Forbes insights

Perception Gaps in Cyber Resilience: Where Are Your Blind Spots?

The hidden risks of shadow IT, cloud and cyber insurance

IN ASSOCIATION WITH:

kyndryl™

Forbes insights

TABLE OF CONTENTS

INTRODUCTION

Protecting enterprise systems against cyber threats is a strategic priority and a well-funded, highly analyzed process at most organizations. But as technological ecosystems grow beyond the four walls of the organization, there arise a number of gray areas, where it is not clear who is responsible for security and who bears the costs if there is a breach, an outage, a simple error or outright sabotage. Shadow IT, availability coverage by cloud-service providers and cyber insurance coverage are three of the most vexing and persistent blind spots for CIOs today.

The democratization of IT, for example, is raising the threat that an organization could be blindsided by technology it cannot directly control. Any line-of-business manager can subscribe to a cloud-based software service customized for his or her operations—and many do so with little regard for security. Most organizations rely on their service providers to manage security in the cloud. But what happens if a third-party application developer sets the wrong access parameters and leaves your organization's cloud-based service wide open?

Mitigating some of that risk with cyber insurance sounds like a wise choice, but what does it actually cover? Many organizations have discovered the hard way that insurance is no substitute for a strong resilience profile.

There is more at stake than avoiding a major disaster. IDC points out that the digital future will rely on diverse, distributed and dynamic data. IDC believes that most organizations will leverage an intelligent core infrastructure that will turn business activity insights into actionable intelligence in a streamlined, continuous process. This makes data critical to business survival, but the programs and capabilities designed to protect data flow are lagging.

At the same time, greater diversity means that an organization's core infrastructure will rely not only on familiar structured systems but also unstructured data such as time series data, machine-generated data and streaming data—any of which, if corrupted, could potentially skew automated processes or machine learning. Data is also more dynamic, as telemetry data is generated from sensors and devices, many of which will be interacting in real time. Data is now distributed widely, in edge locations, on devices and in cloud-services.

As systems and processes become hyperconnected, one small, discrete event can reverberate through an entire organization. The immediate cost of a breach or outage does not even begin to cover potential losses in present and future sales, production and working time. Plus, there may well be reputational damage, legal and regulatory ramifications or the less tangible cost that corrupt or incomplete data can have on an intelligent infrastructure.

Even the most robust cybersecurity program could never prevent every possible breach or disruption. Most organizations already plan for the inevitable with a plan for restoration and recovery. But will recovery plans be enough to protect against data corruption? Will they be enough to recover from a significant disruption to processes that rely on a continuous, dynamic, real-time data flow, such as those for an automated vehicle?

True cyber resilience means having a plan that could protect data and systems as they evolve and minimizing damage and disruption that could come from new threats. It means addressing the life cycle of data as it is created, dispersed and stored as well as building resilience into every step.

This report is based on a Forbes Insights and Kyndryl, formerly IBM Infrastructure Services, survey of 353 executives across the globe, which reveals a significant disconnect between how executives view resilience and responsibility when it comes to the gray areas of their expanding technology ecosystems. The survey focuses on the three areas where perception gaps and blind spots may be causing the greatest confusion and disappointment when it comes to cyber resilience:

- **Shadow IT: You can't protect what you can't see**
- **Availability coverage by cloud-service providers: Who bears the true cost of a cyber event?**
- **Cyber insurance: What does it actually cover?**

In many cases, these perception gaps exist between those who should be responsible when something goes wrong and those who actually bear the costs when it does. Wherever there are gaps in responsibility, resilience is at risk.

KEY FINDINGS

- ✓ **Only 42% of surveyed executives are confident their organization could recover from a major cyber event without impacting their business**
- ✓ **More than 50% of surveyed organizations have experienced at least one cyber incident in the last three years**
- ✓ **21% of organizations experienced cyber events due to a non-sanctioned IT resource**
- ✓ **60% of organizations don't include shadow IT in their threat assessment**
- ✓ **13% of organizations have lost data or faced downtime due to incidents with their cloud-service provider; 58% of these incidents were security breaches**
- ✓ **56% of those who suffered losses due to a cloud incident were not compensated by their providers**
- ✓ **Among the executives who purchased cyber insurance, only four in 10 believe that costs of data recovery and crisis management would actually be covered**
- ✓ **Just 27% believe their top management understands the difference between mitigating cyber risk and working toward a more comprehensive, orchestrated, dynamic cyber-resilience strategy**

CYBER RESILIENCE: What could go wrong?

