5 Disaster Disconnects: Survey Shows Partners Must Educate Customers on BC/DR

By Eyvonne Sharp

OCTOBER 2017 | US$25 | S351017

Channel Partners™

5 Disaster Disconnects: Survey Shows Partners Must Educate Customers on BC/DR

By Eyvonne Sharp

OCTOBER 2017 | US$25 | S351017

Channel Partners™

Table of Contents

Channel Partners™

About the Author

EYVONNE SHARP is a network architect for a Fortune 100 health care enterprise. She's a co-founder of Network Collective, a biweekly video roundtable and podcast where network engineers talk about industry trends, challenging projects, and what it takes to do network engineering day-to-day. Before working in the enterprise, she spent 10 years working for small VARs and integrators in the SMB space.

linkedin.com/in/eyvonne-sharp/
@sharpnetwork

5 Disaster Disconnects: Survey Shows Partners Must Educate Customers on BC/DR

Talk about a DR divide: We surveyed channel partners and IT pros about the state of business continuity and disaster recovery strategies, from connectivity to security to RTO/RPO. The fact is, partners can deliver good recoverability, across all locations, for less money. Are your customers taking advantage?

Key Findings

- **About half, 52%**, of IT pros say they have effective BC/DR programs. Channel pros disagree, with most saying fewer than half of their customers have effective plans. That puts the channel slightly more pessimistic, but no matter how you slice it, only half of respondents think they could recover.
- **For IT**, the belief they can't get the right connectivity was the No. 2 reason for a lack of a strategy. Just 13% of channel pros cite a lack of connectivity, indicating that we're not educating customers on options like satellite and SD-WAN.
- **Ransomware** is cited by channel pros as the top BC/DR driver, followed by connectivity failure. For IT pros, connectivity failure is No. 1, with ransomware in fourth place.
- **59% of IT pros** say it's somewhat or very difficult to provide adequate connectivity at an affordable cost to remote sites to achieve BC/DR objectives; 39% of channel pros say the same.
- **Half of channel pros** expect BC/DR budgets to increase somewhat. IT pros? 61% say spending will stay level, while 29% expect increases. The good news: Few see spend decreasing.

Other observations: Encryption use is spotty, leadership buy-in is hard to come by and critical data has been lost.

"It won't happen to us" is a familiar refrain for partners. When it comes to preparing for disaster, customers who have yet to experience a business-impacting disruption fail to prioritize business continuity planning. As trusted advisers, partners need to deliver a reality check: You've seen major business disruptions firsthand and helped cope with the data loss, productivity and reputation hit, and hard financial costs incurred when an organization fails to properly plan for extended downtime.

How can you help customers understand the risks and be more prepared when disaster strikes?

We decided to survey the state of disaster preparedness from the perspective of both IT professionals involved in their companies' business continuity/disaster recovery strategies and channel partners who sell and/or manage BC/DR services, technologies and connectivity, hoping to uncover the disconnects that are putting customers at risk.

Among 138 total respondents, we excluded 43 who were either not well qualified or who didn't answer all required questions. The final split: 41 IT pro and 58 channel respondents. Among channel pros, the largest groups were MSPs (44 percent) followed by consultants, agents and master agents (find the full demographic breakdown here).

We started with the premise that today's technologies and connectivity options can deliver better and faster recoverability, across all locations, for less money than even just a few years ago. Are your customers taking advantage?

Survey says: Maybe not.

Among IT pro respondents, more than half say their companies lack effective BC/DR plans. Of those respondents, the No. 1 reason cited for the lack of an actionable strategy is no urgency from the business. Think about that: Nearly half of respondents do not have a valid plan to maintain operations. Worse, they don't have a mandate from leadership to address the problem.

In short, your IT pro customers know they need to do better. They've felt the scramble when circuits fail, when cloud applications are unreachable, when email is not accessible. But they're struggling to receive buy-in.

"We're a mess, but leaders figure it can't happen to us," said one respondent. Our survey results indicate this IT pro is far from alone. How is that possible given wall-to-wall coverage of natural disasters, ransomware, malicious insiders and other mayhem?

Rose-Colored Glasses, Circa 2017

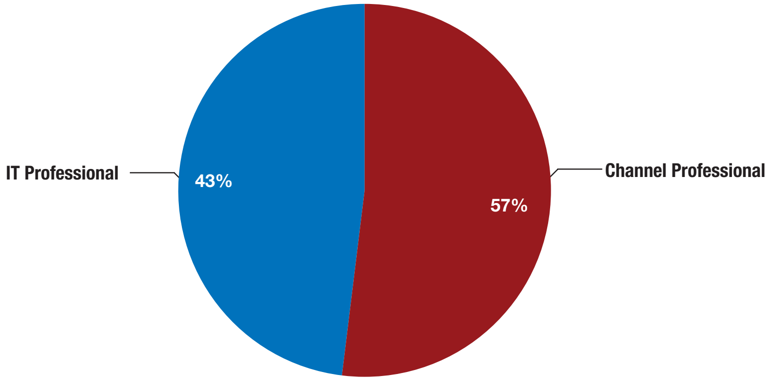
To understand how executives make decisions, and how you can help them understand that, yes, it can happen to them, we must look beyond purely technical drivers. Leading psychologists and neuroscientists have identified a phenomenon in human decision-making called "optimism bias." Simply described, people are wired for hopefulness. They both overestimate positive outcomes and underestimate negative ones. In our context, customers will magnify their ability to complete a project within the desired timeframe, while downplaying the risk that they will incur a catastrophic event.

Hence, the business will be inclined to over-invest in future-state technology and under-invest in core (read: not sexy) solutions.

Aside from tinkering with evolutionary brain development, what can trusted advisers do to protect customers from themselves?

One proven method to counteract optimism bias is to connect individuals with relatable peers who have effectively — or ineffectively — managed disaster situations. The more relatable the situation, and the more we can personalize peer experiences, the more effectively business leaders will accept the need for disaster recovery

What best describes you?



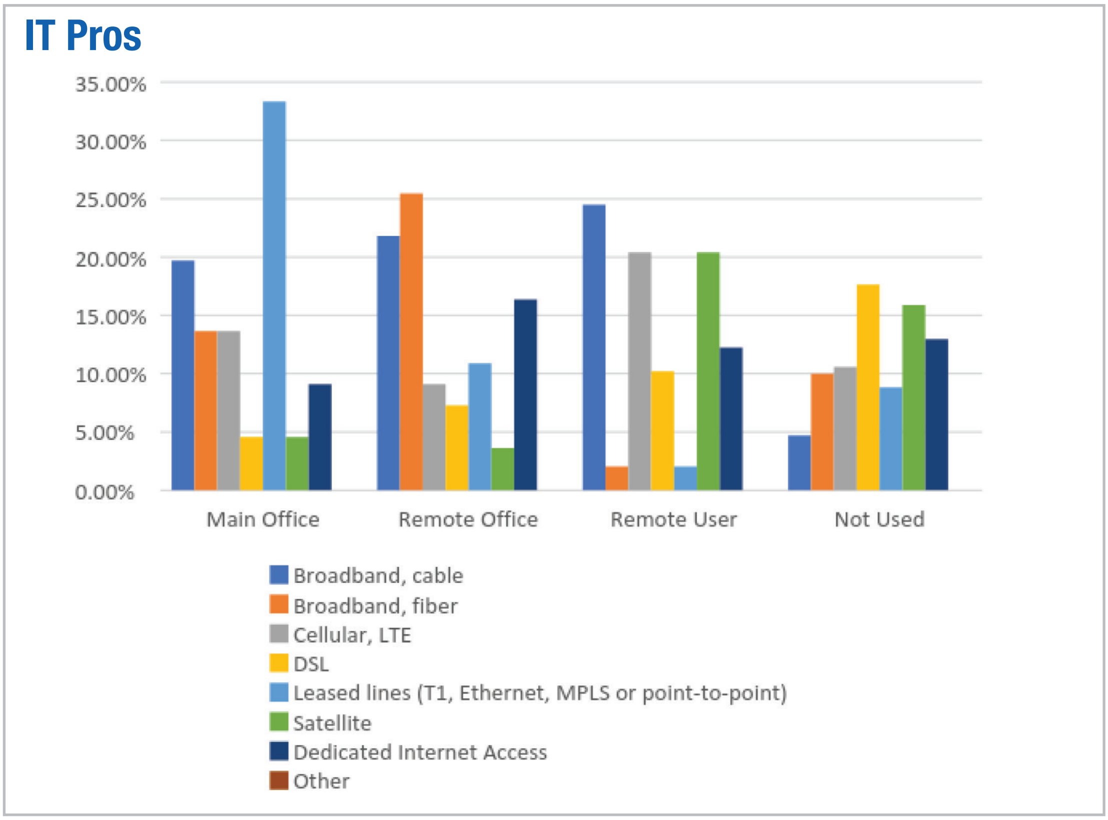
Source: Channel Partners BC/DR Survey, 2017

solutions. This method is most effective when IT leaders can see a direct correlation between their realities and the experience of others. For example, the CEO of a midsize company will be more influenced by a peer business leader of a company of similar size and operating model than a reseller, her own IT staff or a Fortune 500 IT leader.

As a trusted advisor, consider connecting customers, who have been hit by disaster and successfully recovered, with peers who are vulnerable to similar mishaps, but in denial. This could be live, as with a workshop or lunch and learn, or via a published case study. Partners who have a strong vertical specialization have an advantage here.

Get Connected

What other BC/DR inhibitors do IT pros mention? Twenty-five percent of customers said their primary reason for neglecting a BC/DR strategy is a failure to find the right connectivity. In addition, connectivity failure is the No. 1 most significant driver for investing in BC/DR, and fully 59 percent say it's somewhat (32 percent) or very (27 percent) difficult to provide adequate connectivity at an affordable cost to all the sites that need to be protected to achieve BC/DR objectives. Tellingly, 56 percent of IT pros manage the connectivity for your BC/DR plans themselves versus 12 percent enlisting a third-party consultant.



Source: Channel Partners BC/DR Survey, 2017

Among channel partners? Only 13 percent perceive limited connectivity options as a BC/DR inhibitor. To resolve this huge gap, education is in order. Many businesses negotiate connectivity contracts on a three-year cycle. Customers who haven't investigated the connectivity landscape in the last 24 to 36 months are missing a sea change in how organizations large and small think about corporate connectivity.

And, drivers for a connectivity refresh go beyond BC/DR to better support for branch offices and remote employees and new IoT and digital opportunities.

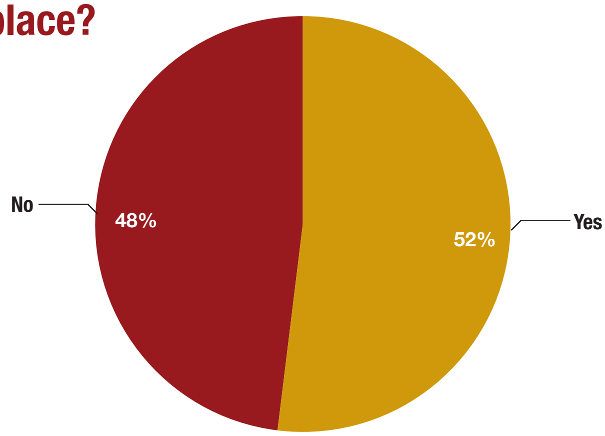
In the past, consumer technologies like cable or fiber lacked the reliability and feature set to meet mission-critical business needs. Organizations were forced to use high-cost leased lines to achieve the uptime and reliability the business demands. Today, high-speed links are more affordable and available in more places than ever. A combination of broadband, 4G/LTE and satellite provide affordable primary and secondary connectivity options for even the most remote sites, which were previously considered too costly to protect with BC/DR.

When asked how much they would be willing to pay for a secondary connection, more than 50 percent of IT respondents answered between $100 and $500 per site per month. Considering most businesses perceive that backup connections must be expensive leased-line services, it's easy to see why they believe adequate connectivity is out of their reach.

When channel partners are asked what connectivity their customers use for BC/DR, their responses are starkly different from IT pros.

IT pros indicate that line services are, by far, the most utilized BC/DR connectivity types in the main office. Channel pros tag satellite, followed by fiber broadband and cable broadband as the most often used secondary connectivity. And, wireless options, both satellite and 4G/5G, continue to make leaps in throughput. It's time to help customers expand their understanding of the connectivity landscape beyond traditional leased-line services.

Do you believe your company has an effective business continuity/disaster recovery (BC/DR) plan in place?



Source: Channel Partners BC/DR Survey, 2017

"Customers no longer have a tolerance for internet outages or loss of connectivity to anything," said one channel respondent. "It's our job to make sure that we've done everything possible to ensure that these systems and services are always available."

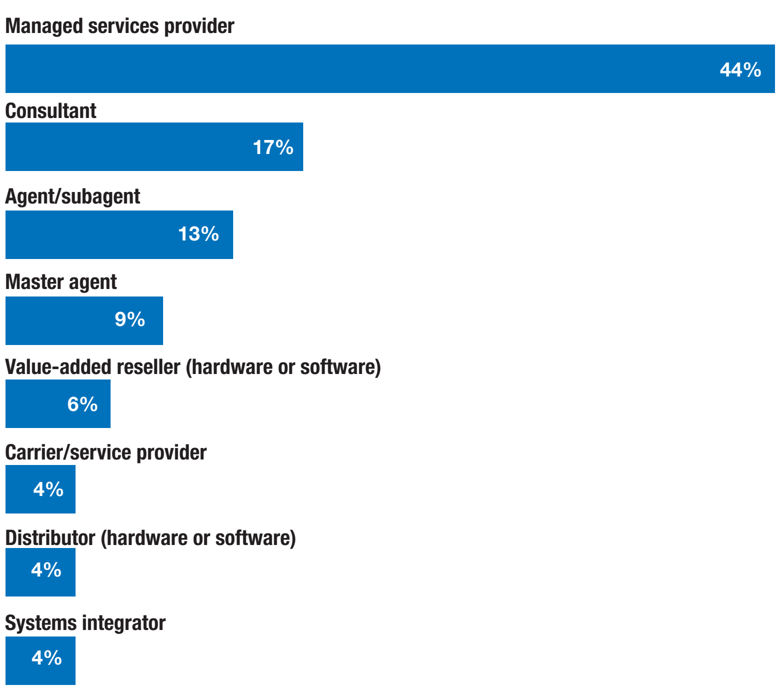
That includes educating customers that, when coupled with SD-WAN technology, any reliable connectivity service becomes a viable option for backup — or even primary — connectivity.

