2016 Disaster Recovery as a Service Attitudes & Adoption Report

Scott D. Lowe
David M. Davis
James Green
Partners, ActualTech Media

Spring 2016

Infrascale™

Table of Contents

List of Figures

Executive Summary

Disaster recovery might just be the most overlooked responsibility in IT departments around the globe. That's especially unfortunate, considering that there are products available on the market that can bring to all companies – from the SMB to the enterprise – comprehensive disaster recovery capabilities that enable the gold standard in recovery – a 15-minute recovery period for all applications – while also being budget friendly.

As you'll learn in this report, the market for Disaster Recovery as a Service (DRaaS) providers is ripe with opportunity to educate customers on the potential business benefits of a well thought out disaster recovery plan.

Here are some of the highlights from our report:

- 20% of businesses are still **entirely without a disaster recovery solution**
- Tape-based backups still account for **almost 40% of the existing disaster recovery strategies**. These companies still rely on yesterday's technologies for DR, which don't actually provide failover services and get their users back to business fast.
- **22% of respondents report experiencing more than a single outage in the past 6 months**. This reinforces the idea that many companies may be throwing away money by not investing in an on-demand failover solution to protect them.
- Not surprisingly, cost was *the most cited criteria* for not having an on-demand failover solution and *the most important factor* when evaluating an on-demand failover solution. **The perception of high cost is the biggest hurdle for organizations**. Rounding out the top four challenges:
    - Security
    - Infrastructure compatibility
    - Concerns around the reliability of the DR solution
- **37% of respondents can't even speculate what an outage costs their business**. On the harmless side, this could just be due to the respondent's position in their organization. On the more dangerous side, however, is the possibility that the respondents who are decision makers aren't even aware of their risk in the event of an outage. Given the financial challenges and public relations issues that can result from an outage, this is a pretty scary situation.
- 22% of respondents test their DR plans **less than one time per year – or never**.

Please note that we limited survey results to US-based companies with 100 to 5,000 employees only and requested that only those responsible for disaster recovery complete the survey. Bear in mind as you review the in-depth survey results.

Introduction

Although disaster recovery is not likely to be listed by many IT professionals as their favorite data center topic, the fact remains that it's a vital consideration in the greater data center strategy. A robust disaster recovery strategy can be the difference between surviving the roller coaster of modern business and closing up shop when disaster strikes.

For a variety of reasons – the primary ones being cost and complexity – an unsettling number of businesses opt out of investing in disaster recovery solutions. But more often than choosing to ignore disaster recovery altogether, many organizations make the difficult decision to protect a subset of their entire application landscape in the interest of balancing risk mitigation and cost. This isn't a decision that any IT leader wants to make though; clearly, it would be preferred to protect *every* workload in the data center.

Infrascale is working to enable companies of all sizes with reliable and affordable DR services. By providing a comprehensive disaster recovery as a service (DRaaS) product, Infrascale wants to bring disaster recovery to everyone in a way that is budget friendly while making it feasible to protect all workloads.

To this end, in 2015 Infrascale commissioned ActualTech Media to undertake a study of how organizations were handling their disaster recovery needs. This report – the 2016 edition – is the second version of that effort, and shows how the market has changed over the last year and reveals new insights about the reality of the disaster recovery landscape.

Herein, you will learn how your peers are handling disaster recovery and be able to compare your own processes and procedures. You will also learn how Infrascale can help you tackle even the most challenging disaster recovery needs and achieve 15-minute enterprise-class disaster recovery for your own organization.

Do you currently have a disaster recovery solution in place? (N=274)

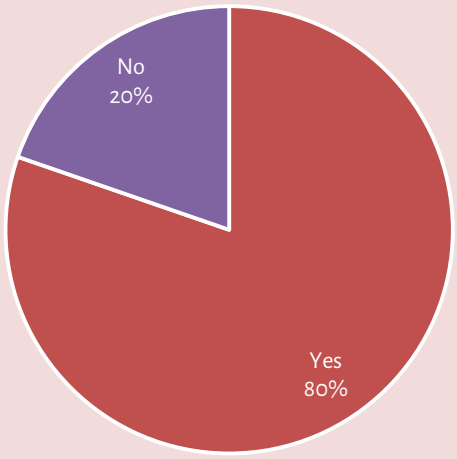


Figure 1: Current disaster recovery solution in place

Before taking respondents into the main section of the survey, we first sought to understand their position in the disaster recovery journey. As seen in Figure 1, 80% of respondents do have some form of protection from a disaster. This is roughly the same result as last year, which suggests one of two possibilities:

- The urgency of data protection is still lost on the other 20% of organizations, or is perceived as too expensive or challenging.
- The 20% without a disaster recovery solution have yet to discover a solution that fits both their needs *and* their budget.

It's interesting to look at the organizations that do or do not have a disaster recovery solution in place with regard to industry verticals. Figure 2 shows that according to respondents, *Government* and *Finance, Banking, or Insurance* are the most risk averse or – as is more likely the case – the most regulated. Many government and financial companies will be required to possess a certain level for disaster recovery capability to be compliant with industry standards. On the other hand, *Retail* and *Energy or Oil & Gas* seem to enjoy living life on the edge.

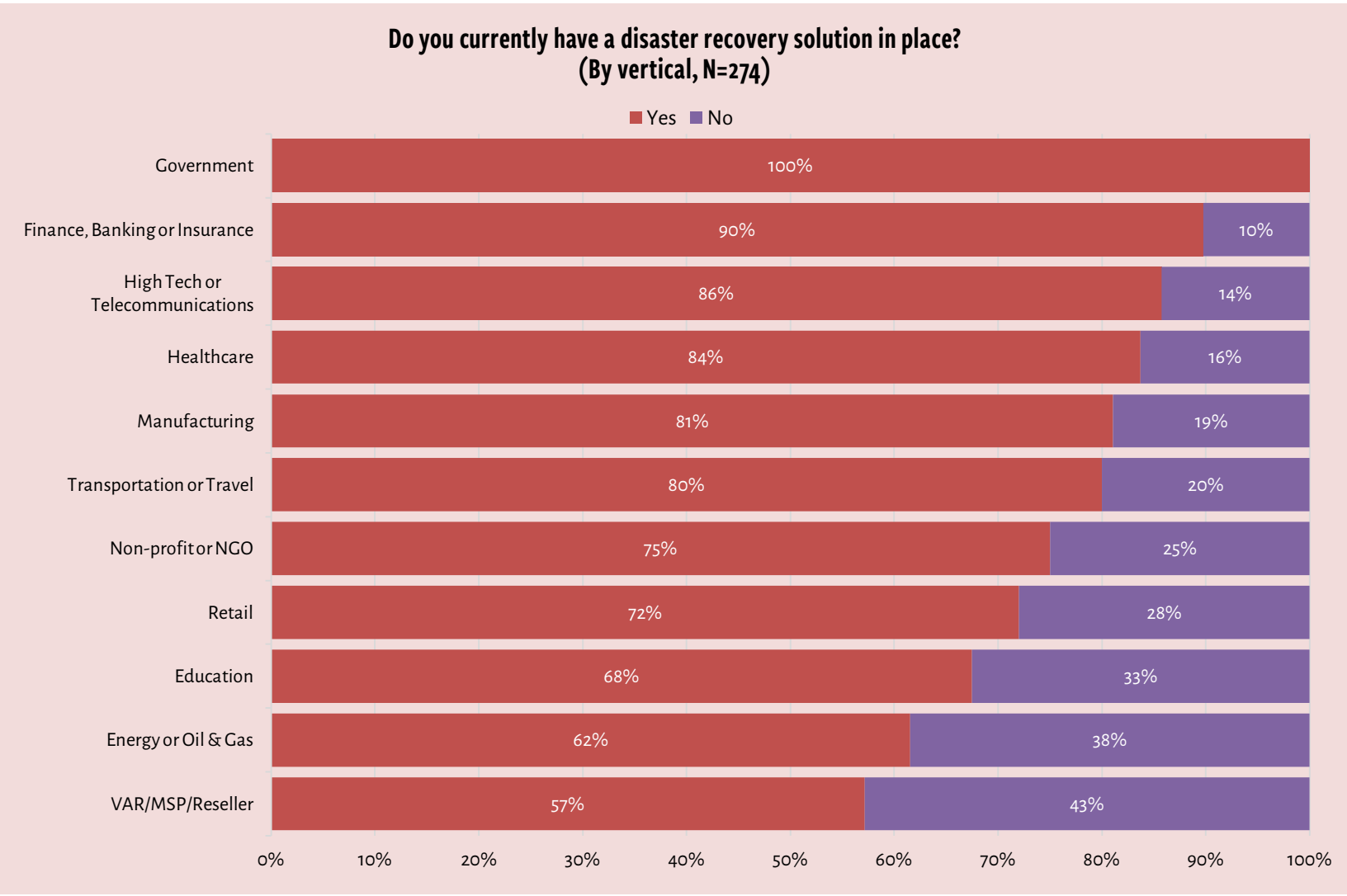


Figure 2: DR solution capability by vertical

As shown in Figure 3, 20% of respondents indicated that they are *very familiar* with the term "disaster recovery as a service." It seems plausible that they are either existing DRaaS users or their organizations have recently been doing active research into disaster recovery solutions. Consistent with last year's survey, there remains significant opportunity for vendors to continue educating customers on both the concept and the value of DRaaS. As you can see in Figure 3, 67% of respondents have *some* familiarity with the term; 20% are very familiar with the term, and the remainder are completely unfamiliar. Cumulatively, 87% of respondents are at least somewhat familiar with the term.