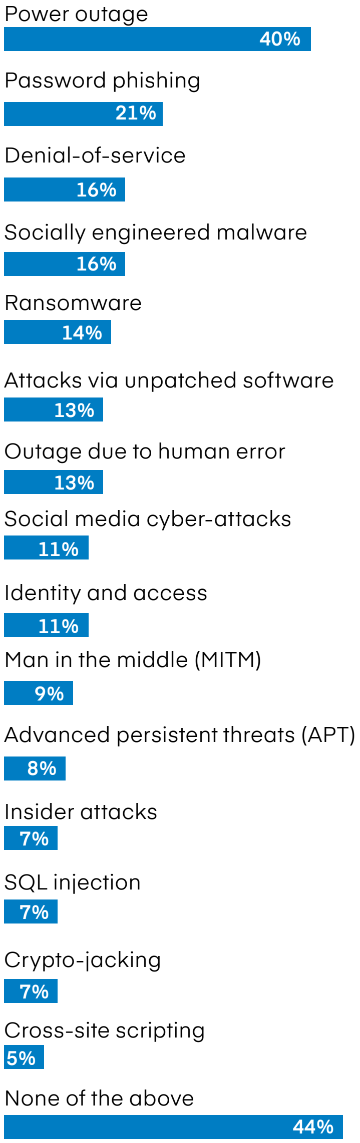
Digital transformation ups the stakes of any cyber event. That is raising the pressure on IT leaders to step up security, but increasing security is not enough to ensure resilience. Cybersecurity by its nature is focused on defending against specific threats and vulnerabilities. Resilience, on the other hand, requires a more holistic and strategic view: What could go wrong, and how would your organization deal with it?

There is no way to defend against every potential cyber threat, just as there is no way to prevent a fire or a hurricane from taking out a power supply or a data center. If your organization suffered a major event, how long could you survive? Only four out of 10 executives in our survey are confident their organization could recover without impacting their business.

More than half of respondents have experienced a cyber event in the past three years. The most widely reported cause was not a particular cyber exploit or criminal activity; it was a power outage. Organizations with a strong resilience profile recognize the need to build in redundancy and prepare. "They've done the table-top exercises and the what-if analysis and developed the readiness to deal with a cyber event," explains Larry Ponemon, founder of the Ponemon Institute, a technology research firm dedicated to helping organizations conceptualize the true cost of a cyber event.

Four out of 10 executives name robust cybersecurity as a top factor in meeting strategic goals. However, building cyber resilience in a hyperconnected environment ranks far lower at 22%, and that worries many executives—particularly IT executives. Four out of 10 also say that hyperconnectivity makes recovery from a cyber event more challenging. Only 27% believe their top management understands the difference between mitigating cyber risk and working toward a more comprehensive cyber resilience strategy.

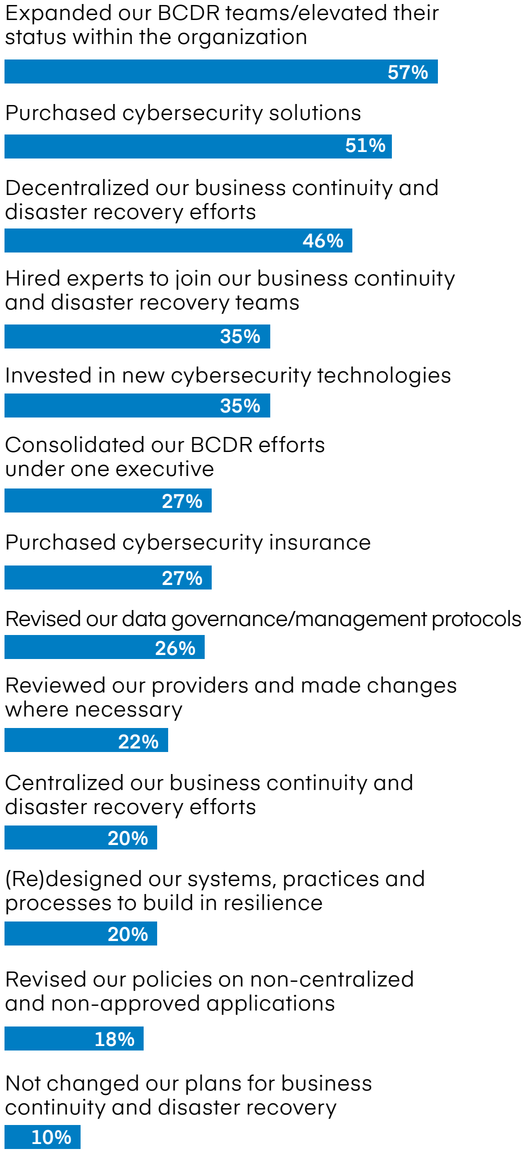
Figure 1. Has your organization been impacted by any of the following cyber events in the last three years?