SD-WAN uses intelligent routing, integrated performance monitoring and overlay technologies to unify disparate connectivity types in an easy-to-manage solution. Instead of using a single costly leased-line circuit, organizations have found they can add inexpensive connectivity options that increase bandwidth and provide redundancy in the event their primary circuit fails. In fact, for many use cases, customers have abandoned expensive leased-line services altogether in favor of multiple emerging connectivity services.

SD-WAN solutions can fully utilize multiple available circuits — whether DIA, MPLS, broadband or satellite — and quickly and seamlessly shift traffic off a failed link. SD-WAN is particularly valuable for retail or transient work sites and branch offices, as we discuss in this report.

Our survey shows IT pros are not yet taking advantage of the plethora of connectivity services available to their businesses. Among respondents, just 12 percent incorporate SD-WAN into their BC/DR plans. Again, and likely not coincidentally, 56 percent manage their own recovery plans and may be unaware of new technologies that allow them to cost-effectively utilize those connectivity options.

What best describes your business model?



* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

SD-WAN has recently reached the maturity level to achieve mass deployment. Your customers need to know about this technology, which can achieve better daily operational performance and increase their ability to survive a connectivity failure.

A Cautionary Security Tale

"Customers don't think ransomware can happen to them, they think they're too small or don't have data hackers want," said one channel respondent. "They also don't think they can afford DRaaS or redundant connections. Our answer is, you can't afford not to have them."

Good luck making that case without data.

When IT pros were asked about the most significant drivers for investing in BC/DR solutions, connectivity failure was the primary concern, followed by equipment failure and natural disasters — leaving security threats like malware and ransomware fourth. However, when asked about the leading cause of outages that activated their BC/DR plans, ransomware or other malware was the most-cited cause.

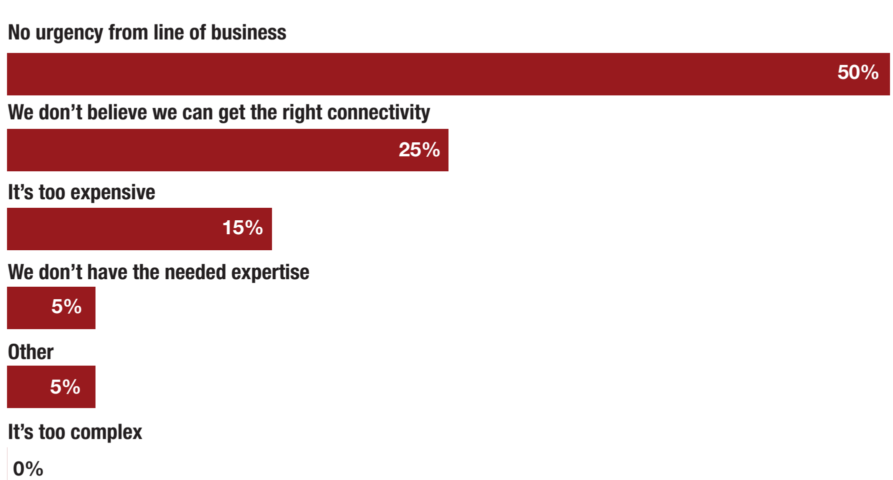
In contrast, partners overwhelmingly recognize the value of disaster recovery in bringing data back from a ransom attack without shelling out bitcoin. They ranked security threats like malware and ransomware as the primary driver for implementing a BC/DR strategy.

Why the disconnect? Again, lack of education. Customers are planning for connectivity and equipment failure, but are executing these plans to recover from security-related failures and human error.

"Selling DRaaS is all about ransomware, ransomware, ransomware with some cut lines/no connection thrown in," said one channel pro.

If connectivity concerns bring customers to the BC/DR party, malware and ransomware are taking them home. Yet, it appears IT pros have not internalized this reality even though there's plenty of data showing the reality of the threat. For

What is the top reason you don't have a BC/DR strategy?



Source: Channel Partners BC/DR Survey, 2017

example, 38 percent of SMB organizations in the second annual Malwarebytes State of Ransomware report experienced a ransomware attack during the last 12 months. For roughly one in six impacted organizations, a ransomware infection caused 25 or more hours of downtime, with some reporting it caused systems to be down for more than 100 hours. Seventy-two percent of respondents believe ransomware demands should never be paid.

News flash: The only way to be sure you can recover data without paying for the encryption key is an isolated backup.

Look, among IT pro respondents, 76 percent think it should take no more than four hours to bring mission-critical applications back online, and 70 percent say it's acceptable to lose no more than two hours of data. When we asked what RTO and RPO metrics customers demand, partners reinforced those expectations. But a survey of 500 cybersecurity decision makers by Vanson Bourne showed it actually takes 33 hours, and just 45 percent were able to get their files decrypted. Most, 67 percent, of our respondents say there been instances where critical customer data was unrecoverable. So again, rosy expectations are unlikely to be fulfilled without a good plan.

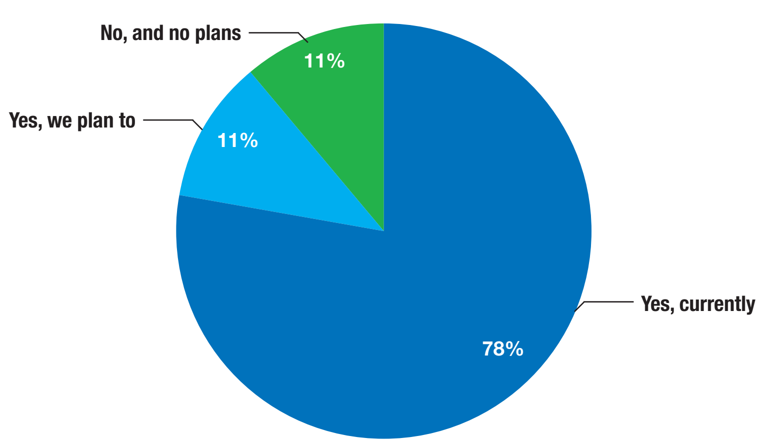
A Look Ahead

As we look forward to 2018, expect businesses to grow more reliant on software as a service. Gartner just forecast an 18.5 percent increase in 2017 cloud spending compared with 2016.

IaaS revenues are expected to grow by close to 37 percent, to $34.7 billion. SaaS will grow more slowly, but still account for more spend: 21 percent growth in 2017 with revenues jumping from $48.2 billion to $58.6 billion.

As core applications shift from on-premises to the cloud, agents are in a good place. Customers will further reduce their reliance on internal IT infrastructure, minimizing challenges around hardware and software life cycle, licensing and maintenance, while demand for reliable, always-on connectivity will continue to increase.

Do you currently or plan to resell DRaaS?

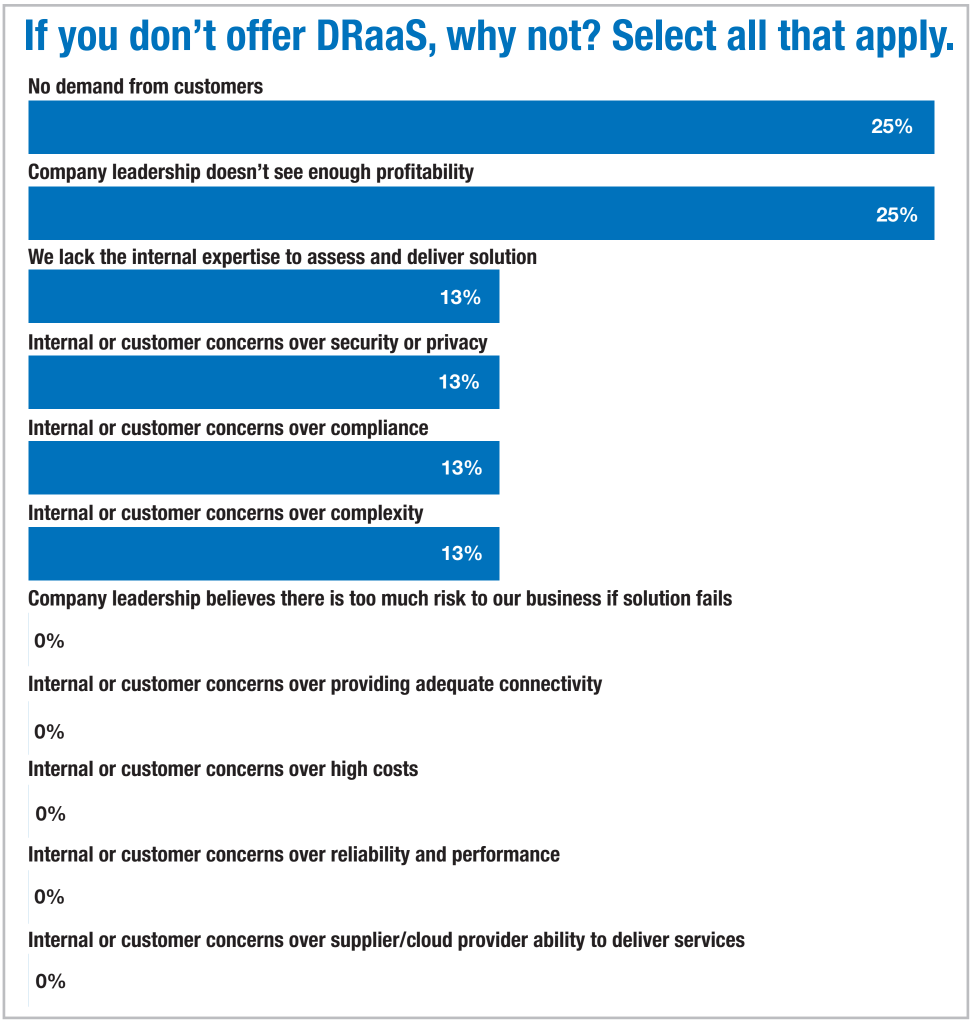


Source: Channel Partners BC/DR Survey, 2017

The good news is solid connectivity options have never been more prevalent. The challenge for most customers will be to realize that running the business on SaaS and using colocation or public cloud for storage and compute doesn't make them bulletproof. In fact, the cloud increases the risks associated with connectivity failure.

"Companies don't seem to realize that running everything in the cloud means they're in big trouble if they lose internet," said one partner. "We have customers with retail offices in remote locations that are at risk. They've been lucky so far, but we are pushing for better backup connections." From another: "The more customers use cloud, the less they worry about disaster because they figure it's now AWS's problem. We have to explain that ransomware and slow connections could still hurt them."

Again, a more effective strategy than throwing scare stats at customers is to combine their optimism regarding emerging technologies like cloud-based DRaaS and insights into what's currently possible and affordable in terms of connectivity. You can deliver levels of RTO and RPO that just a few years ago were achievable only for deep-pocketed enterprises.



* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

Explain that as customers look to a future where less physical infrastructure resides in their buildings. They need to rethink their connectivity models and implement systems that are redundant by default. They will no longer be able to rely on a single connectivity provider. They will, however, need expert guidance to knit WAN technologies, connectivity types and the cloud together to provide a more robust IT infrastructure.

About Our Survey

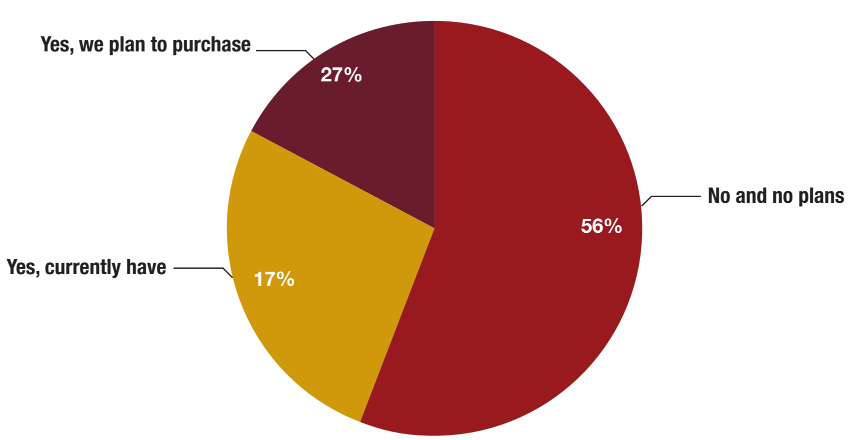
We ran the survey in August and September 2017. Respondents were solicited from the Channel Partners audience via email, newsletter, site ads and social promos. We received 138 responses, but excluded 43 who were either not well qualified or who didn't answer all required questions. We had 41 IT pro and 58 channel respondents.

For purposes of this survey, we defined BC/DR as the set of processes and techniques used to help an organization recover from a disaster and continue or resume routine business operations. It combines the roles and functions of IT and business in the aftermath of a disaster.

Business continuity involves designing and creating policies and procedures that ensure essential business functions/processes are available during and after a disaster. BC can include the replacement of staff, service availability issues, business impact analysis and change management.

Disaster recovery is primarily focused on the IT side of BC/DR. It defines how an organization's IT department will recover from a natural or artificial disaster. The processes within this phase can include server and network restoration, making sure connections are up and adequate, copying data and provisioning backup systems. DR could be delivered as a service in the cloud, by an MSP, in an on-premises model or a mix of these.

Do you currently have or plan to purchase DRaaS?



Source: Channel Partners BC/DR Survey, 2017

Business Continuity & Disaster Recovery: How Connected Are We?

Data volumes have been going nowhere but up for years. So how much is there to lose? Half of the IT pros surveyed have more than 10 TB under protection.

The good news: New techs and connectivity options can deliver better recoverability of all that data, across all locations, for less money. But are we taking advantage?

That depends on who you ask. IT professionals in our survey had a more optimistic outlook than partners who work with a number of firms.