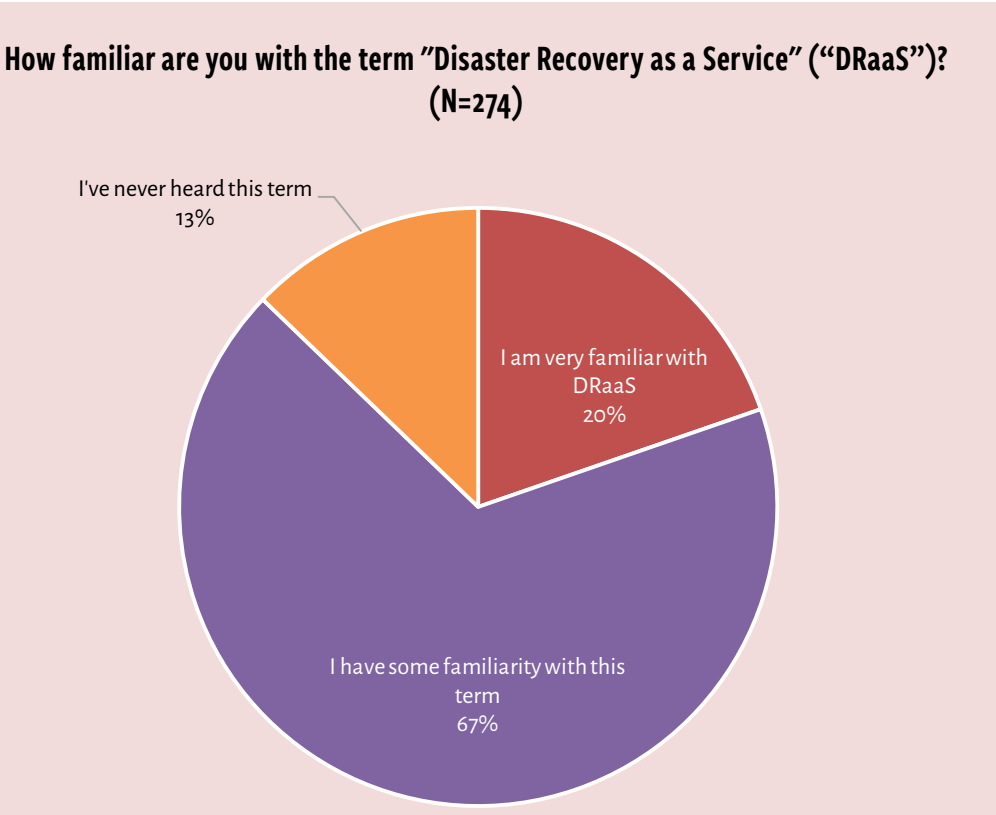


Figure 3: Understanding the term "Disaster Recovery as a Service"

Current Disaster Recovery Capabilities

We asked a number of questions intended to gauge the maturity of existing disaster recovery implementations. Understanding the current state of the environment from an availability standpoint helps make sense of decisions that are being made and also helps to clarify organizational priorities.

With respect to priorities, it all comes down to applications. Since the goal of disaster recovery in general is to ensure the availability of mission-critical business applications, we asked respondents to tell us their tolerance for downtime on certain common business applications. Note that, for 2015, we asked respondents to simply identify their most mission critical applications. For 2016, we requested that respondents tell us their downtime tolerance for each application. It becomes clear in Figure 4 that Databases and E-mail are the most critical to respondents and require the shortest Recovery Time Objective (RTO), which is consistent with last year's results.

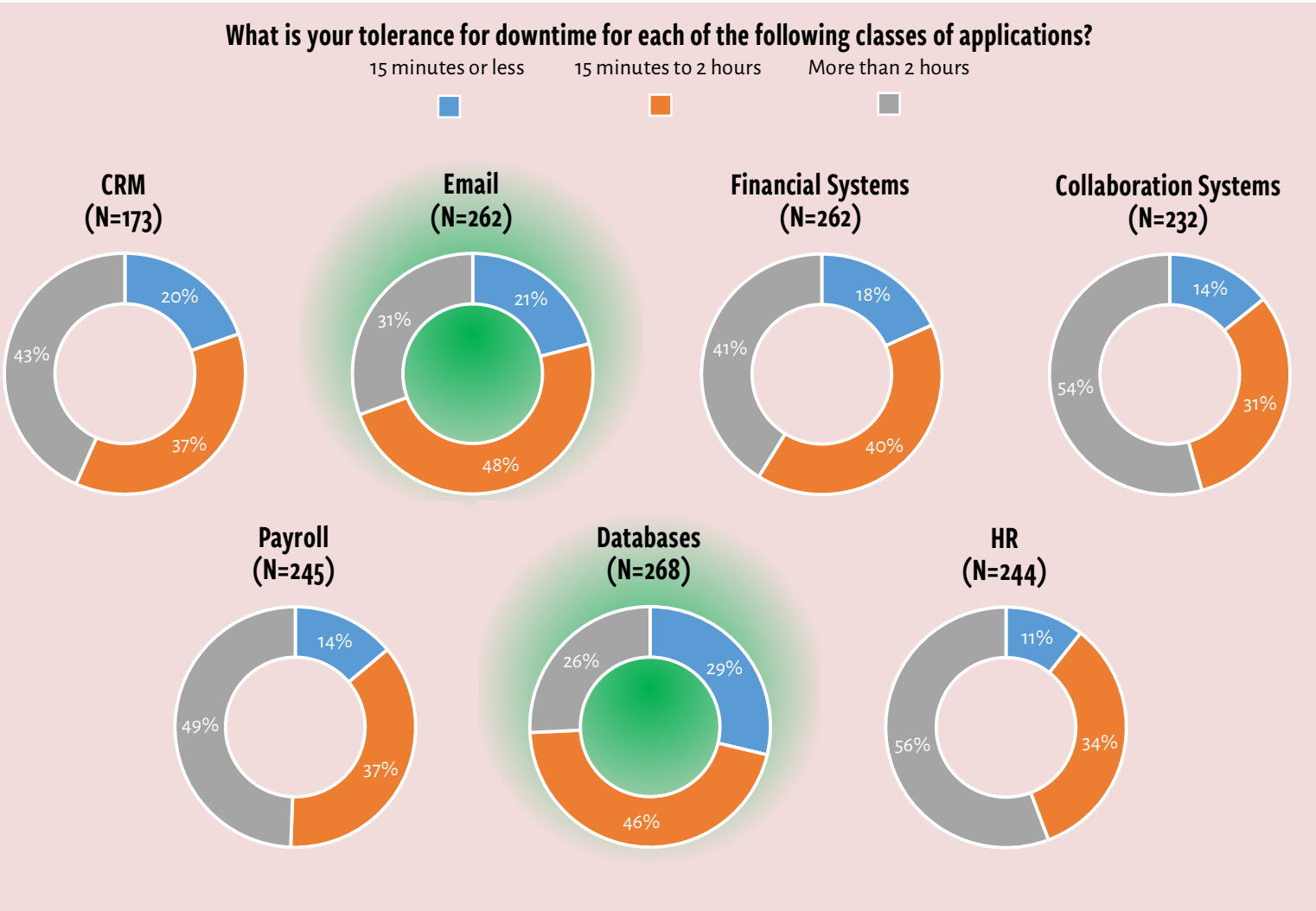


Figure 4: Application criticality breakdown

We want to understand the way that organizations are currently protecting their data. It's no surprise that "tried and true" tape backups – which are stored offsite – remain the most popular method (42%), closely followed by replicating local backups to an offsite appliance (37%).