Only **42%**

are confident their organization could recover from a major cyber event without impacting their business

Figure 2. How did that event change the way your organization plans for business continuity and disaster recovery (BCDR)?



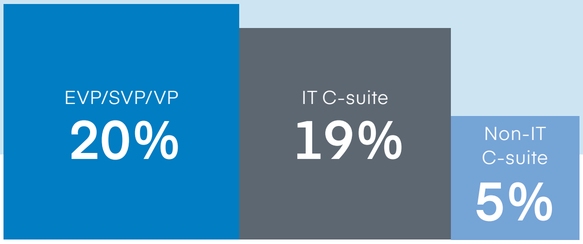
LEADERS LESS CONNECTED TO IT ARE MORE OPTIMISTIC ON SECURITY AND RESILIENCE

Urgency about security and resilience lags among non-technical leadership. C-suite leaders without a technical role are much more operationally focused when evaluating success. Half consider their ability to execute one of the top three factors to determine if they meet their goals, compared with just 21% of IT-driven C-suite positions and 26% of lower-level titles.

In fact, only 5% of non-IT C-suite execs completely agree that because their organization is more hyper-connected than ever, recovery is more challenging, compared with 20% of EVP/SVP/VP executives and a similar percentage of IT C-suite executives.

Non-IT C-suite executives are also more sanguine about how successful their organizations are in integrating resilience into digital strategies. One in five completely agree that resilience is already part of their digital strategy. The view on the ground looks different. Only 9% of IT executives and 11% of executives at the VP level agree completely.

Figure 3. Our organization is more hyperconnected than ever, and that makes recovery more challenging in the face of a cyber event



NOTE: Percentage that completely agree on a scale of 1 to 5, where 1 is completely disagree and 5 is completely agree.

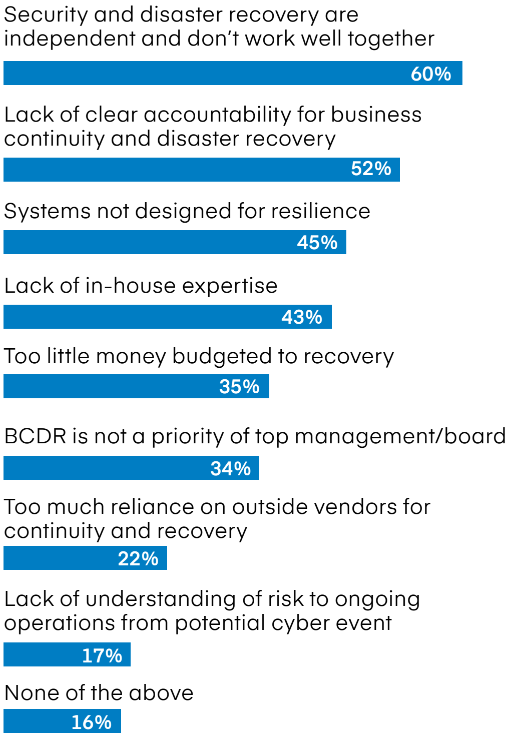
This is reflected in a mismatch between the strategic goals that many organizations put at the top of their list—improving the customer experience and digital transformation—and the always-on technology that is required to reach those goals. Only four out of 10 executives have made cyber resilience integral to their firm's digital transformation.

The main impediments to better resilience are that security and disaster recovery don't work well together (60%) and that there is a lack of clear accountability for business continuity and disaster recovery (52%). There is a wider misperception at many organizations, says James Kaplan, partner and co-leader of IT infrastructure and cybersecurity at McKinsey. “They still think of cybersecurity as a technical issue and not a business issue,” he explains. “What’s more, they often overestimate the purely technical levers they can pull or the things they can do directly within the purview of the security department in contrast to those that would require organizational change.”

