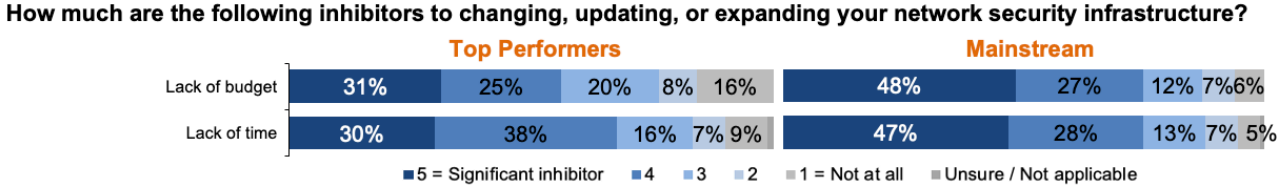

Figure 8

Two more issues which were largely shared across our survey respondents were to do with keeping up-to-date, and are most probably both related to the lack of time mentioned above. Overall, 39% said that not knowing where to focus in an ever-changing threat landscape was a significant or moderate inhibitor, while 35% said the same about the challenge of keeping up with the available range of solutions.

Where the Top Performers and Mainstream diverged was in the area of organizational priorities and stakeholder engagement. On priorities, the Mainstream were around twice as likely to report that disinterest from senior managers and an inability to properly prioritize security were significant inhibitors (Figure 9).

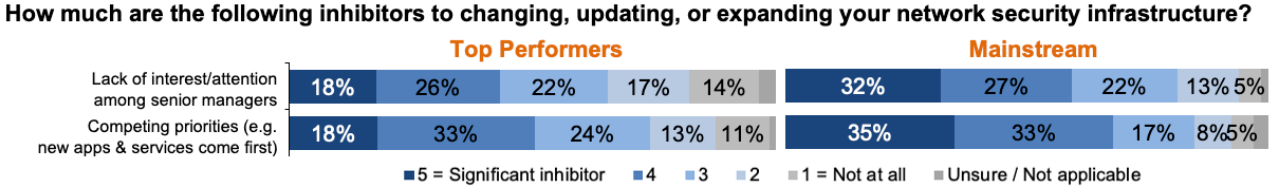

Figure 9

Both these issues suggest there may be problems with stakeholder engagement – that is, getting the proper attention of everyone involved, whether they are a stakeholder because they are technically, managerially or financially responsible, or simply because their day-to-day work requires a secure network. And indeed, stakeholder issues were what we saw when we asked our respondents about the challenges of building a business case, communicating the risks, and dealing with finances (Figure 10).

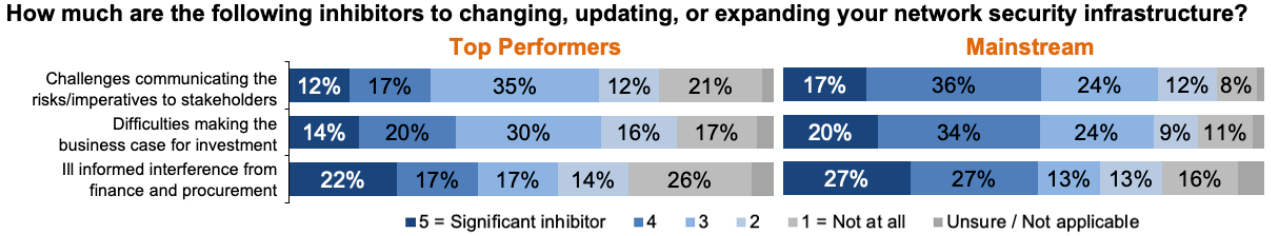

Figure 10

The 'blame game'

This issue of stakeholder engagement, or rather disengagement, links back to other issues mentioned earlier. In particular, we saw how poorly some senior managers view the role of network security, and also the challenges posed for network security practitioners by skills and staff shortages and by their user populations.

To get a deeper understanding of where and how these factors cause problems, and of potential best practice, we explored theory versus reality in network security. We asked a series of questions that revealed how often there are fundamental disconnects between who is legally accountable for network security, and who actually gets to do the work.

These disconnects exist across the board; they are less common among the Top Performers, but they present major challenges whenever they occur. For example, more than two-thirds of the Mainstream reported that senior staff sometimes or often evade their day-to-day responsibility for network security (Figure 11). This is especially worrying because these are the very people who will be legally accountable if something goes wrong, such as a security breach where customer data is lost or stolen.