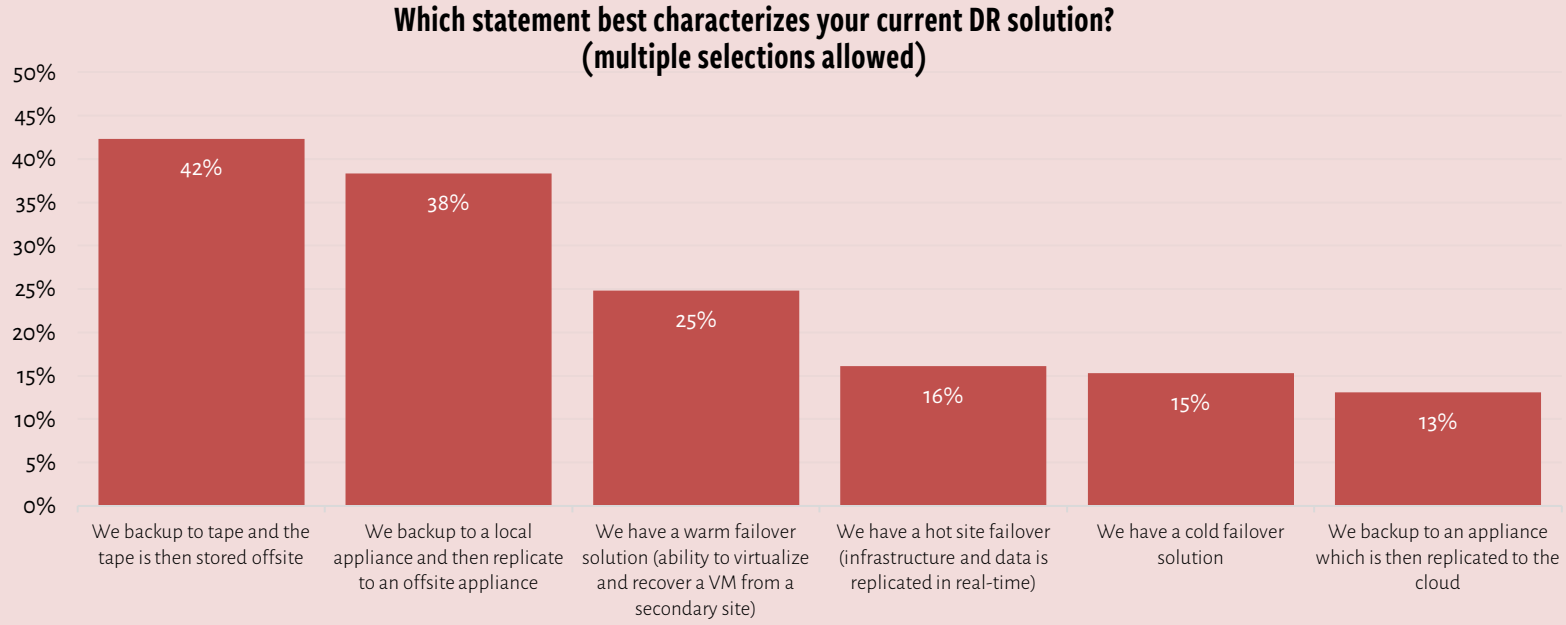


Figure 5: Current disaster recovery solution type

The survey sampling represents businesses from small to quite large in almost equal proportions. Figure 6 shows the breakdown. This data, when viewed in conjunction with the the ability to recover key apps within 15 minutes, suggests that larger companies are generally better able to perform quick recovery, although this is not necessarily a universal truth.

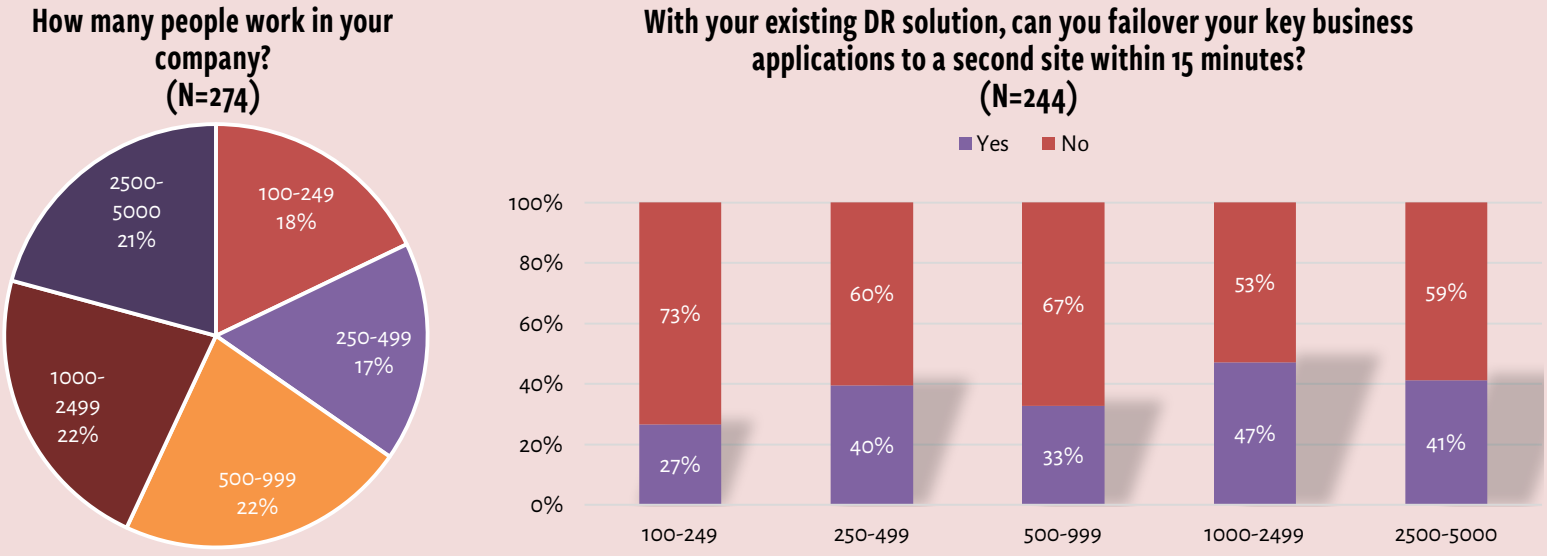


Figure 6: Company size breakdown and ability to recover key business applications within 15 minutes

Different kinds of companies have different needs and requirements when it comes to failing over critical business applications. In Figure 7, you can see that certain verticals are more prepared than others when it comes to the ability to recover key business applications within 15 minutes. Those that provide services to others – VARs and MSPs – seem to be the best prepared, with 57% of respondents in that vertical indicating their ability to recover within 15 minutes. Coming in second and third places are government and financial institutions, with 53% and 47%, respectively. From there, things get a little less positive, with all other verticals falling below the 40% mark.

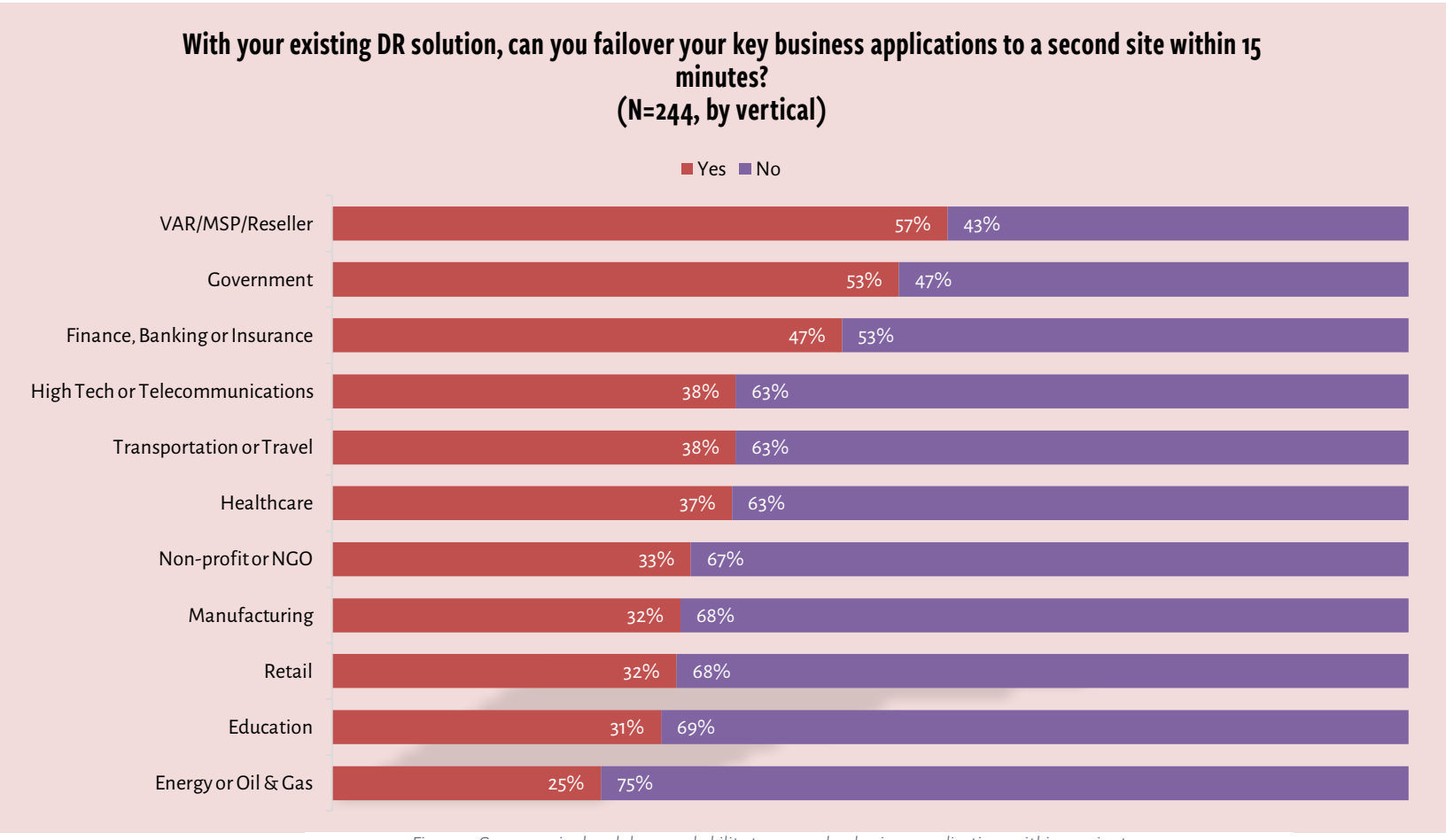


Figure 7: Company size breakdown and ability to recover key business applications within 15 minutes

Since the scope of data center systems under management affects decisions regarding disaster recovery, and since the size of a company from an employee perspective doesn't correlate to the number and scale of applications requiring protection, we asked respondents about the systems that run their business applications.

As you can see in Figure 8, there are far more virtual servers used in respondent organizations than there are physical servers. This makes sense; after all, a single physical server can run dozens of virtual machines.

It's important to understand this breakdown since disaster recovery processes are often challenged for those running a lot of physical servers.