SHADOW IT:
You can’t protect what you can’t see

Shadow IT is perceived as a challenge in terms of data protection, and organizations are clearly divided about how to address the threat posed by non-sanctioned devices, applications and software. For line-of-business executives, the democratization of IT means they no longer have to beg, borrow or steal to get the IT department to give them the technology they want, according to Ponemon. Executives can develop and deploy the technology they need with incredible speed. Why wait for someone who doesn’t know your business as well as you do to tell you what you should use?

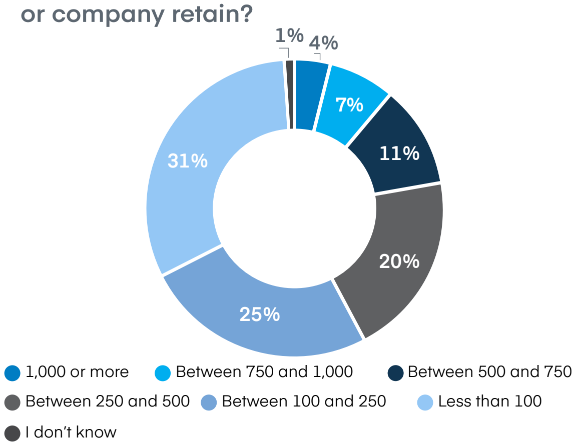
Figure 4. Where do you see impediments to improving your organization’s cyber resilience?



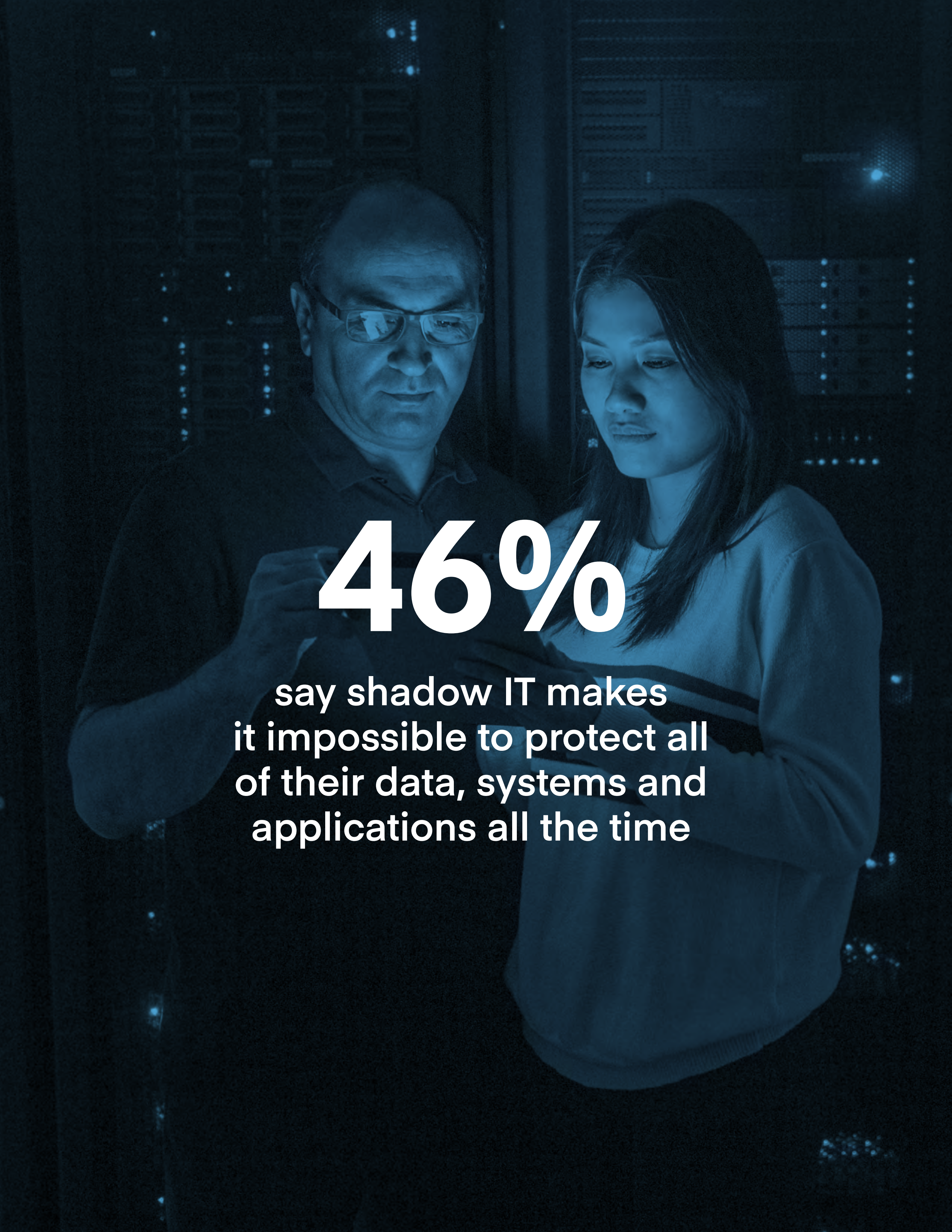
“Many IT decisions are now distributed throughout the organization at the line-of-business level. From a security point of view, it’s a nightmare scenario,” says Ponemon. “People at the business level may not have any knowledge at all about security and be using these tools in ways that put the organization at great risk.” In fact, one in five organizations have experienced a cyber event due to a non-sanctioned IT resource.