Some disconnects:

Lock it up

Encryption use is spotty, even though the technology has advanced, key management can be had as a service — and it's essentially a "get out of compliance jail free" card. When asked if data is encrypted in transit and at rest …

39% of IT pros say yes, all of it

24% of partners agree

Confidence, thy name is IT

They say hubris goes before data loss. When asked about ability to recover from a disaster or cybersecurity incident …

64% of IT pros are very or somewhat sure they could recover fully

41% of partners agree

Pony up

Sure, BC/DR isn't sexy, but it should get more budget than bagel Fridays. We asked about spend on BC/DR as a percentage of the IT budget, including dedicated connectivity, now and in 2018.

39% of IT pros say BC/DR gets less than 5% of the cash, and 61% expect that to continue

30% of partners say 5% is the limit, but 69% expect increases in 2018

Accounting for loss

We asked how much cash was lost to unplanned downtime in the past 12 months, including productivity. We set $10,000 as the line between "OK, we can fix this" and "There goes the holiday party."

18% of IT pros say they lost more than $10,000

56% of partners say a customer lost more than $10,000

Dream on

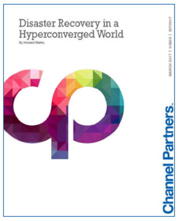
IT doesn't own data, the business does, so the C-suite needs to provide guidance on how much it's OK to lose, and how long workers can sit idle. That is, RPO and RTO metrics.

76% think it should take no more than four hours to bring mission-critical applications back online, and 70 percent say it's acceptable to lose no more than two hours of data

61% of partners say critical data has been unrecoverable. Poof.

Data: Channel Partners 2017 BC/DR Survey

Related Reports

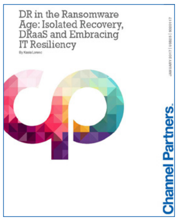


Disaster Recovery in a Hyperconverged World

Hyperconvergence simplifies IT infrastructure design by integrating the storage layer with compute and networking. This reduces complexity and saves money, but it also requires changes in how customer data and applications are protected. This Report explains how to think about disaster recovery solution in the context of HCI.

SD-WAN: A Branch Office, Remote Site Savior

Got clients that want to transition to SD-WAN, but see remote site connectivity as a roadblock? That's where you come in. This Report explains how a hybrid WAN can bundle multiple connection types and provide customers with business-class features, security and connectivity to locations where traditional circuits would be prohibitively expensive.



DR in the Ransomware Age: Isolated Recovery, DRaaS and Embracing IT Resiliency

Ransomware attacks are becoming more frequent, complex and sophisticated. Security experts agree, it's not if an attack will come, but when. Disaster recovery can be your customers' best line of defense. This Report explains how the right tools can help you arm yourself against the devastating effects of ransomware.

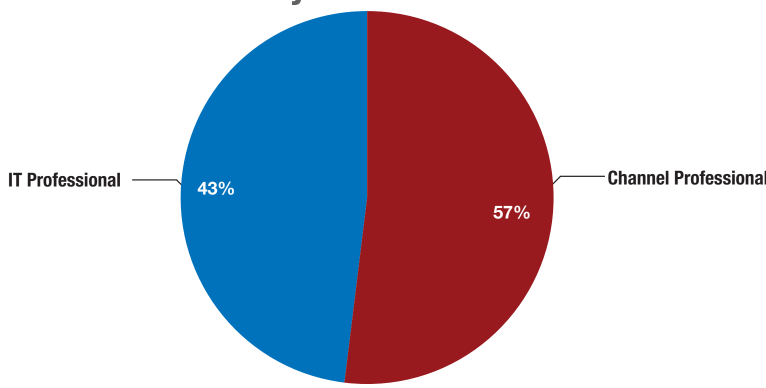
UC Demands Rethinking Disaster Recovery Plans

Voice and UC in the cloud have created expectations of 24/7 contact among your clients and their customers. Helping this happen requires good planning and system design — and represents professional service opportunities for partners. This report examines what's involved in communications disaster planning, as well as the professional services opportunities it presents to partners.

Appendix

All IT Professional Survey Results are in blue and all Channel Professional Results are in red

What best describes you?



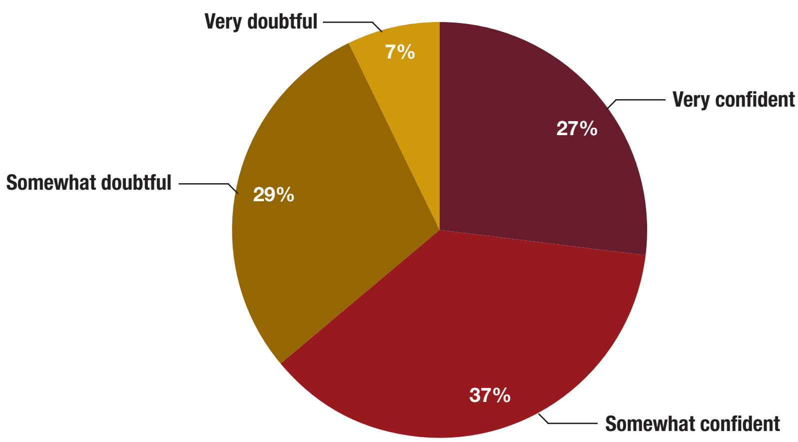
Source: Channel Partners BC/DR Survey, 2017

What are the most significant drivers for investing in BC/DR? Please rank in order of importance.

1	Connectivity failure
2	Equipment failure
3	Future possible natural disaster
4	Security: Ransomware, malware or other threat
5	Power failure
6	Insistence by line-of-business leaders
7	Previously burned by disaster, data loss or other externally driven failure
8	Other

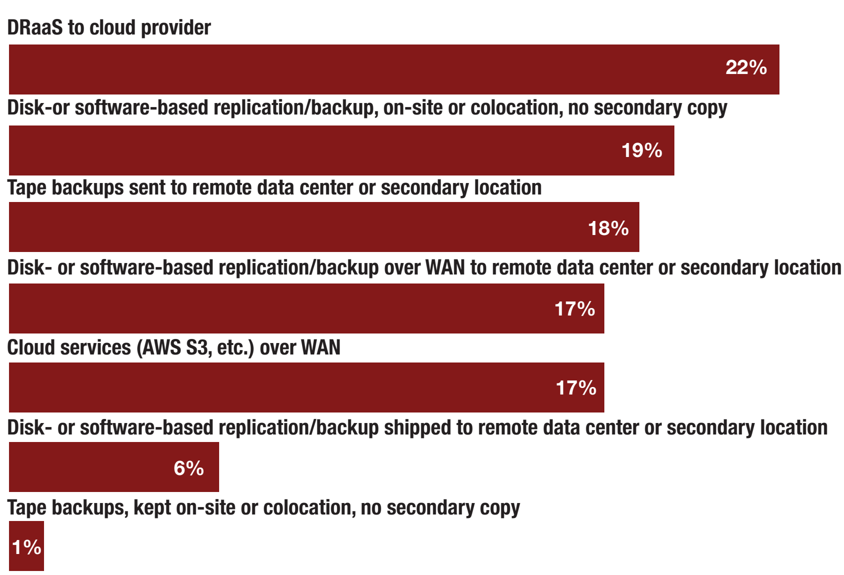
Source: Channel Partners BC/DR Survey, 2017

How confident are you that you could recover fully from a disaster or cybersecurity incident such as ransomware?



Source: Channel Partners BC/DR Survey, 2017

What backup components are included in your BC/DR plans? Select all that apply.



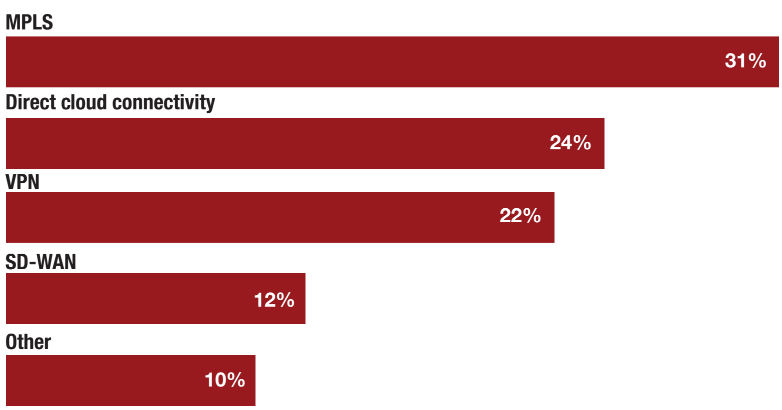
Source: Channel Partners BC/DR Survey, 2017

What connectivity methods are included in your BC/DR plans? Select all that apply for each location.

	Main Office	Remote Office	Remote User	Not Used
Leased lines (T1, Ethernet, MPLS or point-to-point)	22	6	1	15
Broadband, cable	13	12	12	8
Broadband, fiber	9	14	1	17
Cellular, LTE	9	5	10	18
Dedicated Internet Access	6	9	6	22
DSL	3	4	5	30
Satellite	3	2	10	27
Other	1	3	4	33

Source: Channel Partners BC/DR Survey, 2017

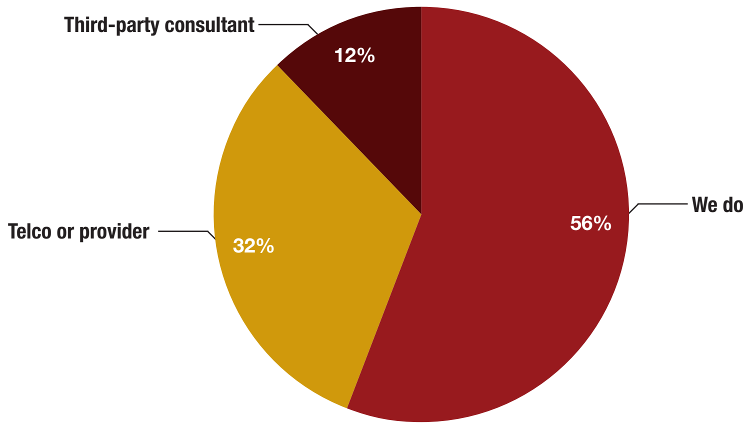
What connectivity technologies are included in your BC/DR plans? Select all that apply



* Figures do not total 100% due to rounding.

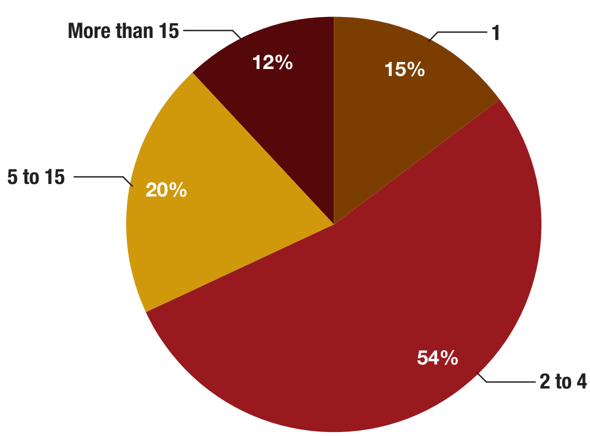
Source: Channel Partners BC/DR Survey, 2017

Who manages the connectivity for your BC/DR plan? Select all that apply



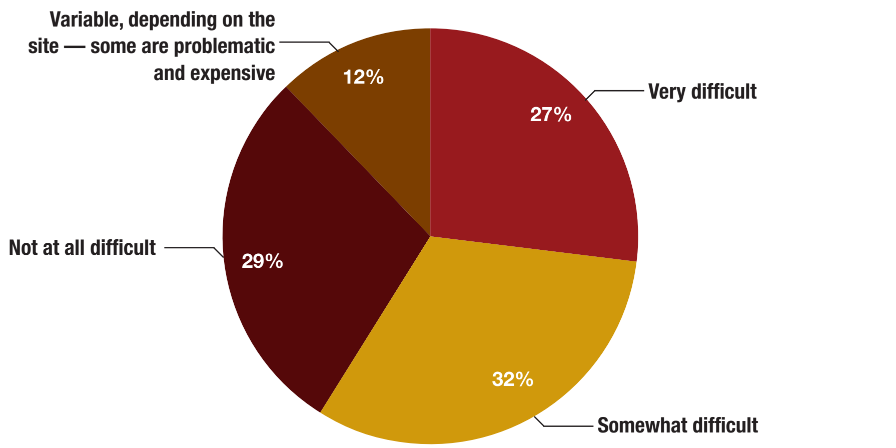
Source: Channel Partners BC/DR Survey, 2017

How many locations are included in your BC/DR plan?



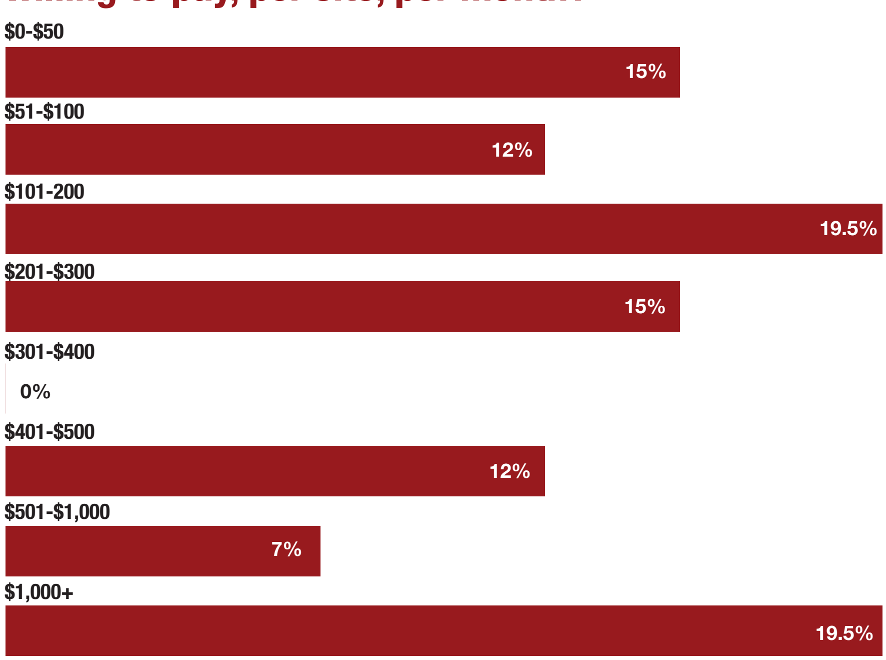
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

How difficult is it to provide adequate connectivity at an affordable cost to these sites to achieve BC/DR objectives?