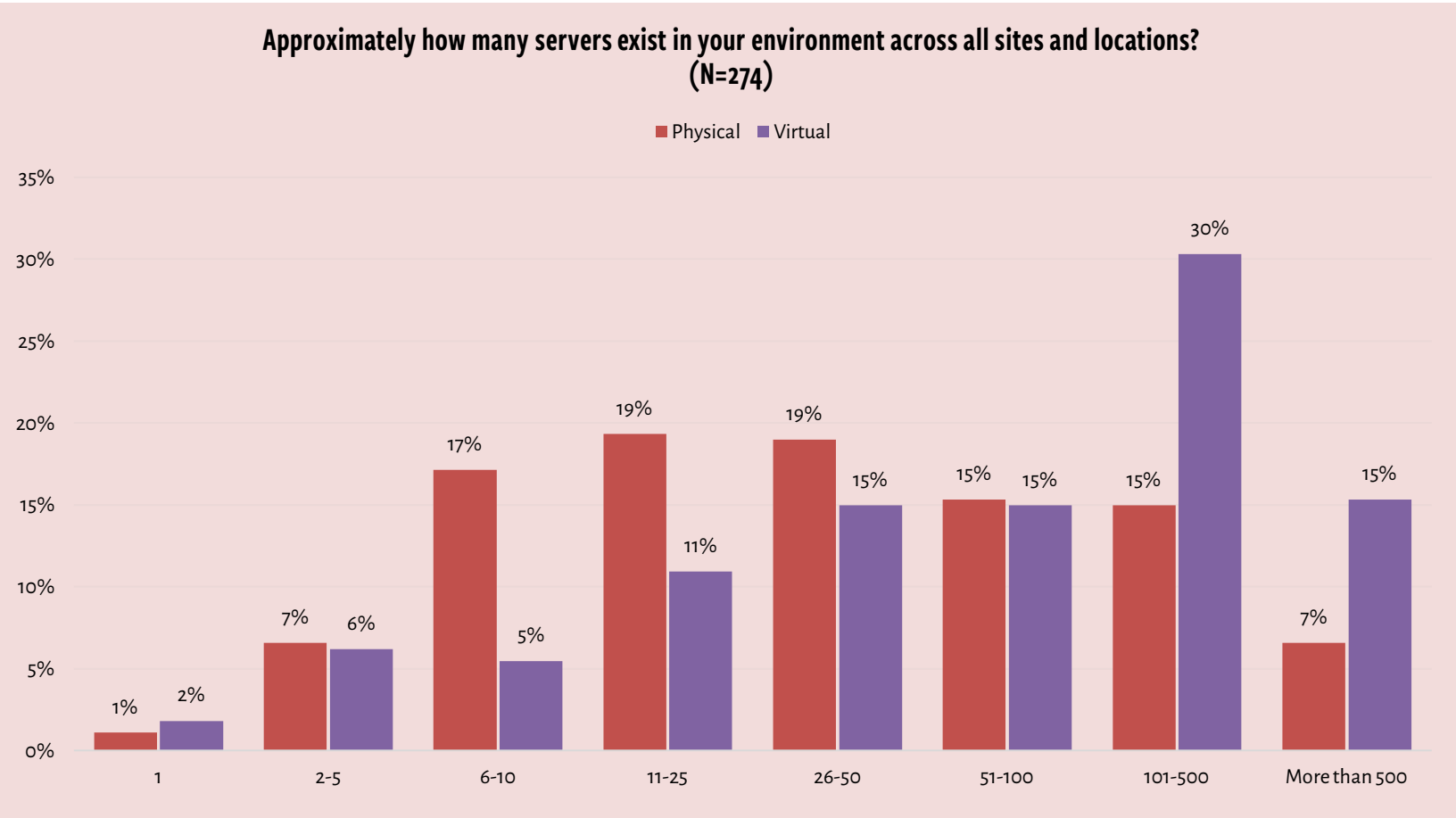


Figure 8: Number of physical and virtual servers under management

Although companies of all sizes need to protect data, it's interesting to understand the amount of data that organizations need to protect. In Figure 9, you can see that 54% of respondents are managing less than 50 TB of data. Interestingly, this is a 16% decrease from the 2015 survey, meaning that the amount of data under management in the organizations surveyed has *grown substantially* over the last year.

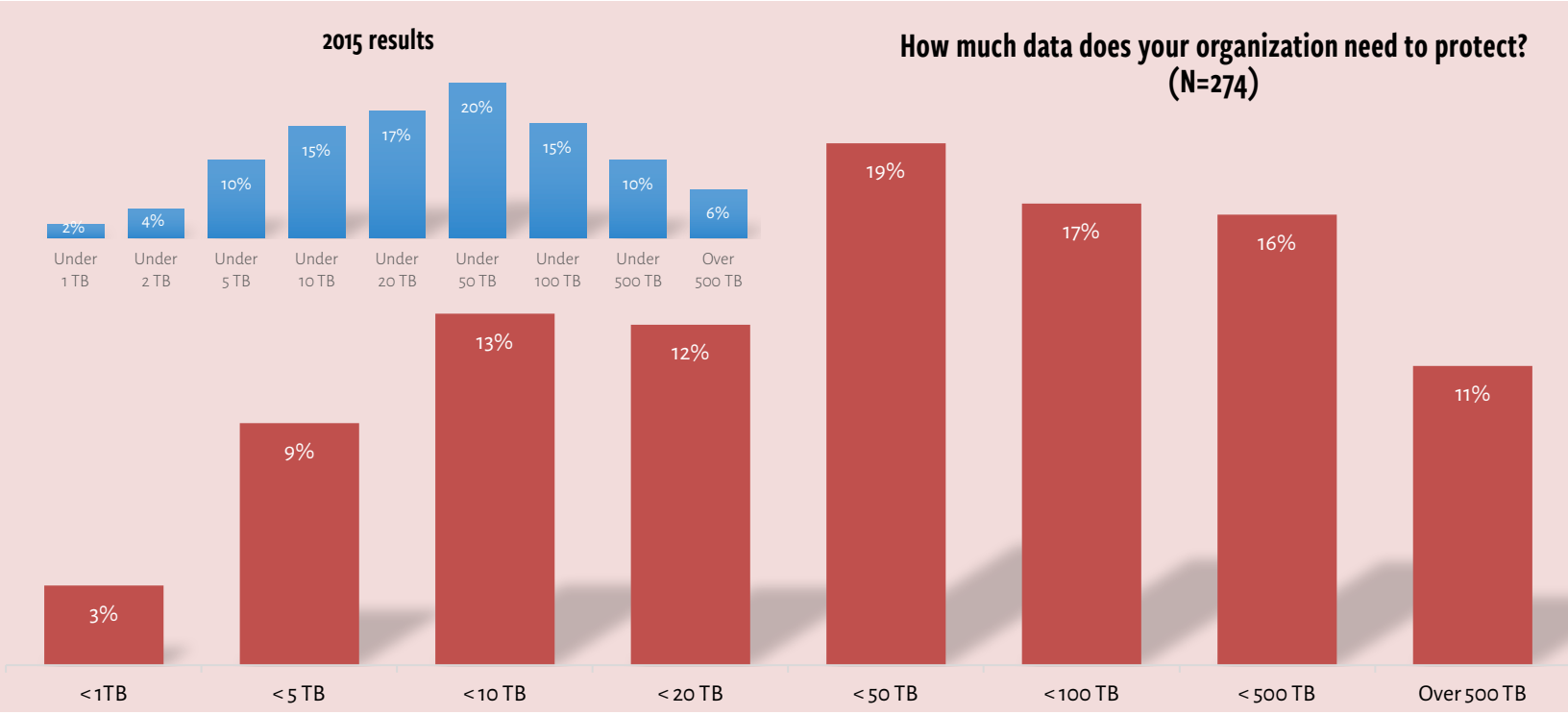


Figure 9: Amount of data that needs to be protected

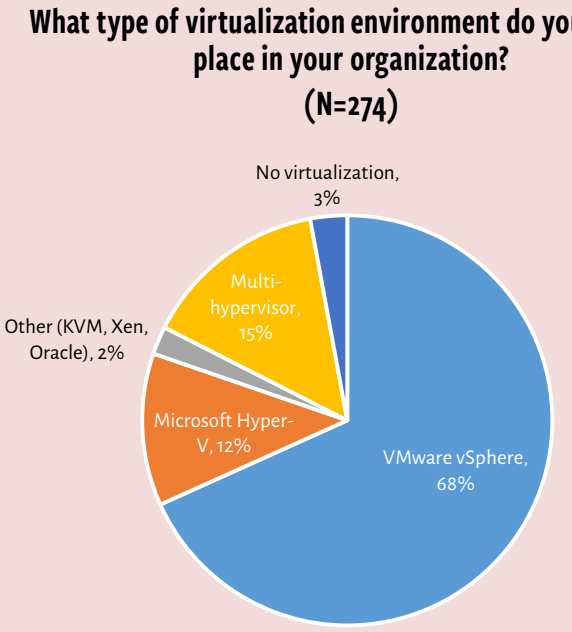


Figure 10: Hypervisors in use

The vast majority of businesses do virtualize some or all of their applications, though the overall percentage of virtualized workloads varies from company to company. This variation in virtualization penetration — from 0% virtual to all virtual all the time — means that customers need disaster recovery solutions that can support a wide breadth of virtual and physical systems and that can support the operating systems and applications that run inside those environments. It's no surprise that, for those who virtualize workloads, VMware vSphere is the clear market leader. It is notable, however, that a full 14% of respondents are operating a multi-hypervisor data center today.