Executives say they are having a hard time keeping up with the explosion of non-sanctioned devices, applications and software. Most organizations run more than 100 different applications, but that number may be only a guess. Less than half of executives are confident that they are even aware of all the technology their employees use. In fact, 46% believe that direct purchasing of software-as-a-service, personal and business applications and other non-sanctioned software by individuals and business units makes it impossible to protect all their organization’s data, systems and applications all of the time. Who

Figure 5. Approximately how many applications does your organization or company retain?



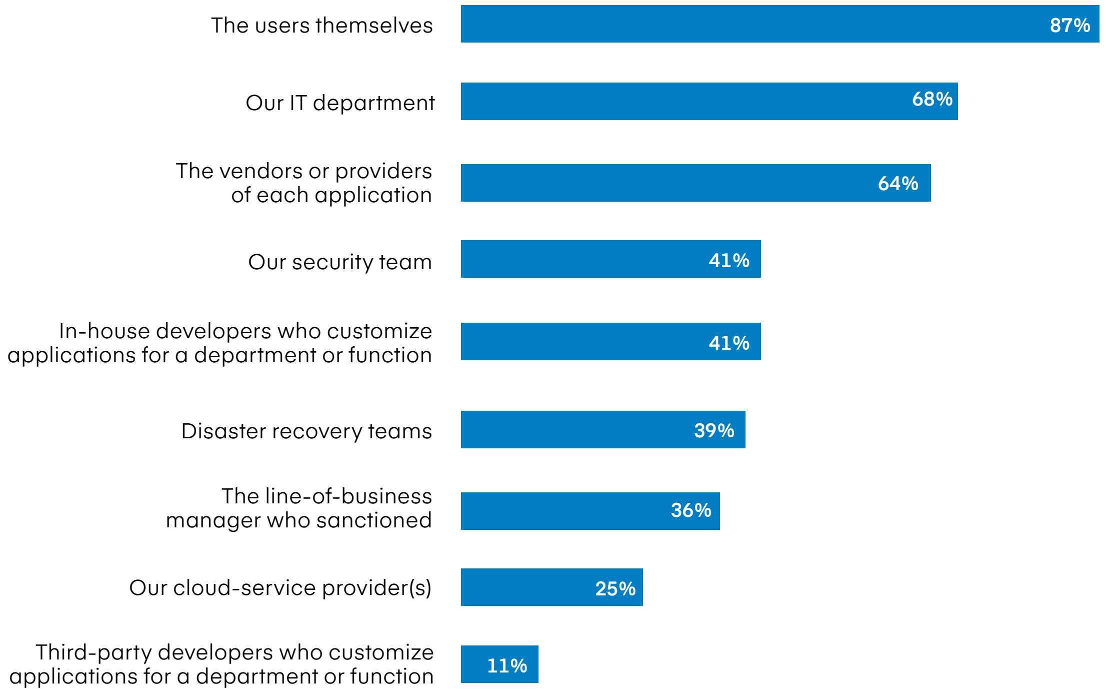
NOTE: Sanctioned and non-sanctioned, including those used by line of business. Does not add to 100% due to rounding.