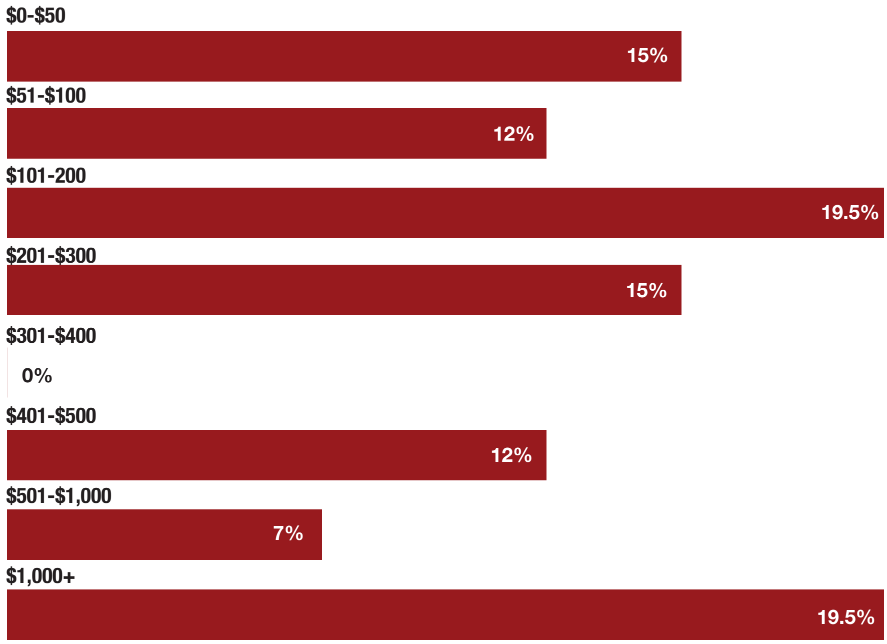
Source: Channel Partners BC/DR Survey, 2017

When deploying a secondary/backup internet connection, what is the maximum price point you are willing to pay, per site, per month?



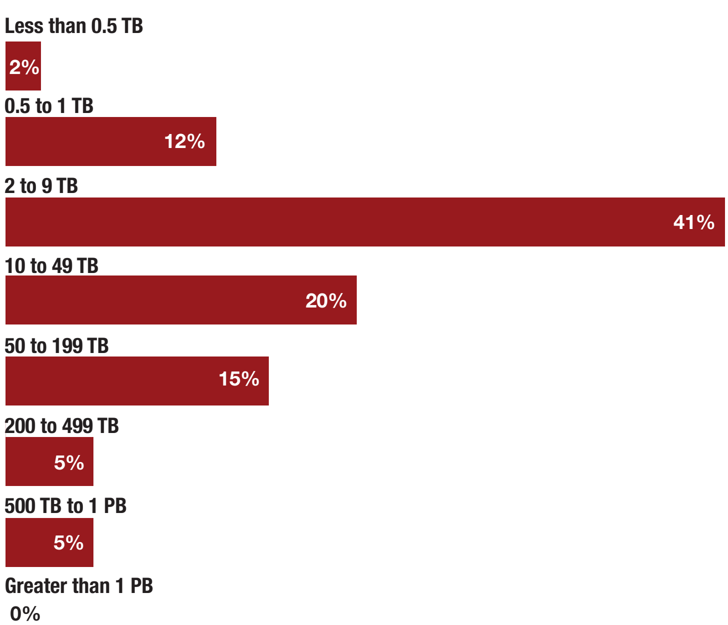
Source: Channel Partners BC/DR Survey, 2017

When deploying a secondary/backup internet connection, what is the maximum price point you are willing to pay, per site, per month?



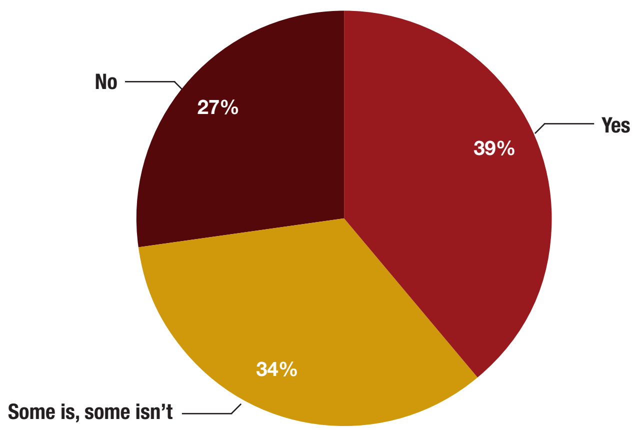
Source: Channel Partners BC/DR Survey, 2017

How much total data is under protection?



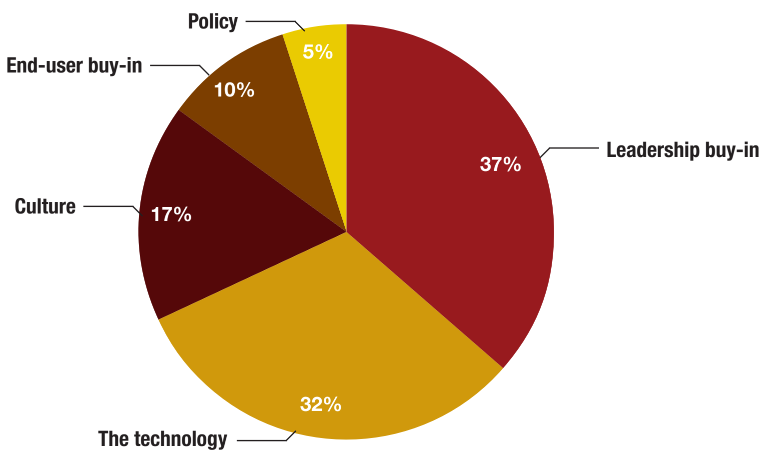
Source: Channel Partners BC/DR Survey, 2017

Is data encrypted in transit and at rest?



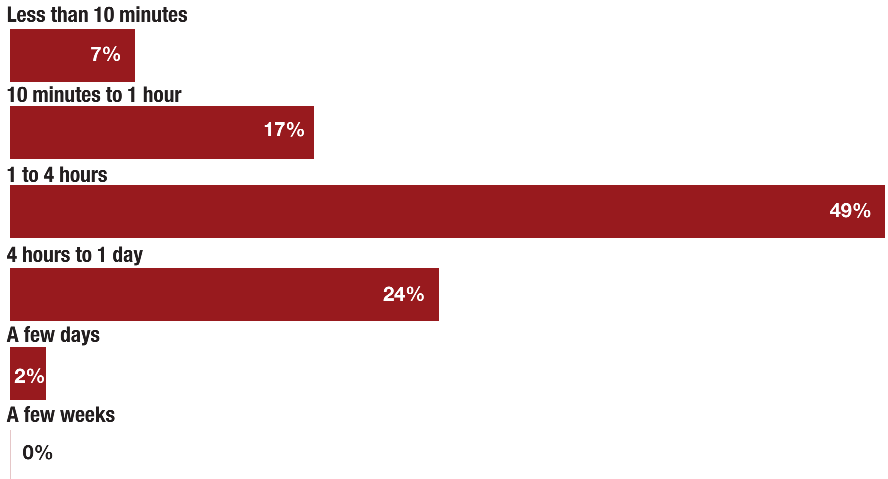
Source: Channel Partners BC/DR Survey, 2017

What's the hardest thing to get right when crafting a business continuity plan?



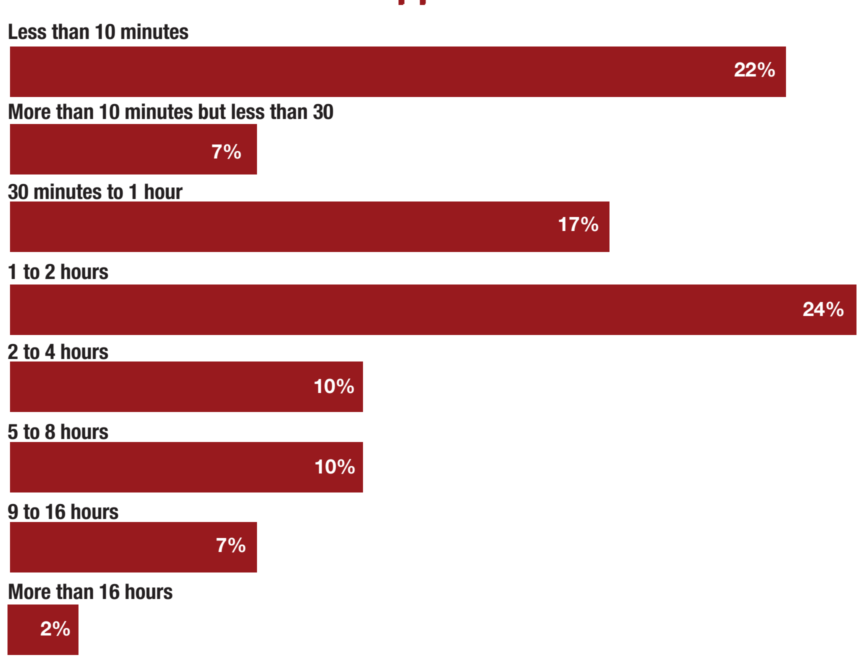
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

RTO: What is your target recovery-time objective? That is, how long should it take to bring mission-critical applications back online?



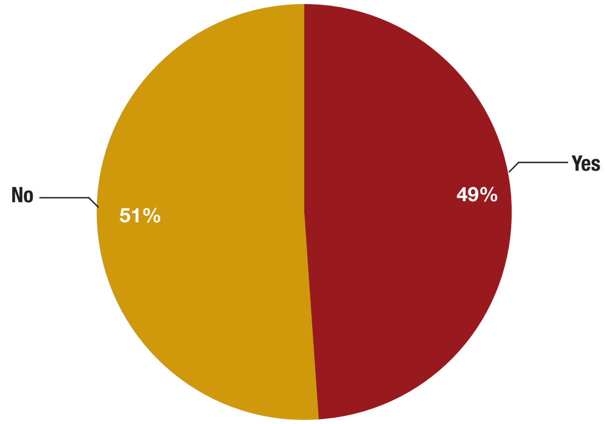
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

RPO: What is your target recovery-point objective? That is, how much data is it acceptable to be lost once mission-critical applications are back online?



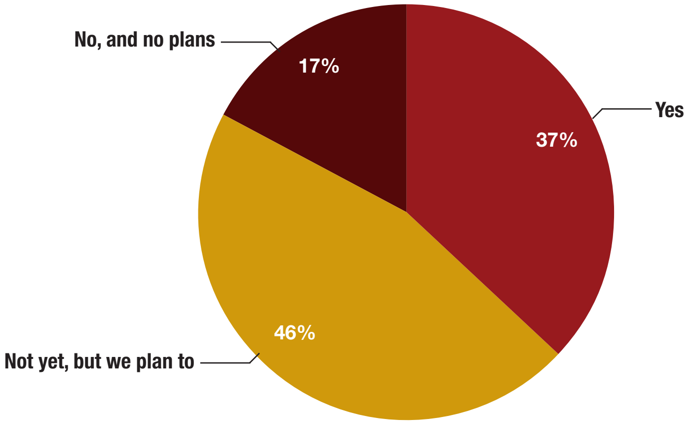
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

Have there been instances where critical data was unrecoverable?



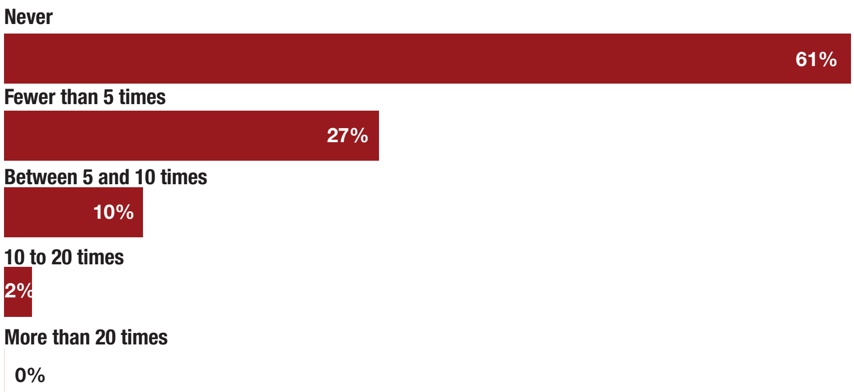
Source: Channel Partners BC/DR Survey, 2017

Do you have ransomware protection in place?



Source: Channel Partners BC/DR Survey, 2017

How many times have you activated your BC/DR plan in the past 12 months?



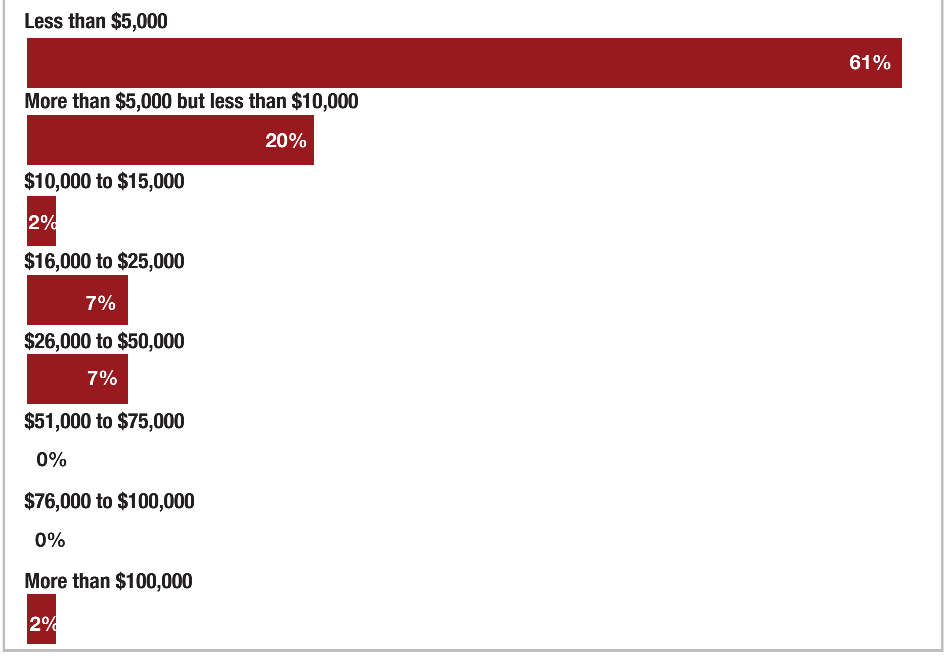
Source: Channel Partners BC/DR Survey, 2017

What caused these outages?