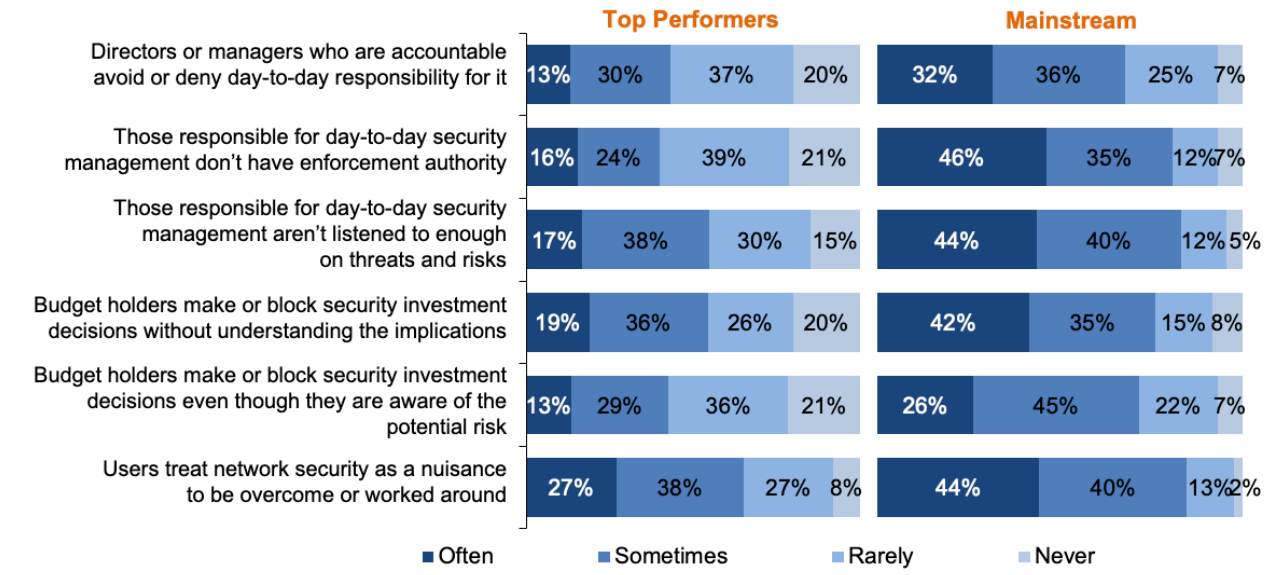

Figure 11

Similarly, more than 80% of the Mainstream (and almost half the Top Performers) said that network security practitioners are sometimes or often not given either the enforcement authority they need or the respect that their knowledge and skills deserve.

This, together with the implication that many organizations do not adequately invest in defending against known risks and threats, is just as dangerous as the evasion of responsibility. It implies a general lack of regard or respect for network security, and a desire on the business side to blame IT for any issues that arise. In addition, if users treat security as a nuisance and managers treat it as an unnecessary expense, rather than as the business enabler mentioned above, how are disempowered security administrators supposed to do their jobs?

This risks creating a vicious circle, as IT struggles to protect users who ignore advice and take risks. The users – and their managers – then blame the technologists for getting in the way of their work and seek to circumvent the network security, and so on.

Breaking the circle

Among the comments we received on how survey respondents had persuaded management to invest in network security were several that related to repositioning security as an enabler rather than a blocker. For example:

"If security is everyone's job, it is 100 times more successful than the ivory tower approach."

"It's important to explain to key stakeholders and senior management the specific risks vs. the investment cost."

"A weekly news email in plain English has helped increase awareness among senior management."

"Widen the scope of the project to be more architectural and for the organization, rather than making it just a 'more of the same' refresh."

However, there were others suggesting that, in some organizations, even a security disaster may well not catalyze change:

"Almost nothing has worked, management stupidity and ignorance overwhelm all."

"Even after multiple public hacks we will spend no time or money on security."

"Lots of ignorance, lots of political manipulation."

"What works? Fear and greed – manipulate managers so they see security as a way to expand their empires and get a fancier job title or a pay rise."

In conclusion

What this study reminds us is that network security is more than simply technology. It is just as much a perception issue – an organization's managers and staff all need to understand why network security is there, what the risks are, and who is legally accountable. Ultimately, network security needs to be seen as an integral part of business success, not as something external to the business process.

So while it may be sad and frustrating that suffering a breach or loss remains the primary trigger for upgrading network security, there is good news too. Understanding where the perception problems arise, and the consequences they can have, is important when you are looking for ways to fix them. And understanding how decisions are made today is key to finding ways to make better decisions tomorrow.

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we help busy IT and business professionals get up to speed on the latest technology developments and make better-informed investment decisions.

For more information, and access to our library of free research, please visit www.freeformdynamics.com or follow us on Twitter @FreeformCentral.

About Juniper Networks

Juniper Networks challenges the inherent complexity that comes with networking in the multicloud era. We do this with products, solutions and services that transform the way people connect, work and live. We simplify the process of transitioning to a secure and automated multicloud environment to enable secure, AI-driven networks that connect the world.

For more information, please visit www.juniper.net