46%

say shadow IT makes it impossible to protect all of their data, systems and applications all the time

Figure 6. Who do you believe should be responsible for security and recovery when it comes to applications that are not directly supported by your organization's IT function?



NOTE: Respondents could choose all that apply.

should be responsible if something goes wrong? Nearly everyone (87%) believes that the users themselves should be responsible for security and recovery if they use non-sanctioned applications, but many also believe the IT department should bear some responsibility, as should application vendors, developers, and security and disaster recovery teams.

The most popular means to protect against non-sanctioned IT include network monitoring, guidelines for devices, cloud-services and third-party applications as well as restricted access to some insecure third-party applications—a black list of insecure devices, applications and cloud-services. A zero-trust policy for anyone logging in to sensitive parts of the network is not as popular. In the future, more organizations may turn to machine learning to flag unusual log-in activity to deny access.

Executives are not optimistic that they are doing enough. Fewer than half believe their organization is aware and responsive to the potential risks and vulnerabilities

Figure 7. What policies and protections does your organization employ toward shadow IT?

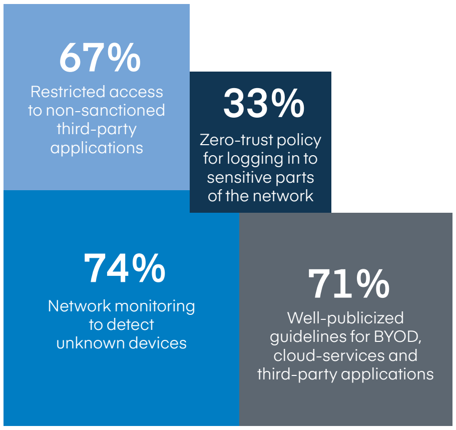
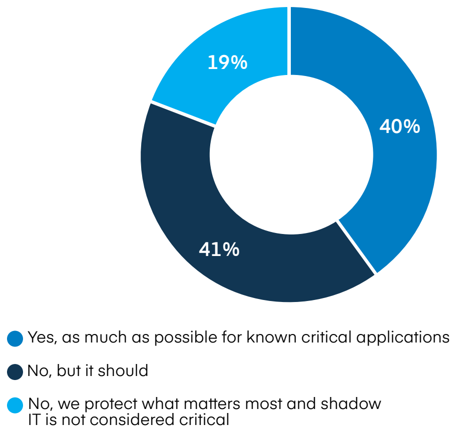


Figure 8. Does your organization's threat/risk assessment include shadow IT?



of shadow IT. Six out of 10 organizations don't include known, critical, shadow IT in their threat assessments, even though they believe that they should, say 41%.

"There are a lot of turf issues when it comes to shadow IT," explains Ponemon. "There are decisions made that can really influence other business units, and there's not a lot of information sharing that goes on. To conquer resilience issues in the world of shadow IT requires more collaboration internally, not making the line of business the bad guy," he says.

Figure 9. Did your cloud-service provider meet service-level agreements following an incident involving downtime or lost data?

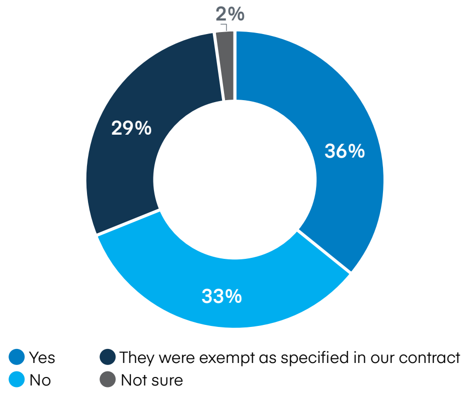
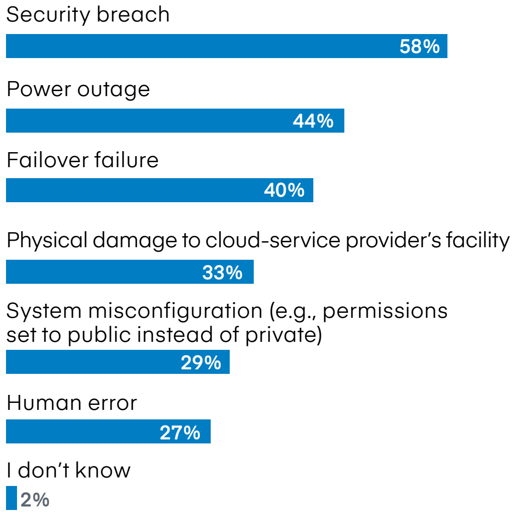


Figure 10. What was the cause of the incident?