	1-3	3-5	5 or more	None
Ransomware or other malware	11	0	1	4
Human error	8	1	2	5
Hardware failure	6	1	2	7
Severed connection line	5	1	2	8
Software failure	4	4	0	8
Power outage	4	1	2	9
Natural disaster	3	2	0	11
Other	2	0	1	13

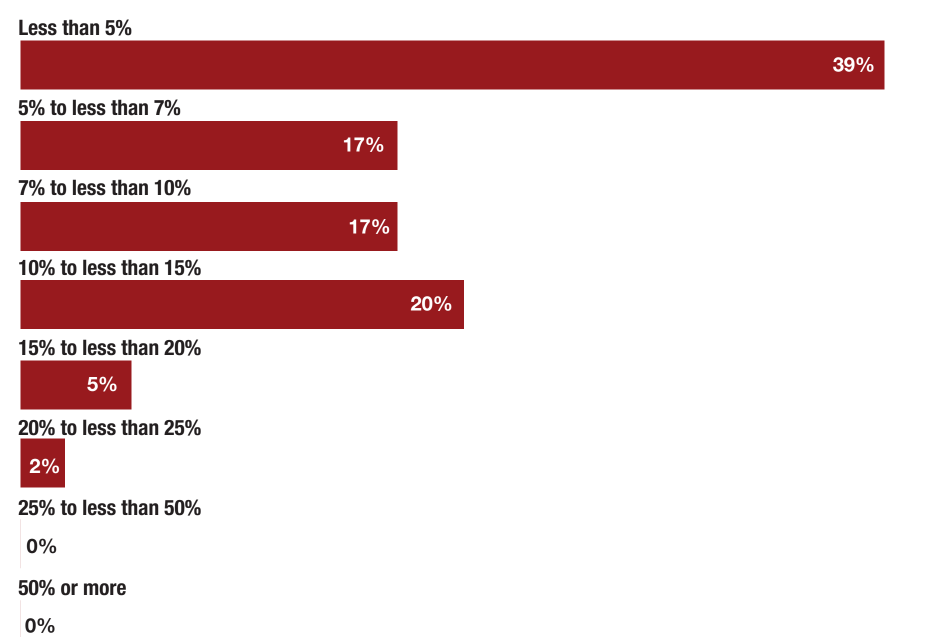
Source: Channel Partners BC/DR Survey, 2017

How much did the business lose to unplanned downtime in the past 12 months, including lost productivity?



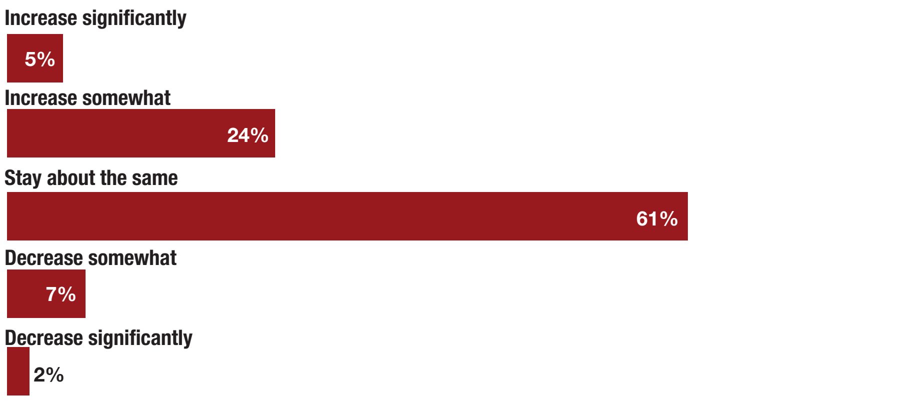
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

What percentage of your budget is currently allocated to BC/DR, including dedicated connectivity?



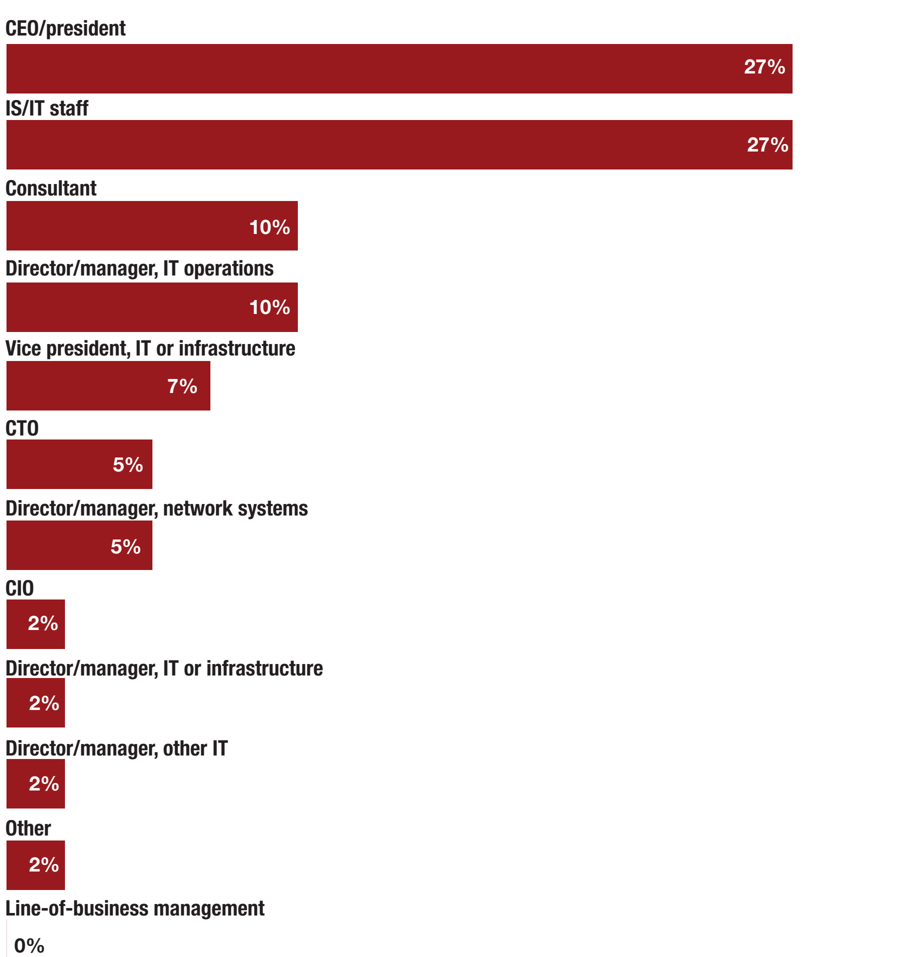
Source: Channel Partners BC/DR Survey, 2017

How do you expect that BC/DR budget to change in 2018?



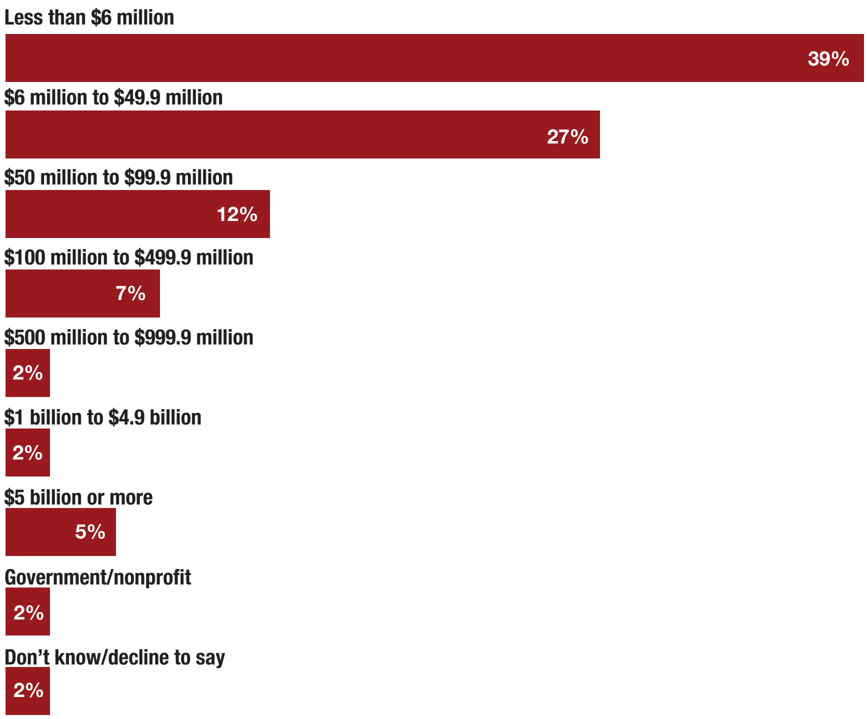
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

Which of the following best describes your job title?



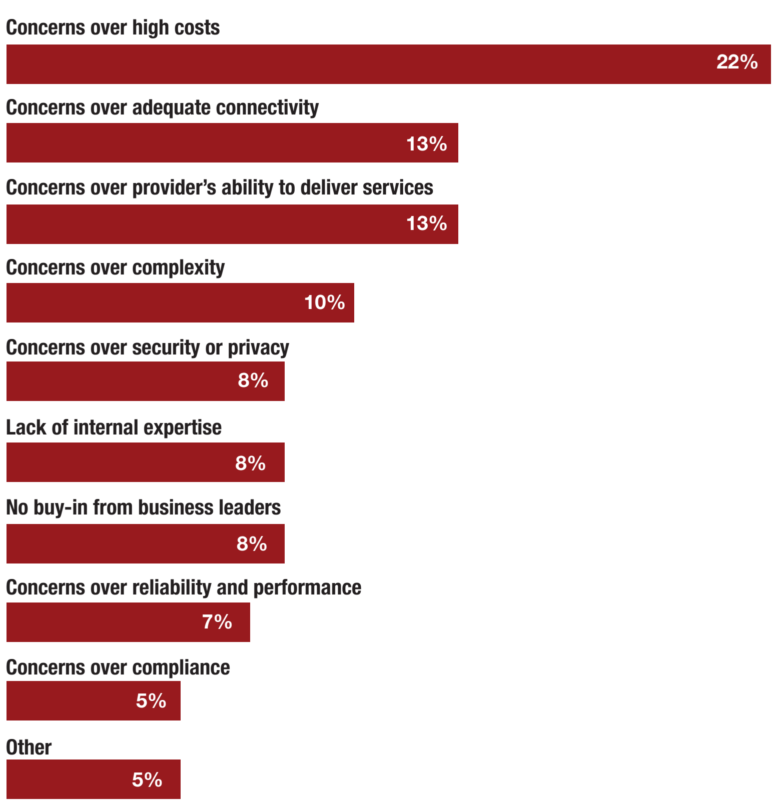
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

Which of the following dollar ranges includes the annual revenue of your entire organization?



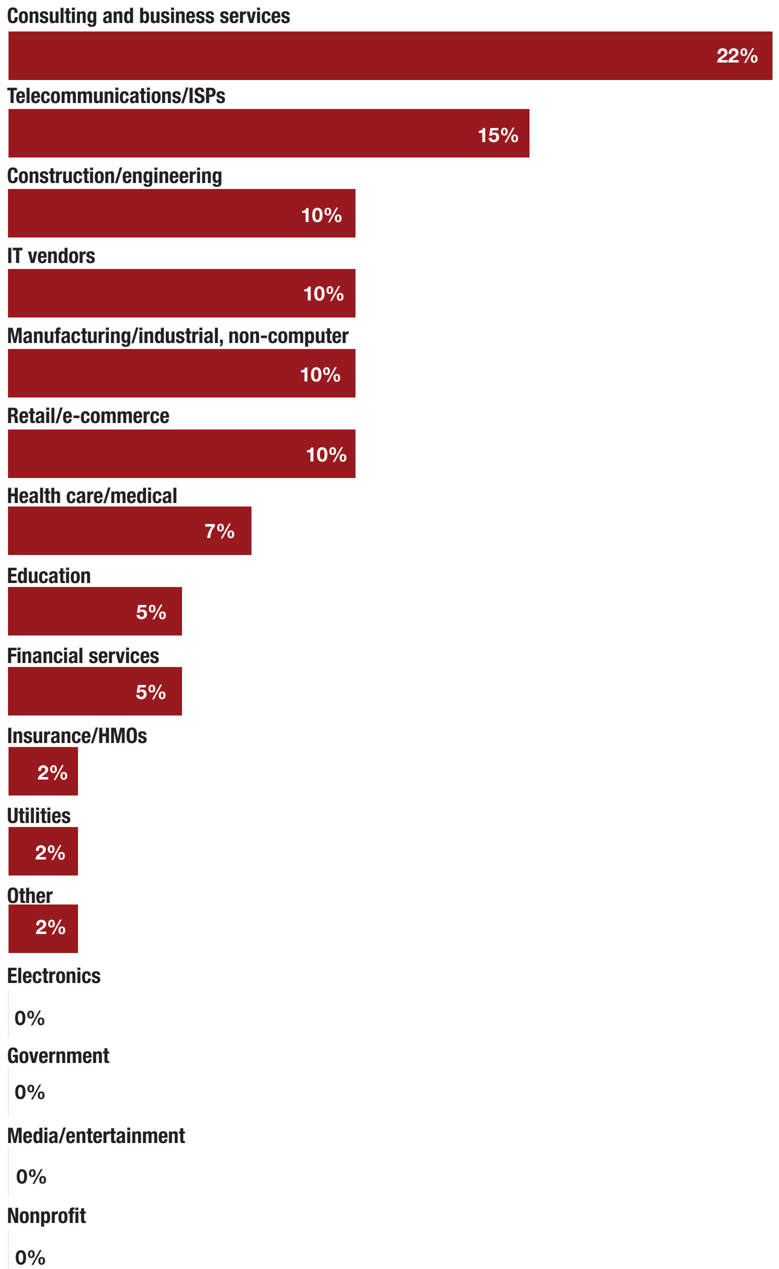
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

If you are not interested in DRaaS, why not? Select all that apply.