Understanding Peer Disaster Recovery Capabilities

Everyone wants to be able to edge out the competition in some way and, believe it or not, disaster recovery capabilities are important enough that they can become a strategic differentiator. After all, if you and your biggest competitor both suffer disasters at the exact same time, but you can recover in 15 minutes, while it takes your competitor 48 hours, the advantage to you is clear.

So, where do you fall when it comes to disaster recovery? We asked respondents a series of questions in order to gauge their current status.

There are multiple services that need to be protected in the data center and, traditionally, companies have had to prioritize which services deserved protection. Disaster recovery for all services was considered too expensive or too complex. However, failover services — a step short from full disaster recovery — have started to become more commonplace as some of these kinds of services are built into the hypervisor and as myriad failover solutions have come on the market in recent years.

Results of our survey support these observations. As shown in Figure 11, more than half of respondents have some capability to survive a disaster by failing over to an alternate resource or facility. While this is good, it also means that a disturbing 45% of respondents will be left in a less desirable position and will to resort to arcane procedures, such as manually restoring from backups

Do you have a failover solution that can protect your organization from an event such as a server failure or natural disaster? (N=274)

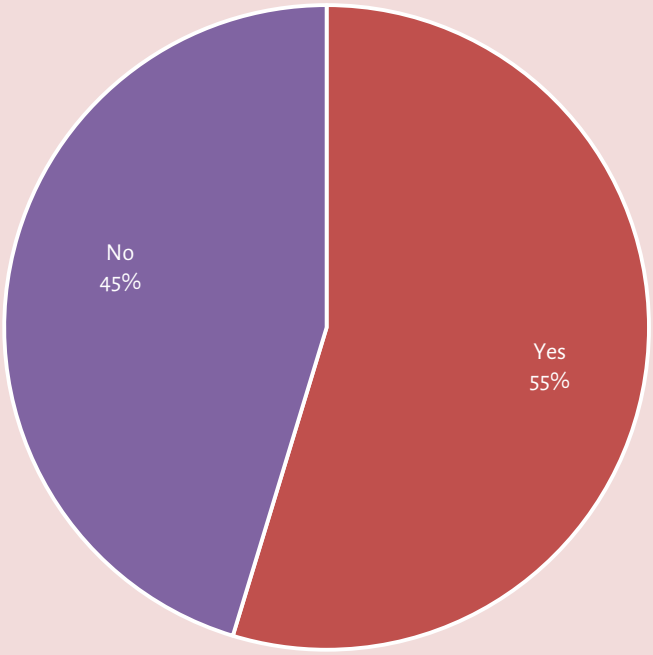


Figure 11: Understanding failover capabilities

The data shown in Figure 11 is useful for understanding the general preparedness of respondents, but the degree to which they're actually prepared is widely variable. To further clarify the exact capabilities respondents have with regard to failover, we asked them to describe their response to a failure, specifically with regard to RTO.

Figure 12 shows that of the respondents who said they had some level of failover capability, only 49% have a 15-minute RTO, and only a meager 18% of those are able to get all of their applications back online within that 15 minute window. This suggests that even among respondents with some failover capability, there's substantial room for improvement in both the number of applications that can be failed over and the speed with which all protected applications can be recovered.

If a server crashes or there is a site-wide failure, which of following answers best describes your DR response? (N=143)

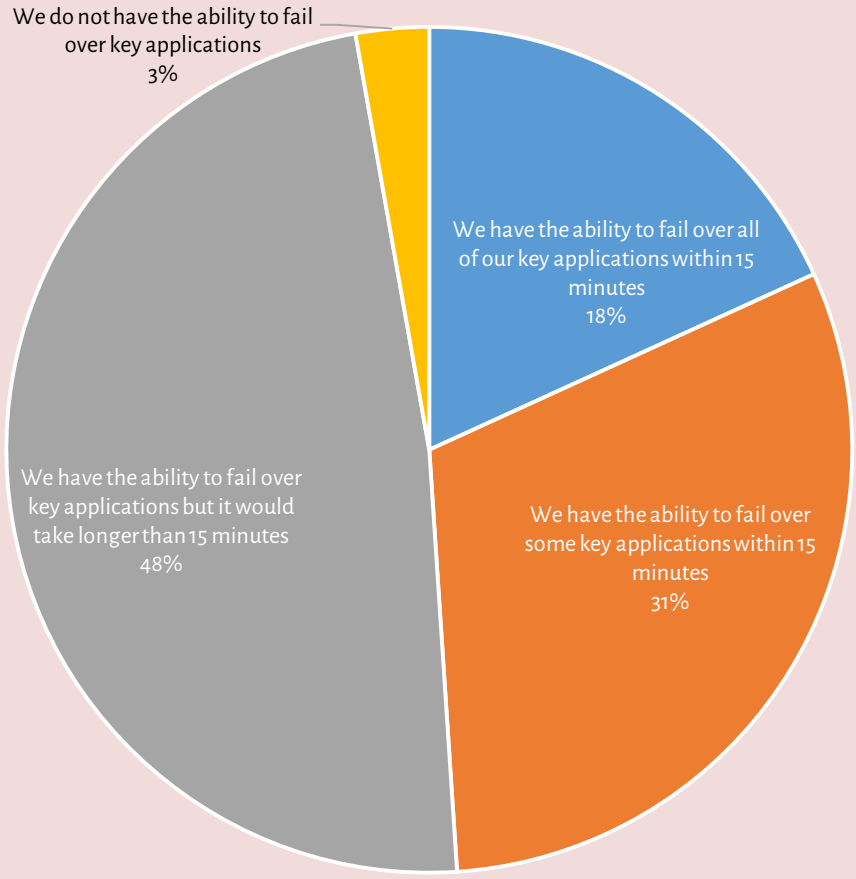


Figure 12: Failover capabilities with regard to RTO

As mentioned earlier in this report, disaster recovery is often neglected and two of the common reasons are cost and complexity. With all of the potential business benefits of an on-demand failover solution, we sought to understand exactly what it is that keeps companies from implementing one. As expected, cost is the primary factor (Figure 13). Interestingly, however, the second most common reason cited for not having an on-demand failover solution is that it just hasn't been a priority. This lends substantial credence to the thesis presented in the introduction that the *urgency* of quality disaster recovery capabilities is just lost on some organizations.

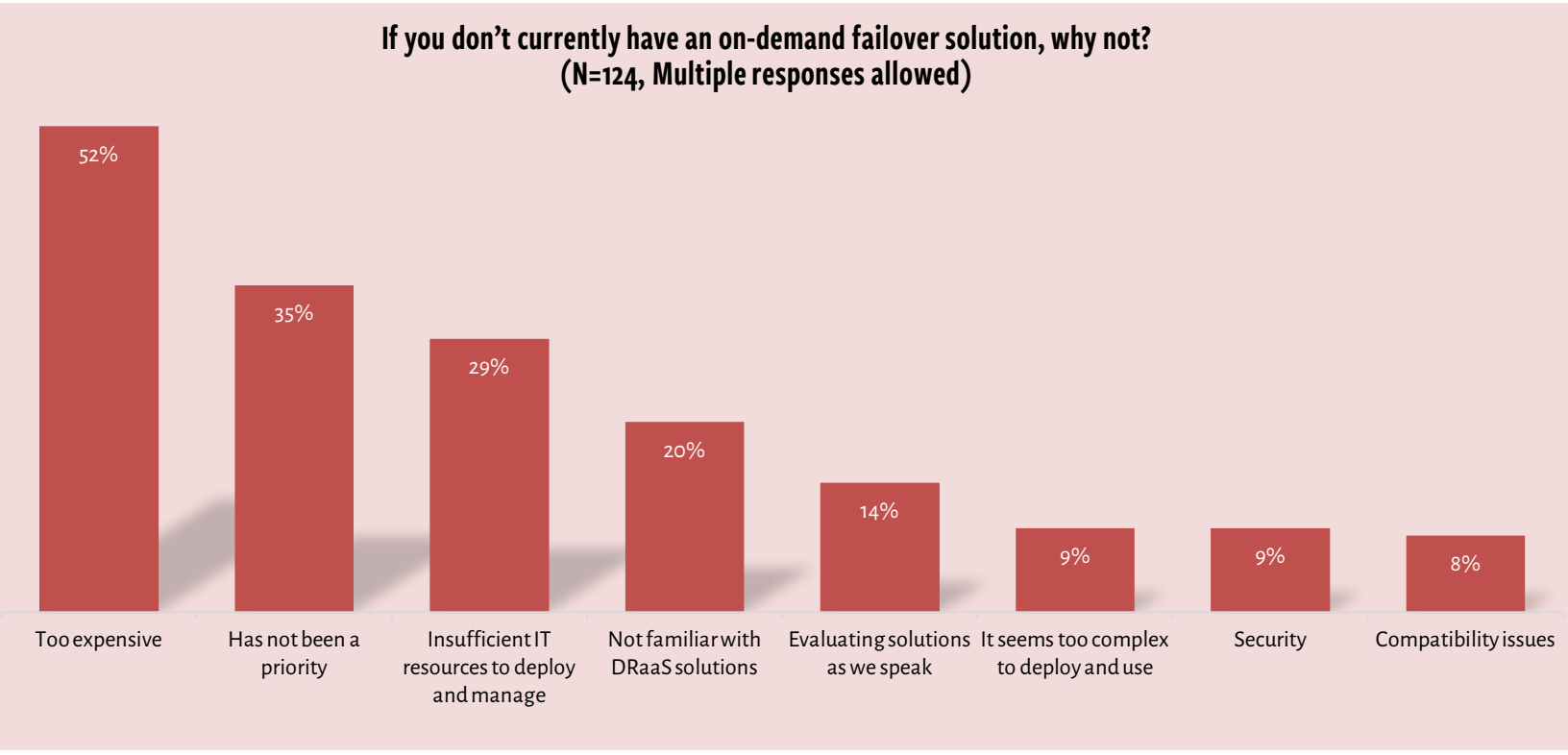


Figure 13: Reasons for lack of on-demand failover capability

Disaster Recovery Testing Processes

We know that DR plans often get tested less frequently than would be ideal, and in some cases they don't even get tested at all. In order to find out just how bad the problem is, we asked our respondents how frequently they actually test their DR plan (Figure 14). We found that 11% of respondents say that they have never tested their DR plan, and 11% more say that they test less often than once per year.