AVAILABILITY COVERAGE BY CLOUD-SERVICE PROVIDERS: Who bears the true cost of a cyber event?

Cloud-service providers promise a level of security and availability, yet more than half of the respondents doubt that cloud-service providers can meet service-level agreements during cyber events. Who bears the cost for a cyber event that begins in the cloud? For the 13% of executives who have lost data or faced downtime due to incidents with their cloud-service provider, more than half were not compensated by their providers. Most incidents were the result of a security breach.

A majority of organizations (65%) rely on their cloud-service providers' guarantees of security, recovery and continuity, yet only 45% are confident their providers can meet service-level agreements in a cyber event. If a cloud-service provider is

65%

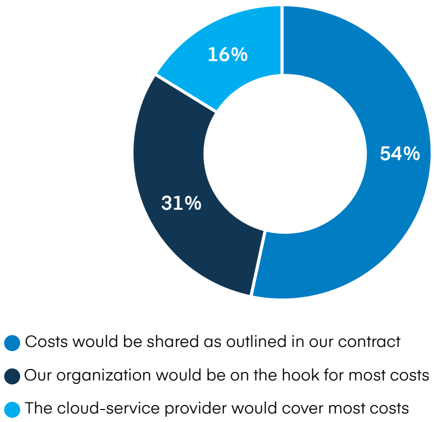
rely on their cloud-service providers’ guarantees of security, recovery and continuity

Yet only

45%

are confident their providers can meet service-level agreements in a cyber event

Figure 11. If a cloud provider is responsible for an outage or a breach and service-level agreements are not met, who would bear the cost for recovery, downtime and any monetary or reputational loss?



NOTE: Does not add to 100% due to rounding.

responsible for a breach or an outage, 85% of executives believe their organization would bear some or all of the costs for recovery, downtime and any monetary or reputational loss.

It is clear that there is not a lot of confidence that cloud-service providers can provide the security that many organizations believe they should. In fact, security and resilience at the biggest cloud providers far outmatch what most organizations could provide for themselves, according to Kaplan at McKinsey. Major cloud providers have the scale to build multiple redundancies, and they can form a vanguard for detecting new threats.

In a recent study, Kaplan and his colleagues looked for examples of breaches but couldn't find any examples where the cloud provider had been compromised. "But we found lots of cases where a developer had misconfigured their environment and left it wide open," he says. For example, one CIO was fond of giving developers unfettered access. "It was like giving a machete to a toddler," explains Kaplan. "His developers did not understand enough about security to be given that kind of access."

Security in the cloud is a shared responsibility, and migrating to the cloud disrupts the traditional cybersecurity models that companies have built up over years. For Kaplan, it's not a question of whether or not the cloud is secure but whether or not organizations can consume the cloud in a secure way. A power outage is a leading cause of outage for cloud-service. "No major cloud provider will guarantee the absence of downtime, but they will say that if you write your app the right way, it can fail over to multiple regions, and there has never been an outage in more than one region at one time," he explains. Organizations also must ensure that they meet data regulation requirements when failing over.

Even for organizations that understand how to design and architect their system for a safe migration to the cloud, they face a backlog of decades worth of applications that don't necessarily comply with that standard. Access is another issue that requires rethinking for applications in the cloud. "If you make it too hard, people will forget their passwords and have to reset them," says Ponemon. That can add frustration for workers and partners as well as customers, who may simply take their business elsewhere. If convenience is improved, security

Figure 12. Does your organization incorporate cloud-service providers in your threat/risk assessment?