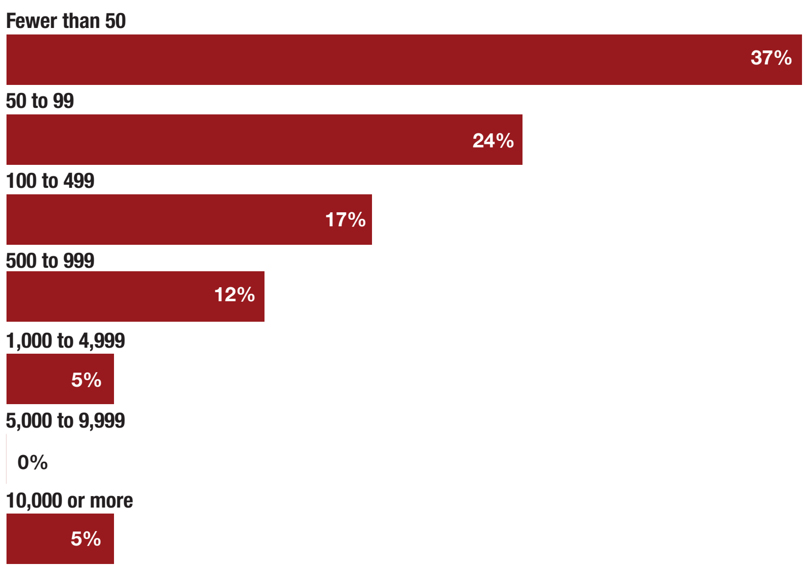
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

What is your organization's primary industry?



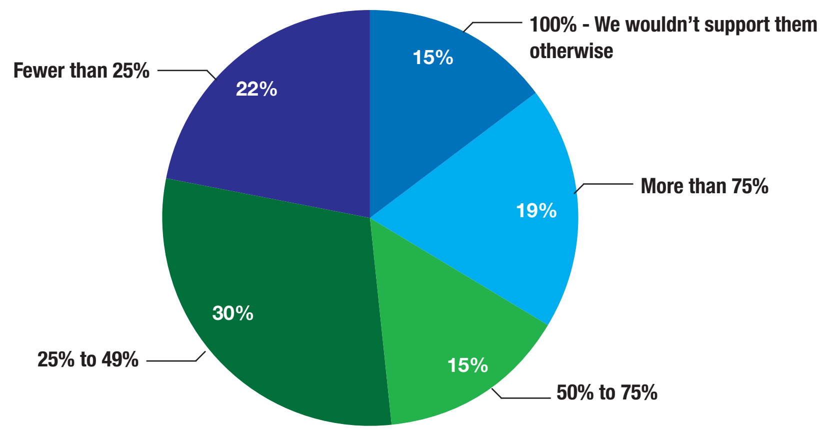
Source: Channel Partners BC/DR Survey, 2017

Approximately how many employees are in your organization?



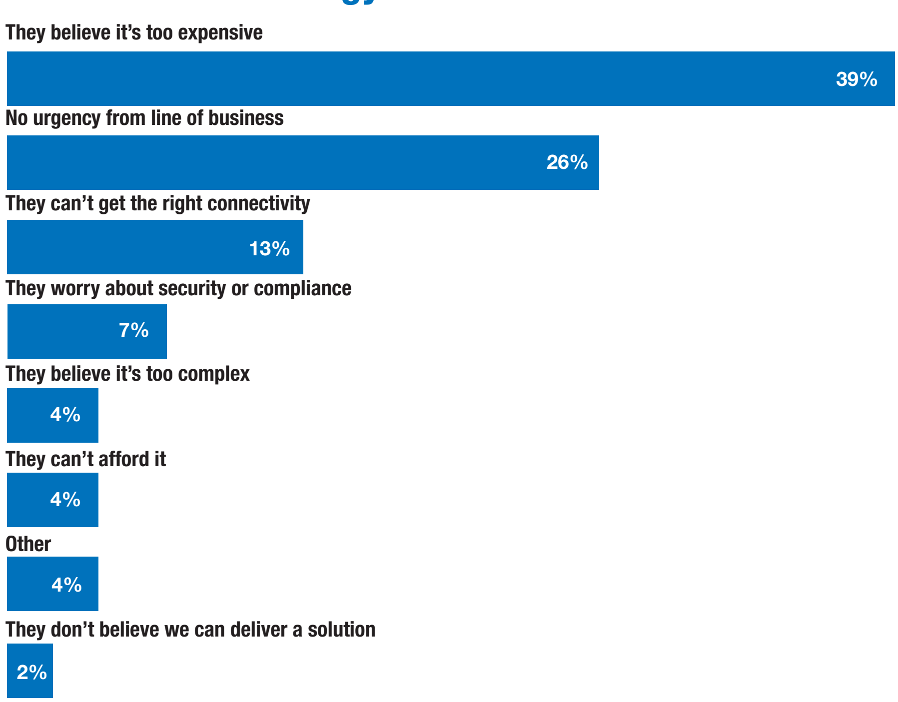
Source: Channel Partners BC/DR Survey, 2017

What percentage of your customers have effective business continuity/disaster recovery (BC/DR) plans?



* Figures do not total 100% due to rounding
Source: Channel Partners BC/DR Survey, 2017

What is the TOP objection for customers that don't have a BC/DR strategy?



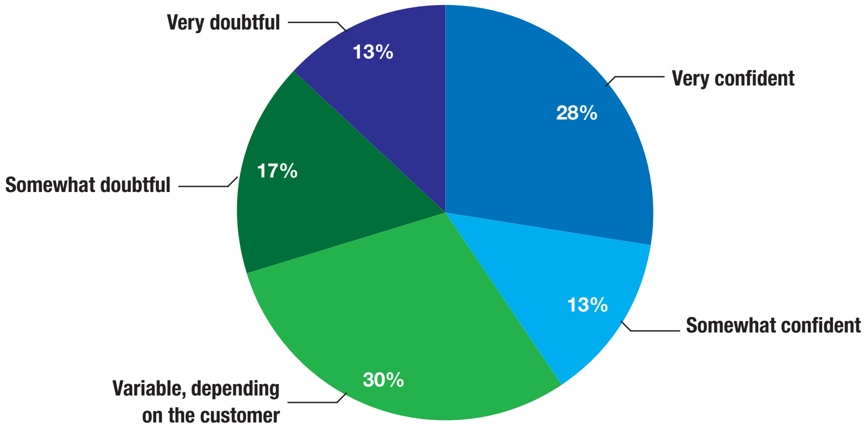
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

What are the most significant drivers for investing in a BC/DR strategy? Please rank in order of importance.

1	Security: Ransomware, malware or other threat
2	Connectivity failure
3	Equipment failure
4	Future possible natural disaster
5	Insistence by line-of-business leaders
6	Previously burned by disaster, data loss or other externally driven failure
7	Power failure
8	Other

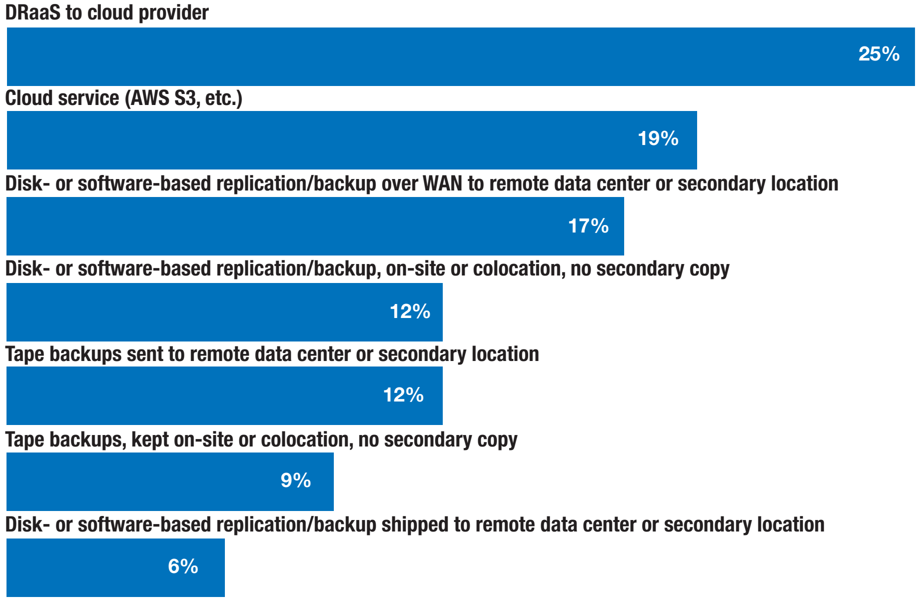
Source: Channel Partners BC/DR Survey, 2017

How confident are you that most of your customers could recover from a disaster or cybersecurity incident such as ransomware?



* Figures do not total 100% due to rounding
Source: Channel Partners BC/DR Survey, 2017

What backup components are included in customers' BC/DR plans? Select all that apply.

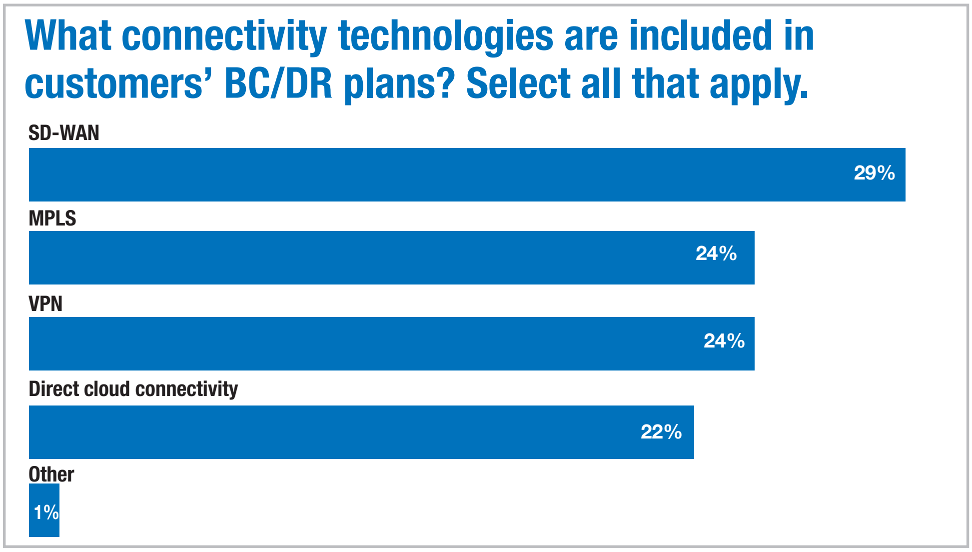


Source: Channel Partners BC/DR Survey, 2017

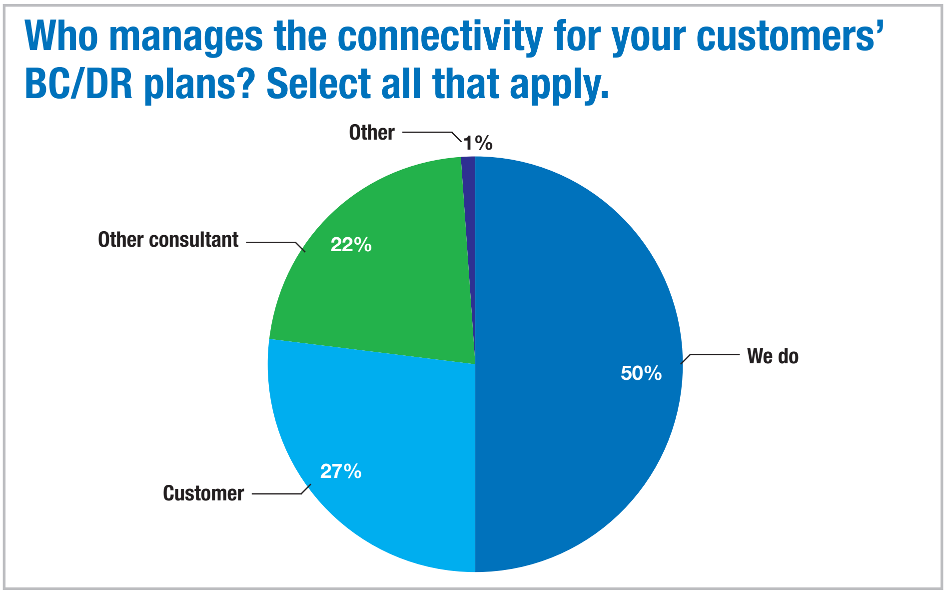
What connectivity methods are included in your BC/DR plans? Select all that apply for each location.