How often do you actually test your DR plan? (N=220)

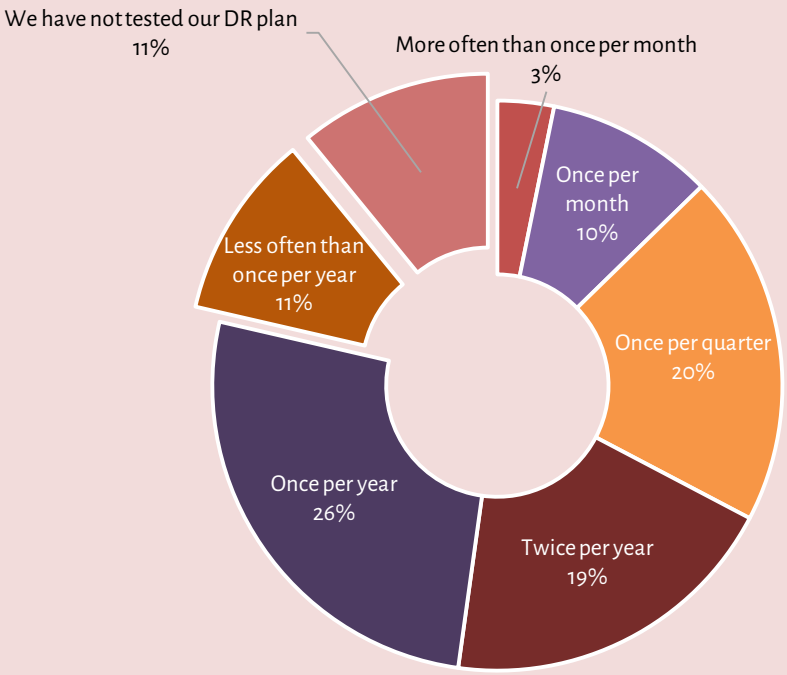


Figure 14: Disaster recovery testing frequency

Does your DR vendor charge you to perform DR tests? (N=274)

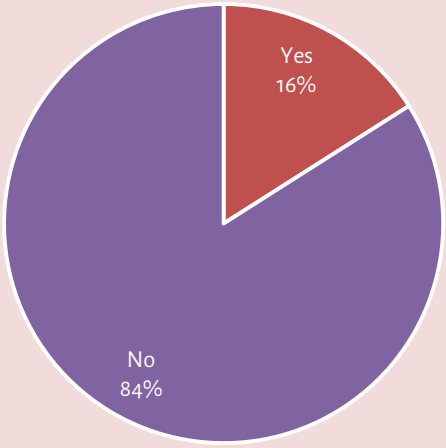


Figure 15: Cost associated with performing DR tests?

We also know that one reason businesses elect to test their DR plan less often is because of the cost of testing. So, we also asked respondents if their current DR vendor charges them to perform DR testing (Figure 15) – 16% of respondents have to pay to test their DR plan.

Outage Handling Experiences

Even the best-designed data center experiences outages. It's an unavoidable certainty. What matters is not whether it will happen, but how it is handled when it does happen. How commonly a company experiences outages and how quick the IT staff are able to recover from the situation can directly correlate to overall profitability of the business. Downtime is like washing money down the drain. To get a better understanding of exactly what outages cost respondents, we asked them to quantify the amount of money their business loses during every hour of downtime (Figure 16). The responses tell us two things:

- 37% of respondents can't even speculate what an outage costs their business. On the harmless side, this could just be due to the respondent's position in their organization. On the more dangerous side, however, is the possibility that the respondents who are decision makers aren't even aware of their risk in the event of an outage.
- Of those who are able to calculate their financial exposure, 44% of respondents' businesses *lose more than $10,000 every hour that an outage continues*. **This means that a single multi-hour outage could conceivably cost more than a reliable, on-demand failover solution**.
- Larger companies experience *far more downtime cost* than smaller companies.

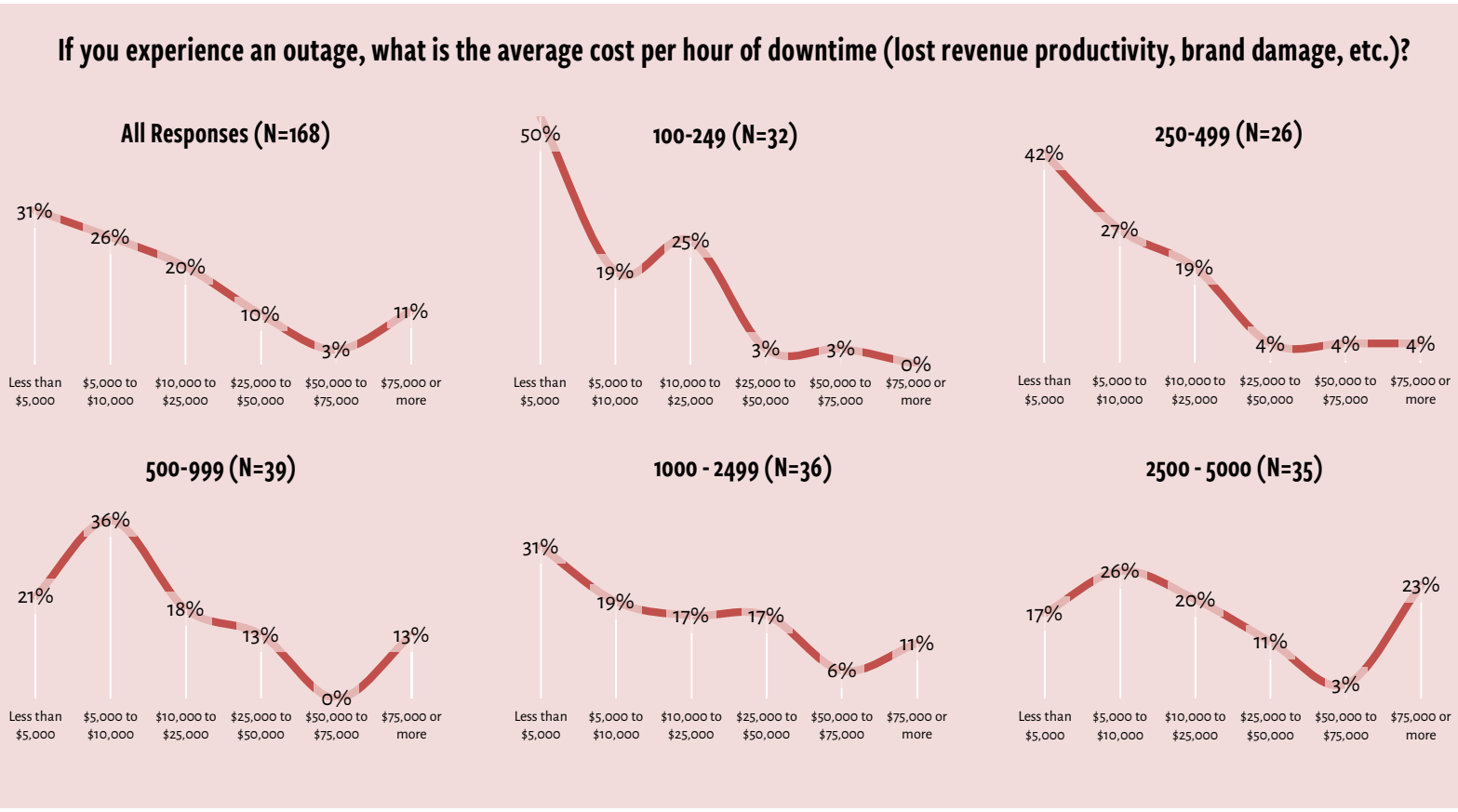
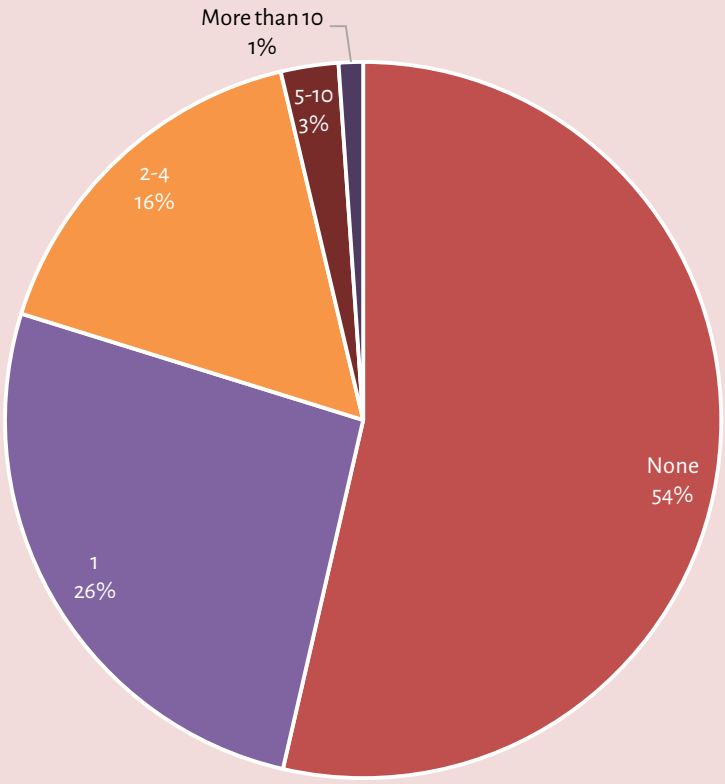


Figure 16: Average cost per hour of downtime

In light of this, we sought to understand how frequently respondents are experiencing outages. Figure 17 shows that 54% of respondents either didn't experience any critical outages in the past 6 months or are not sure. The other 46% did experience some sort of disruption to a vital part of their business.