	Main Office	Remote Office	Remote User	Not Used
Satellite	40	19	2	6
Broadband, fiber	21	18	11	7
Broadband, cable	18	33	11	1
DSL	17	7	2	32
Cellular, LTE	6	16	24	14
Leased lines (T1, Ethernet, MPLS or point-to-point)	6	14	5	31
Dedicated Internet Access	5	8	22	23
Other	3	5	1	47

Source: Channel Partners BC/DR Survey, 2017

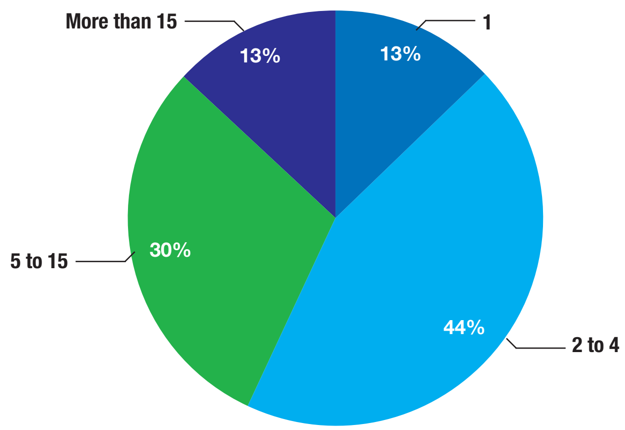


Source: Channel Partners BC/DR Survey, 2017



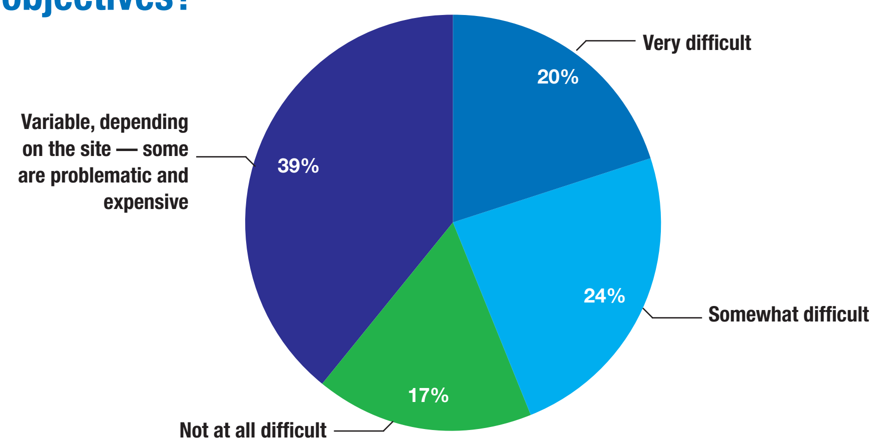
Source: Channel Partners BC/DR Survey, 2017

How many locations are included in your typical customer's BC/DR plan?



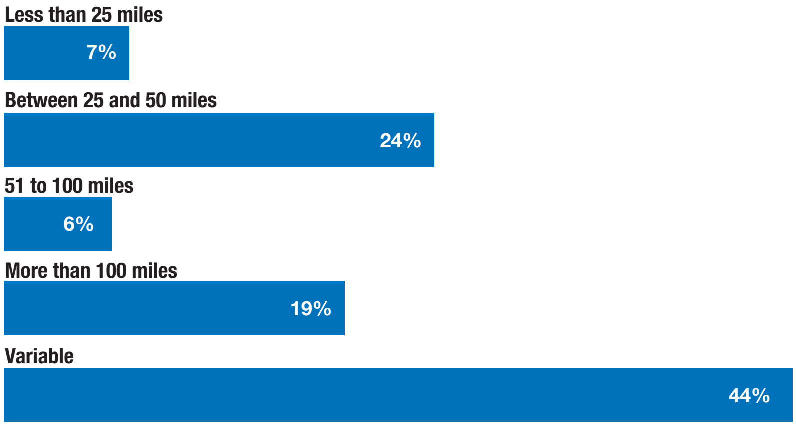
Source: Channel Partners BC/DR Survey, 2017

How difficult is it to provide adequate connectivity at an affordable cost to these sites to achieve BC/DR objectives?



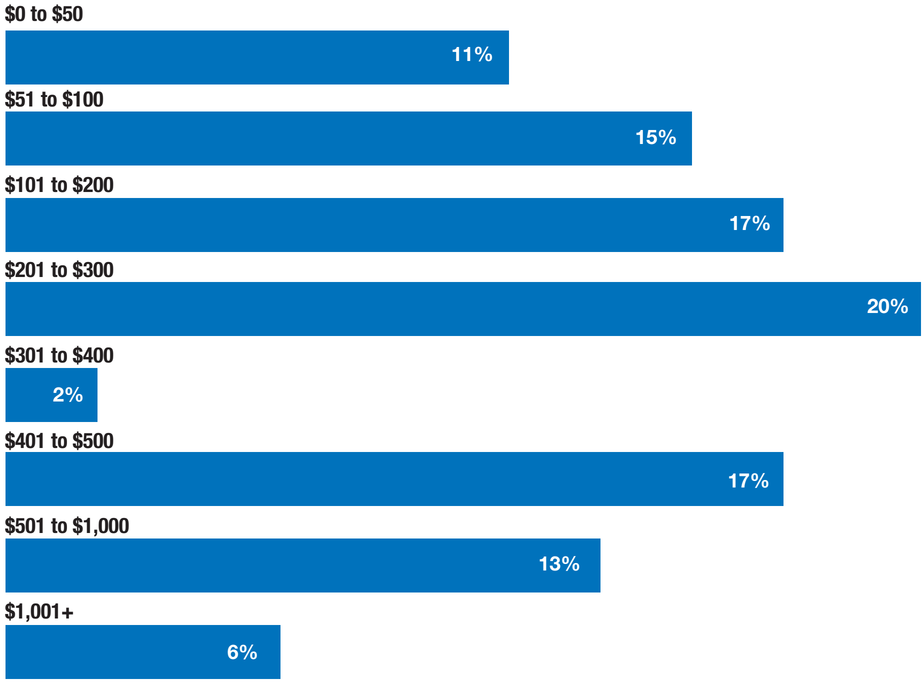
Source: Channel Partners BC/DR Survey, 2017

Typically, how far are secondary sites from primary sites?



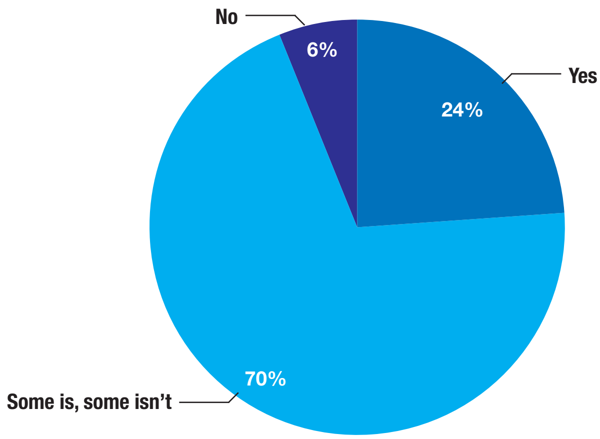
Source: Channel Partners BC/DR Survey, 2017

When deploying a secondary/backup internet connection, what price point are your customers willing to pay, per site, per month?



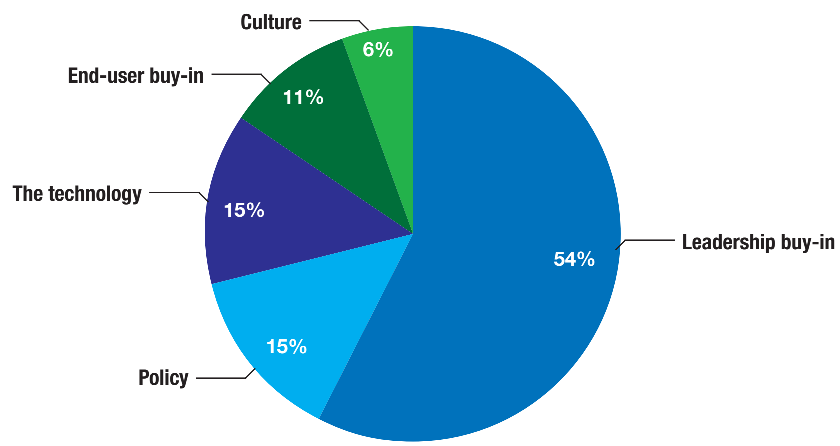
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

Is customer data encrypted in transit and at rest?



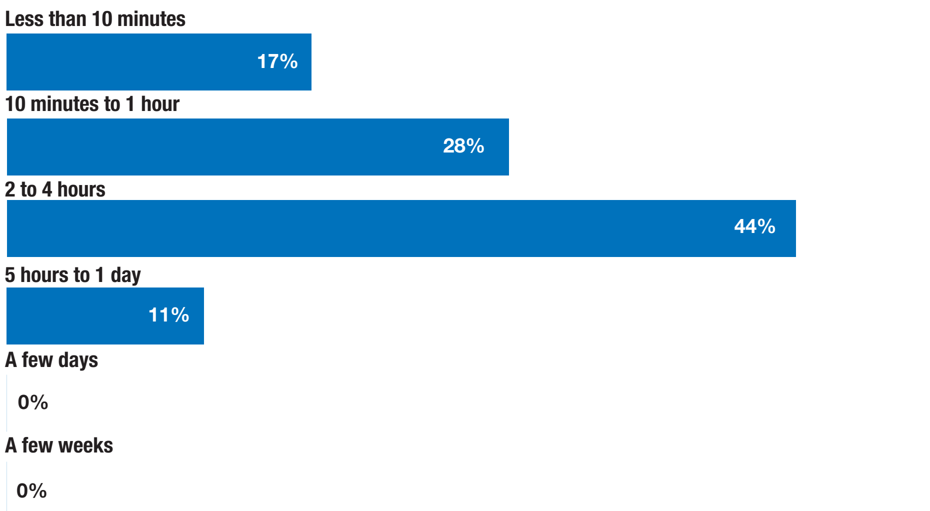
Source: Channel Partners BC/DR Survey, 2017

What's the hardest thing to get right when helping customers craft a business continuity plan?



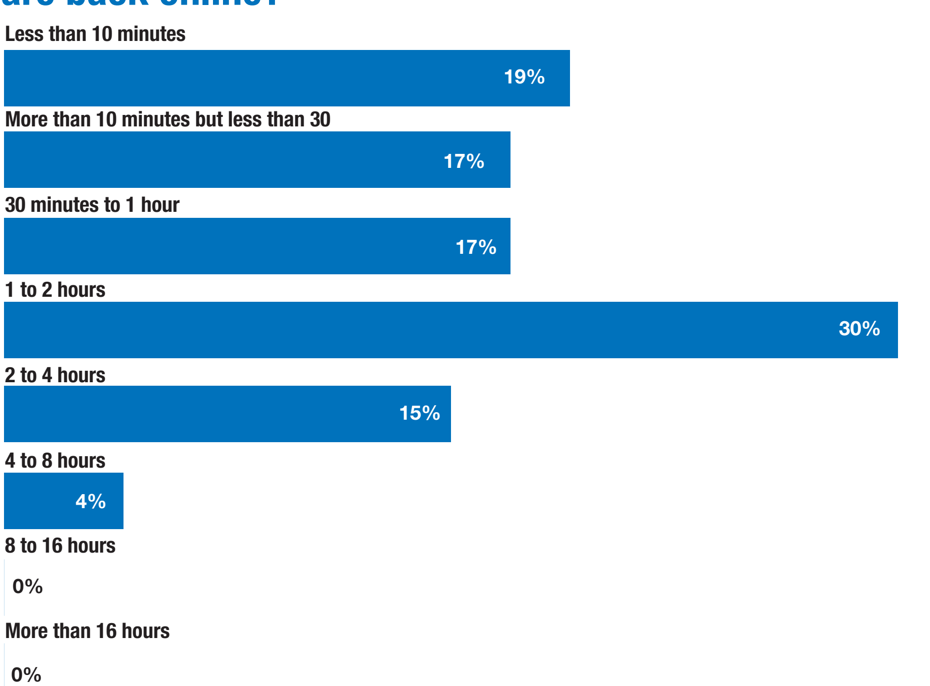
* Figures do not total 100% due to rounding
Source: Channel Partners BC/DR Survey, 2017

RTO: What is the typical recovery-time objective demanded by customers? That is, how long is it acceptable to take to bring mission-critical applications back online?



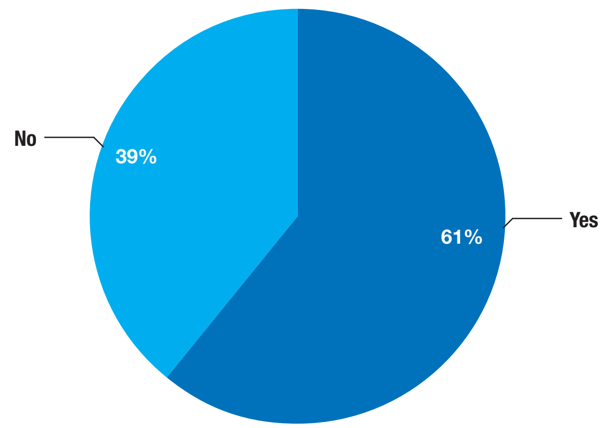
Source: Channel Partners BC/DR Survey, 2017

RPO: What is the typical recovery-point objective demanded by customers? That is, how much data is it acceptable to be lost once mission-critical applications are back online?



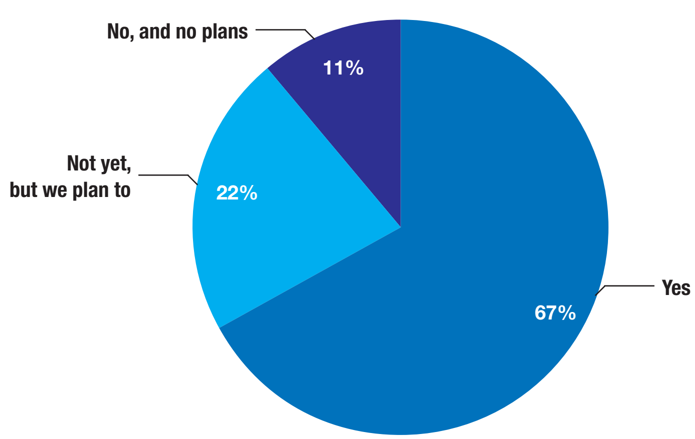
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

Have there been instances where critical customer data was unrecoverable?



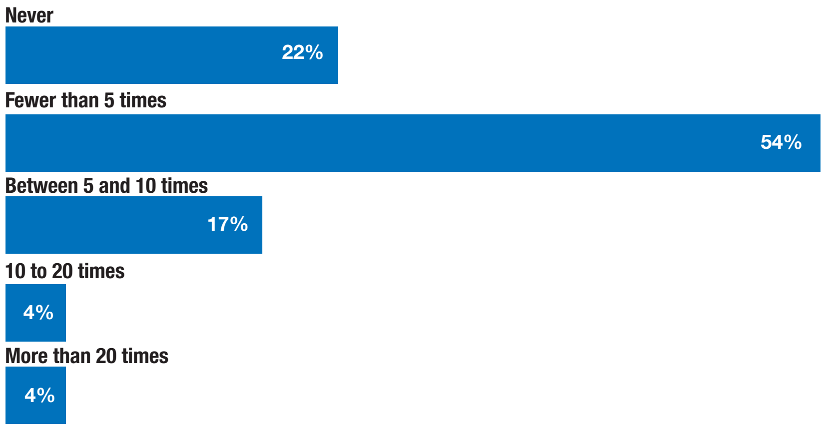
Source: Channel Partners BC/DR Survey, 2017

Do you have a specific plan or product to provide ransomware protection?



Source: Channel Partners BC/DR Survey, 2017

How many times have you activated a customer's BC/DR plan in the past 12 months?



* Figures do not total 100% due to rounding.

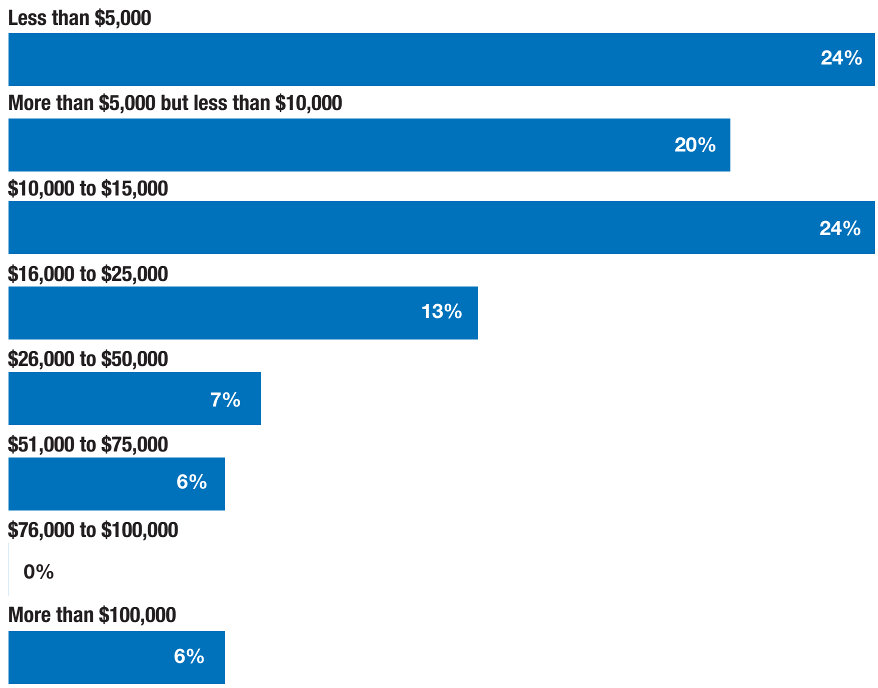
Source: Channel Partners BC/DR Survey, 2017

What caused these outages?

	1-3	3-5	5 or more	None
Ransomware or other malware	24	7	2	9
Hardware failure	19	3	1	19
Human error	16	4	3	19
Natural disaster	10	1	0	31
Severed connection line	9	1	1	31
Software failure	6	1	1	34
Power outage	5	3	0	34
Other	2	1	0	39

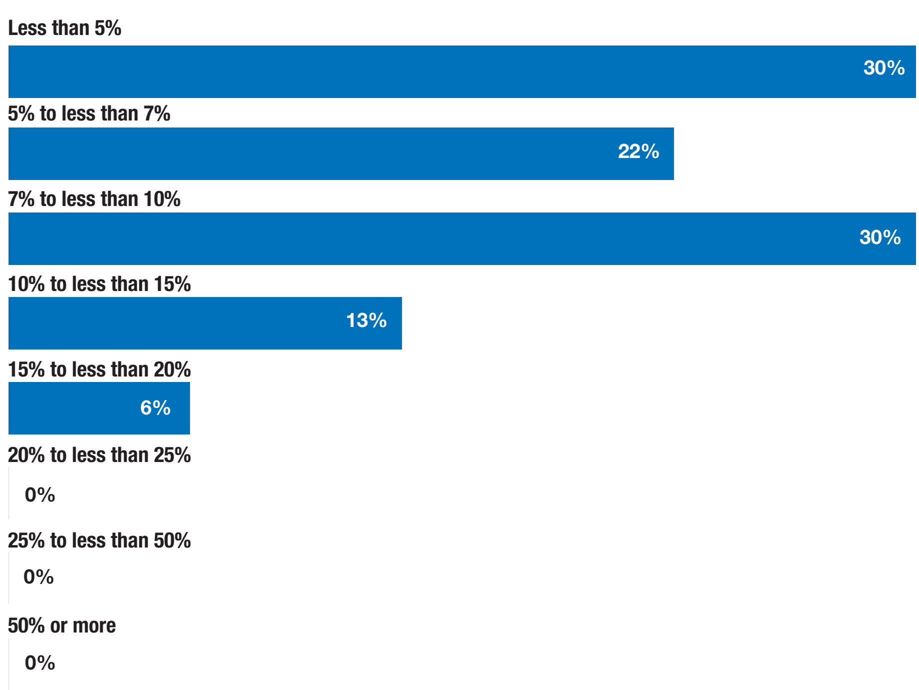
Source: Channel Partners BC/DR Survey, 2017

How much did these incidents cost customers, including lost productivity?



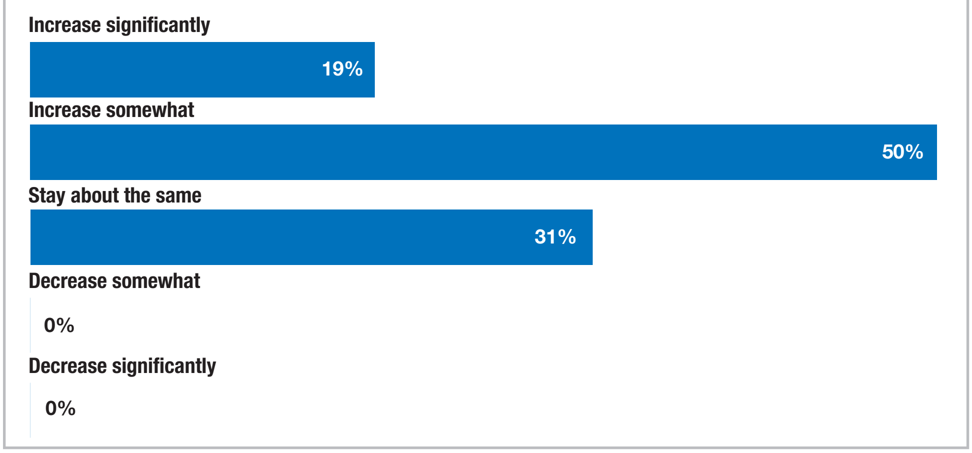
Source: Channel Partners BC/DR Survey, 2017

What percentage of your typical customer's current FY IT budget is allocated for BC/DR, including upgraded connectivity?



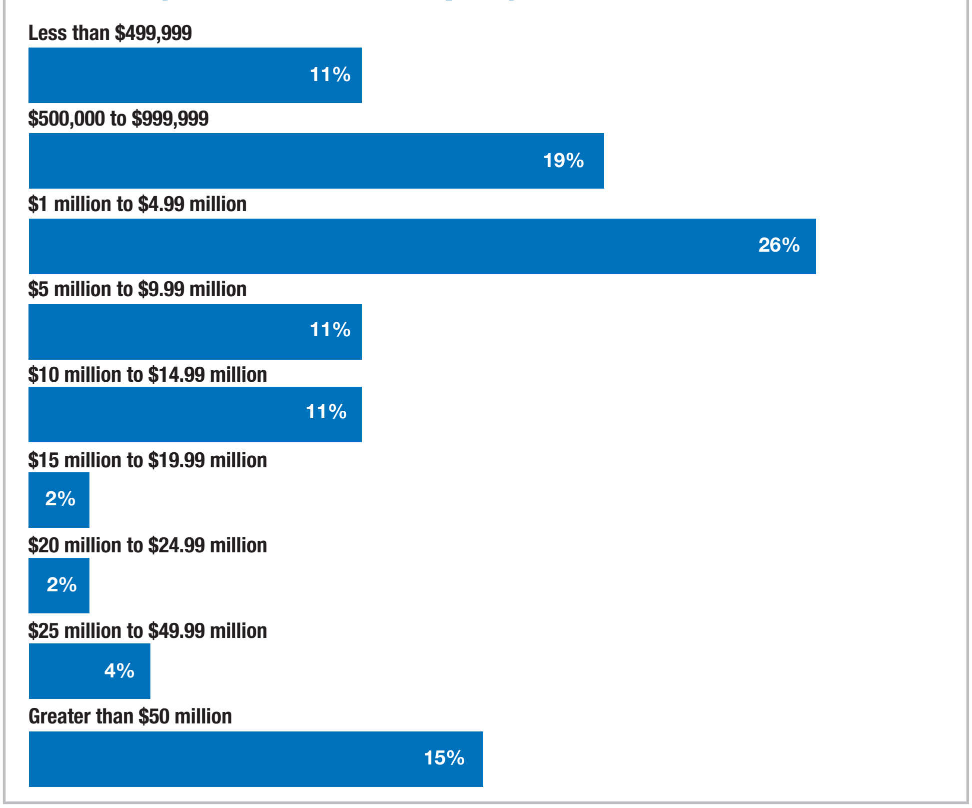
* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017

How do you expect BC/DR budgets to move in 2018?

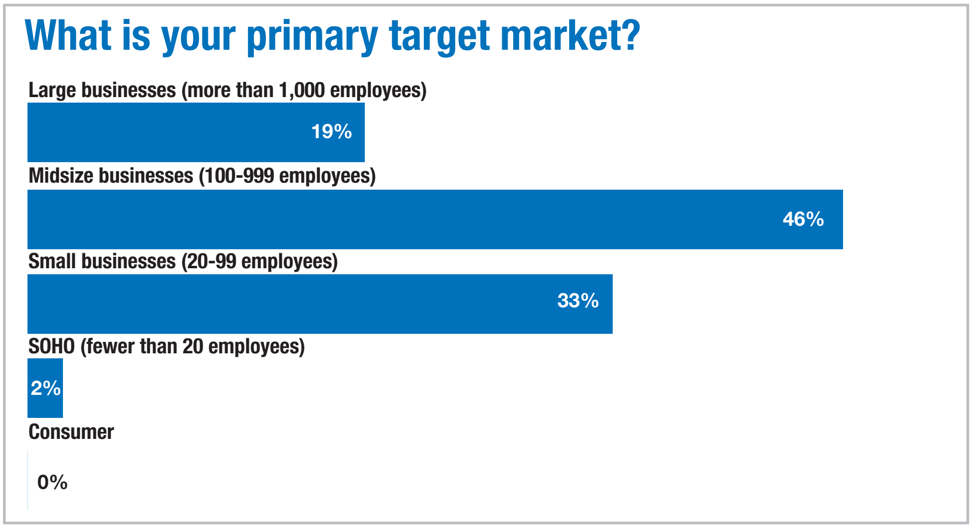


Source: Channel Partners BC/DR Survey, 2017

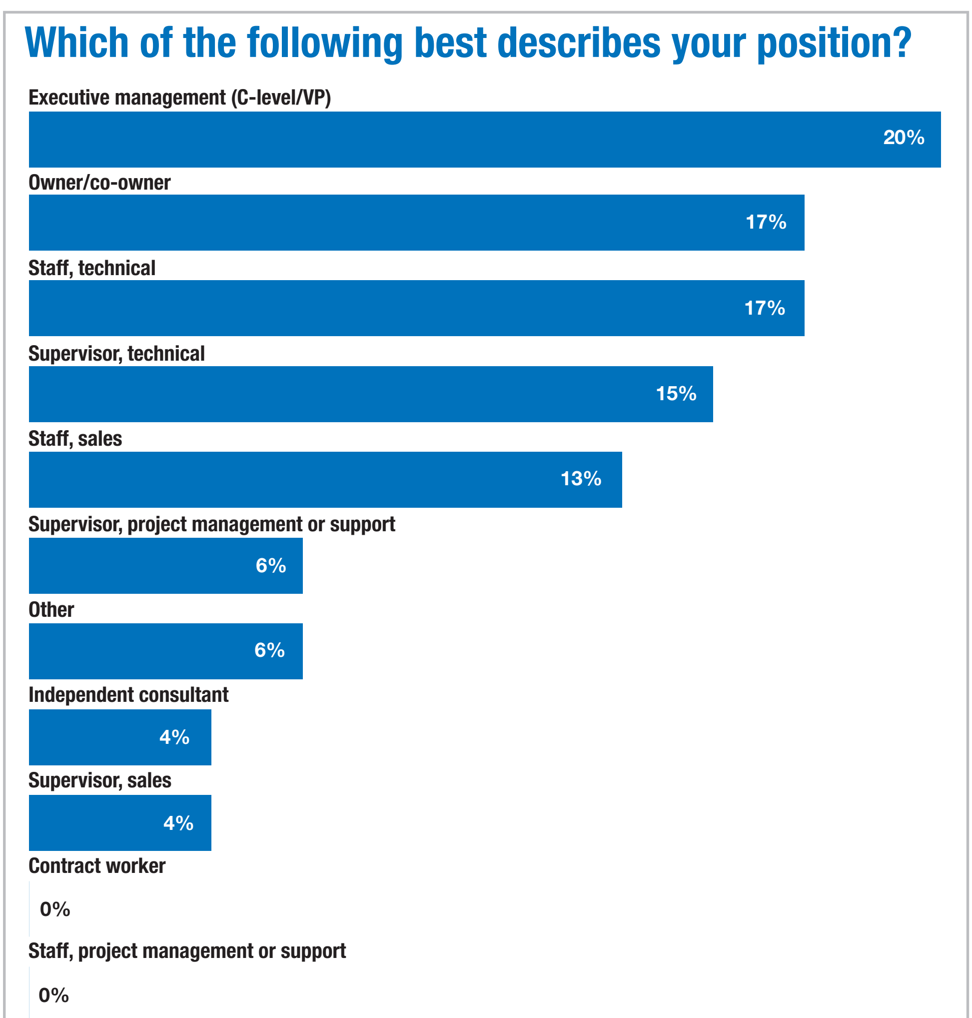
What is your annual company revenue?



* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017



Source: Channel Partners BC/DR Survey, 2017



* Figures do not total 100% due to rounding.
Source: Channel Partners BC/DR Survey, 2017