Figure 17 also shows that 20% of respondents report experiencing more than a single outage in the past 6 months. In the context of Figure 16, this reinforces the idea that many companies may be throwing away money by not investing in an on-demand failover solution to protect them.



Over the last 6 months, how many critical application outages has your company experienced?

Figure 17: Outages experienced in the past six months

When an outage occurs, there are two recovery time metrics in play.

- How long the runbook says it should take to recover (Figure 18)
- How long it actually takes to recover (Figure 19)

To get a sense of what the ongoing reality is in the experience of our respondents, we asked about both. We found some good news here in that respondents are actually able to recover faster than their projections in many cases. The bad news, however, is that 68% of respondents are not able to achieve an actual RTO of 15 minutes or less. Since all downtime translates to a loss of profits in some form, recovery times measured in hours and days are scary.

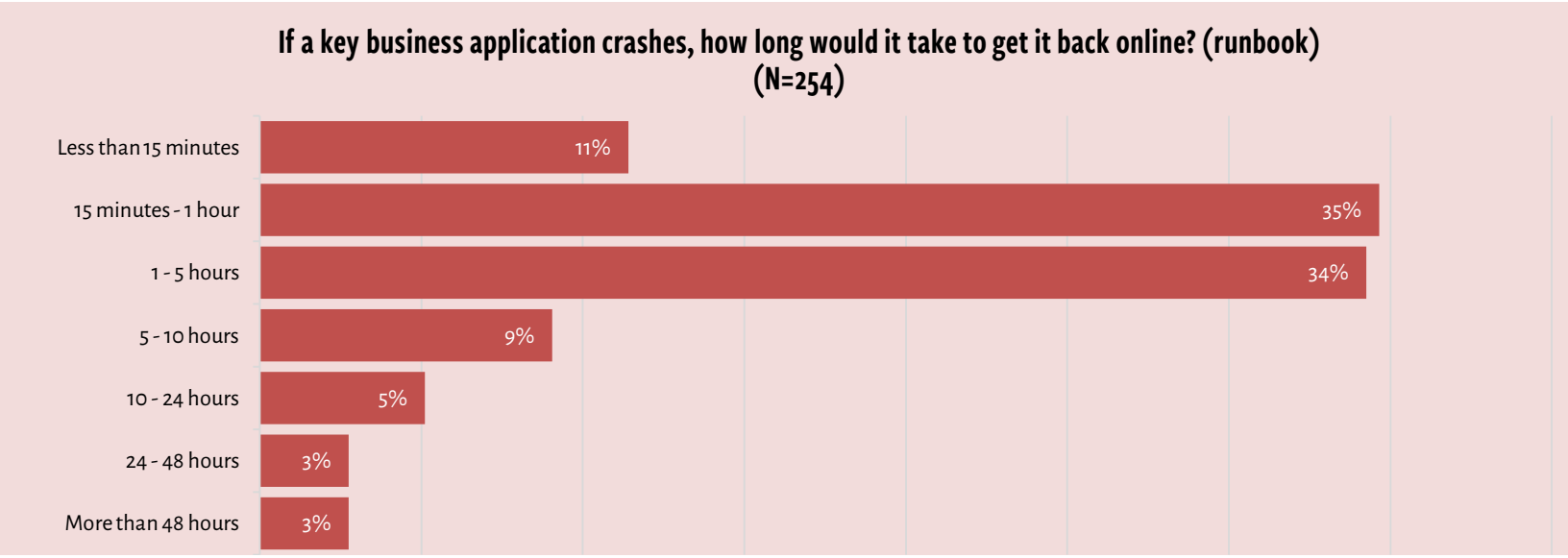


Figure 18: Time to restore a key business application

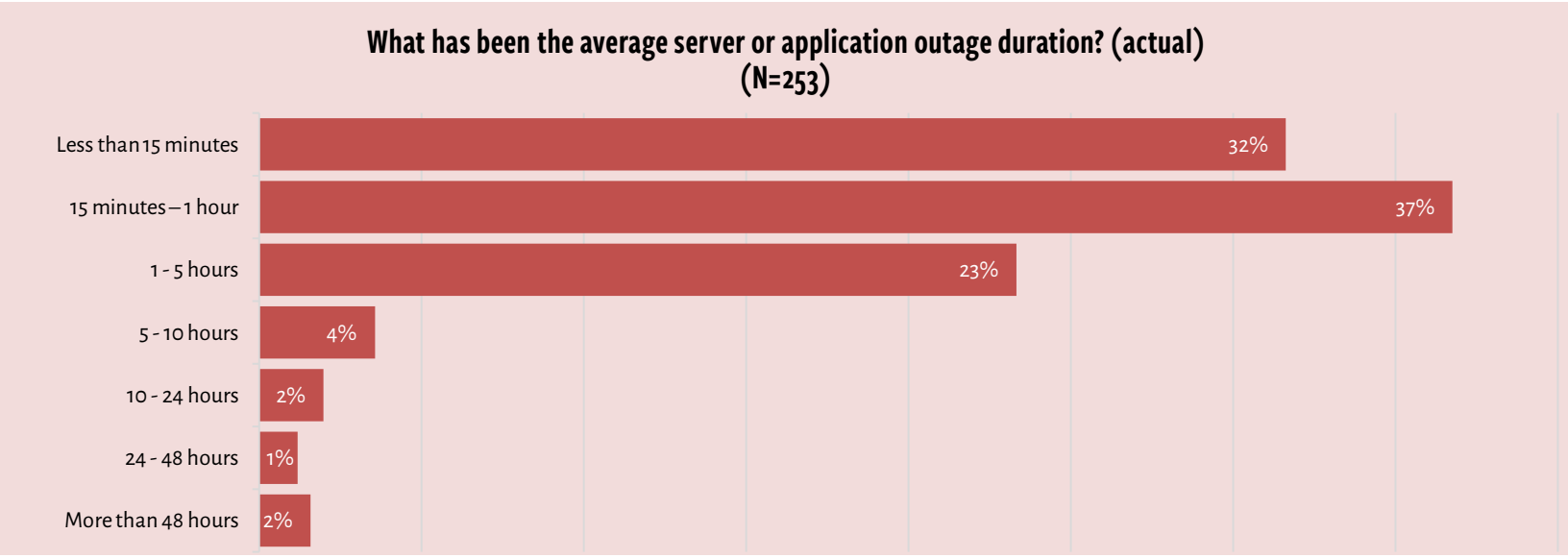


Figure 19: Average duration of past outages

Recovery options vary greatly depending on the disaster recovery solution that is in use and the type of disaster that has occurred. We wanted to know what respondents prefer in terms of the platform for their recovery. As you can see in Figure 20, most respondents are most comfortable recovering the workload to their existing DR site. However, 26% prefer to recover into a cloud infrastructure and 24% would like to boot the workload on the local backup appliance.

Where would you prefer to boot critical applications in the event of a server failure? (N=269)

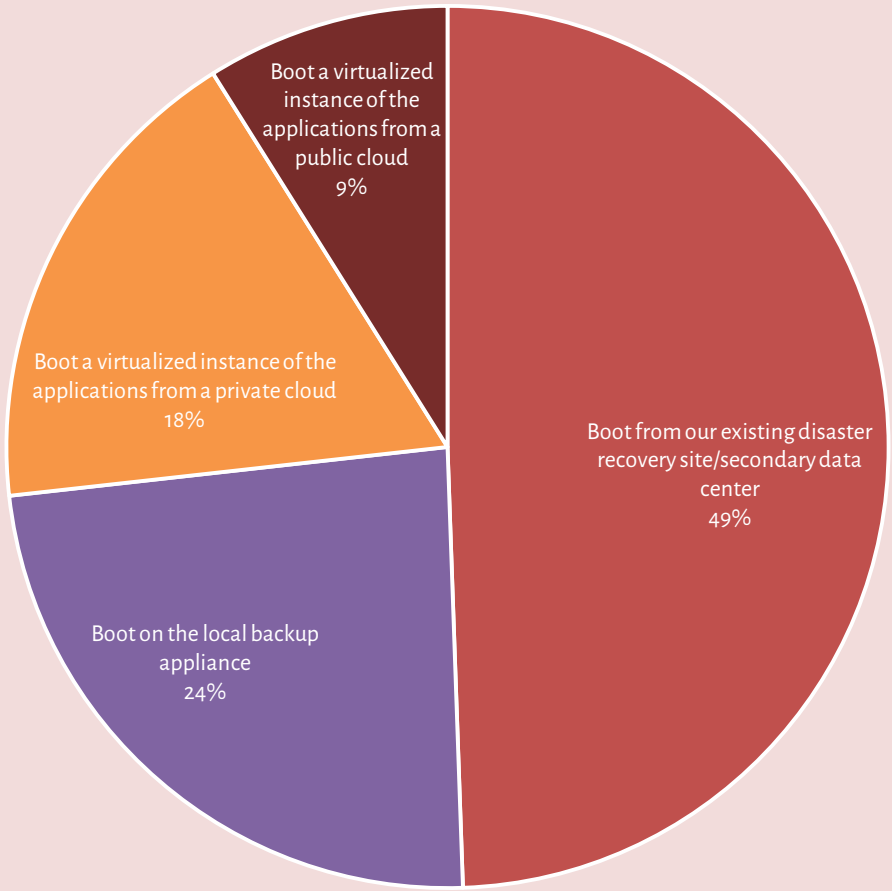


Figure 20: Preferred boot location for recovered workloads

Purchase Intent for Disaster Recovery as a Service

A whopping 46% of respondents indicated that disaster recovery is a top priority for their organization in 2016. In many cases, this will mean a capital purchase. So besides asking how they are prioritizing DR, we asked specifically whether they were evaluating on-demand failover solutions to meet their DR needs. You'll see in Figure 21 that a full 37% are either already using a DRaaS solution or do plan to deploy one. Of those who plan to deploy one, however, 20% of them are still more than 6 months away from deployment.

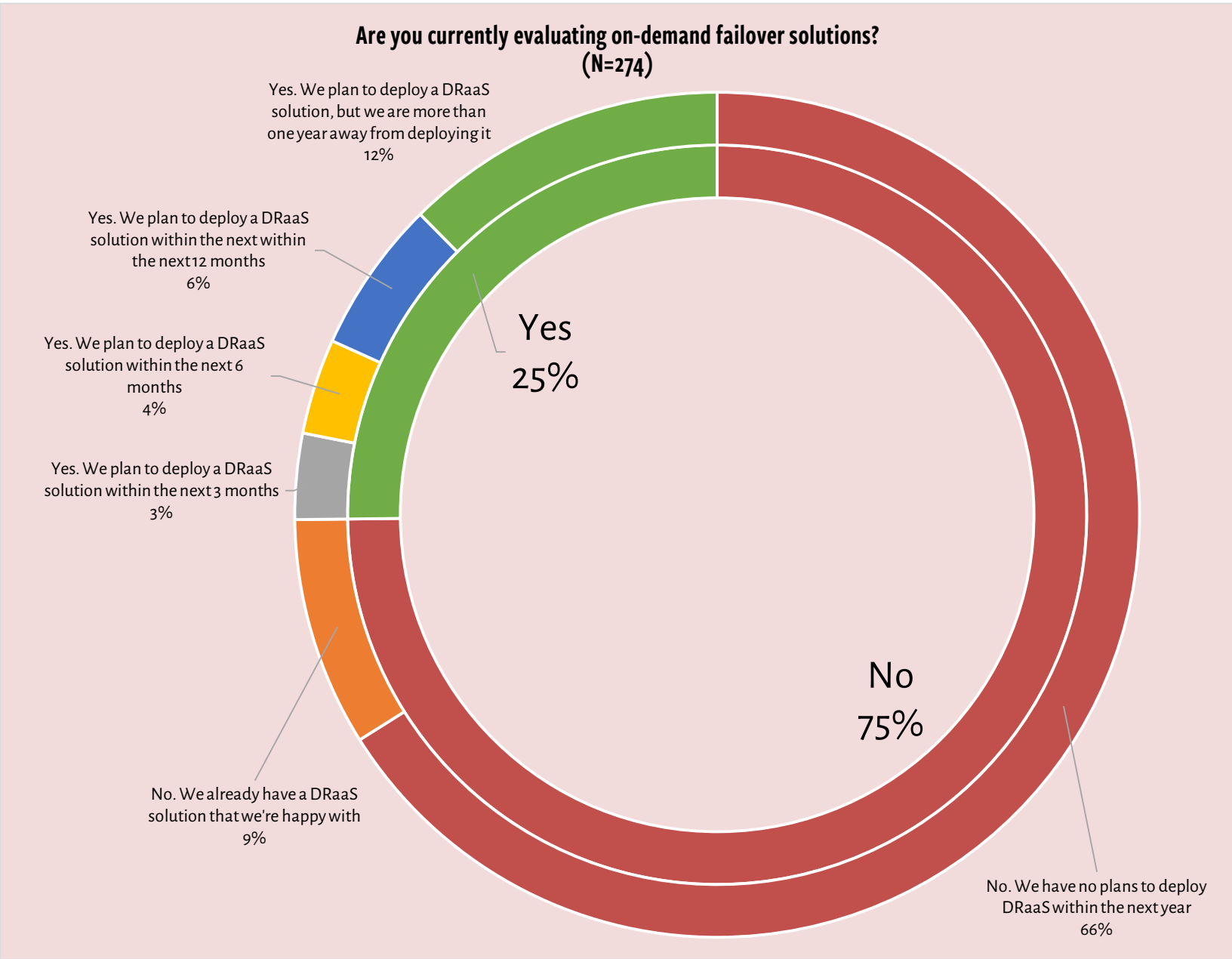


Figure 21: Intent to deploy DRaaS

We asked all respondents – even those not currently in the buying process – which criteria are most important to them when evaluating on-demand failover solutions. Unsurprisingly, the overwhelming leader is cost, as you can see in Figure 22. Reliability, security, and compatibility with existing infrastructure are also ranked highly.

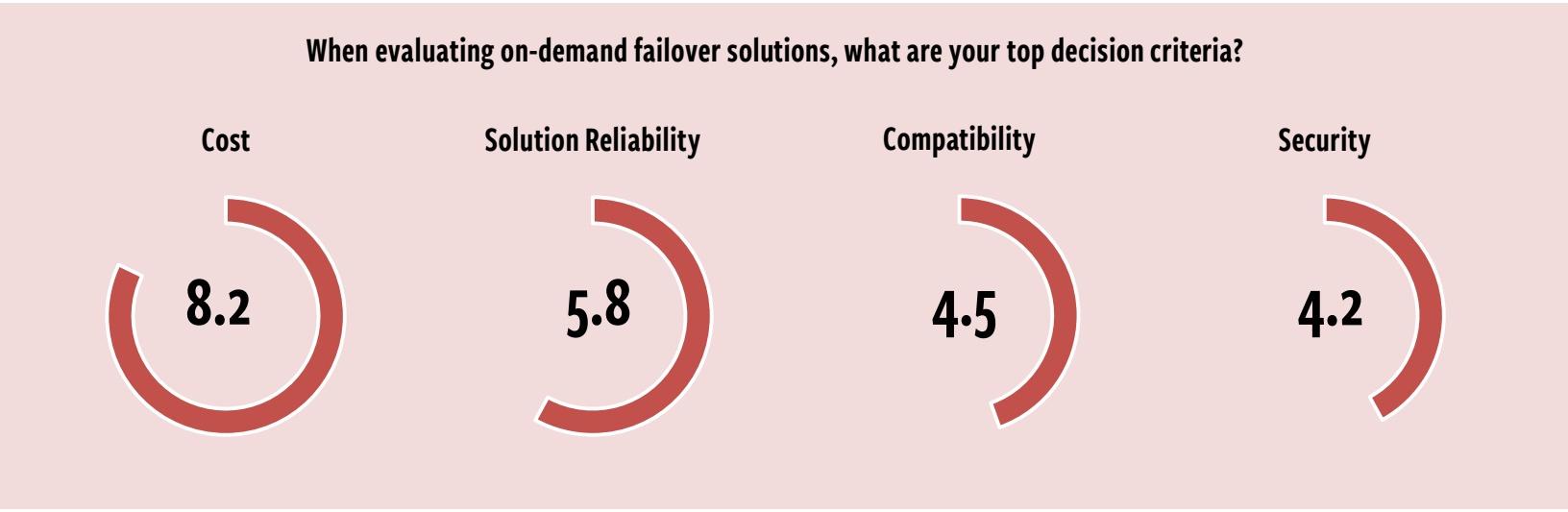


Figure 22: Top evaluation criteria for on-demand failover solutions

About

About Infrascale

Infrascale is a provider of the most powerful disaster recovery solution in the world. Founded in 2006, the company aims to give every company the ability to recover from a disaster – quickly, easily and affordably. Combining intelligent software with the power of the cloud is how Infrascale cracks the disaster recovery cost barrier without complex, expensive hardware, enabling any company to restore operations in less than 15 minutes with a push of a button. Infrascale equips business with the confidence to handle the unexpected by providing less downtime, greater security, and always-on availability.

About ActualTech Media

ActualTech Media delivers authoritative content services and assets for top IT companies across the globe. Leading IT industry influencers Scott D. Lowe, David M. Davis, James Green and partners develop trusted, third-party content designed to educate, convince and convert IT buyers. ActualTech Media helps its clients reach the right technical and business audiences with content that resonates and leads to results.