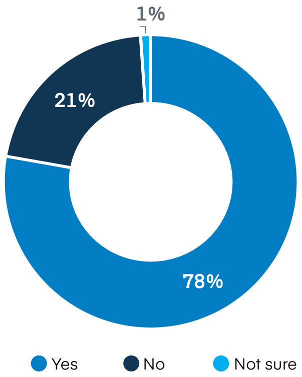
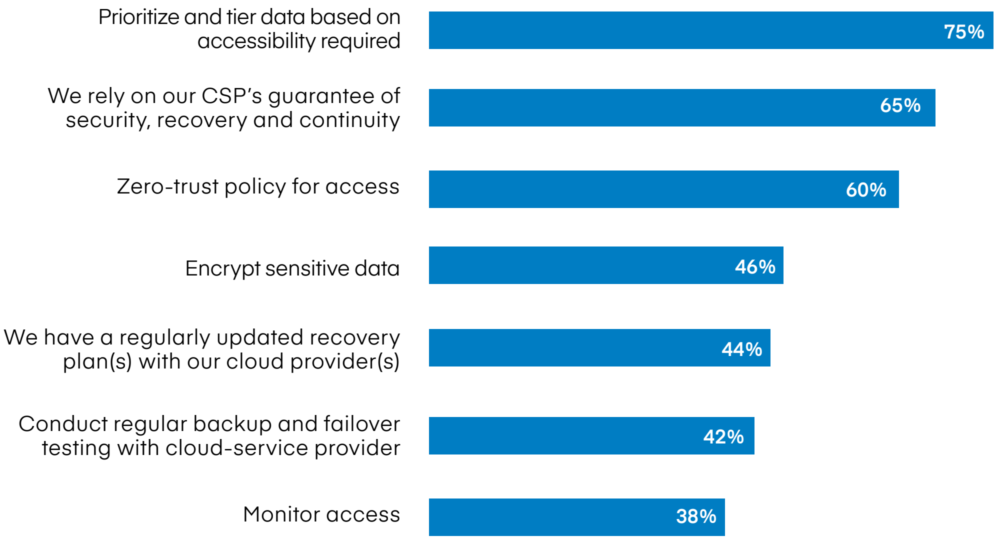


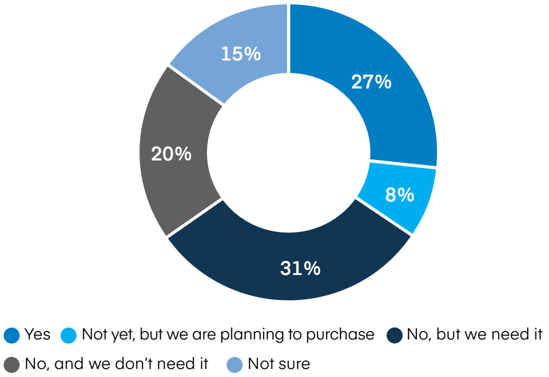
Figure 13. How does your organization secure data in the cloud?



could be diminished. "Balancing those concerns in the world of cloud computing has become very important," he says.

Organizations are taking a proactive approach to resilience in the cloud. Three-quarters say they include their cloud-service providers in their threat assessment, and nearly half say they have a regularly updated recovery plan with their cloud providers. Many also conduct regular backup and failover testing with cloud-service providers.

Figure 14. Does your organization have cyber insurance?



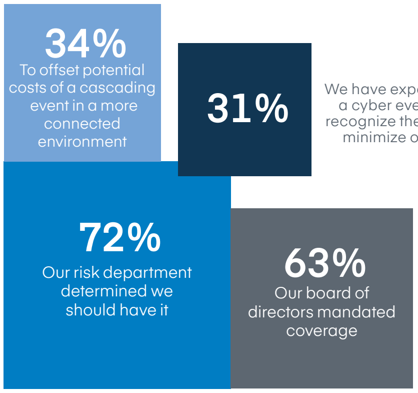
NOTE: Does not add to 100% due to rounding.

CYBER INSURANCE: Read the fine print

Cyber insurance is very hard to underwrite. For insurers, cyber risk has a very long tail. The true cost of a significant breach can easily reach into the hundreds of millions. Insurance companies have managed their risks with relatively low caps and broad exclusions. Remediation costs and notification costs might be covered, at least in part. But what about reputational damage, loss of IP or forensics? Most insurers are simply not willing to underwrite those risks because they don't have the data to calculate them yet.

It's no surprise then that cyber insurance is not commonly used. Less than three out of 10 organizations (27%) carry cyber insurance, a decision largely mandated by their boards (63%) and their risk departments (72%).

Figure 15. What are the most important reasons that your organization initiated or will initiate insurance coverage?



For organizations that would like to insure some of their cyber risks, there is confusion about what is covered—and frustration if they discover they don't have the coverage they thought they had. Some of the biggest breaches of customer data in recent years happened at organizations that carried insurance, but that insurance paid out only a fraction of what those organizations believed they were entitled to receive.

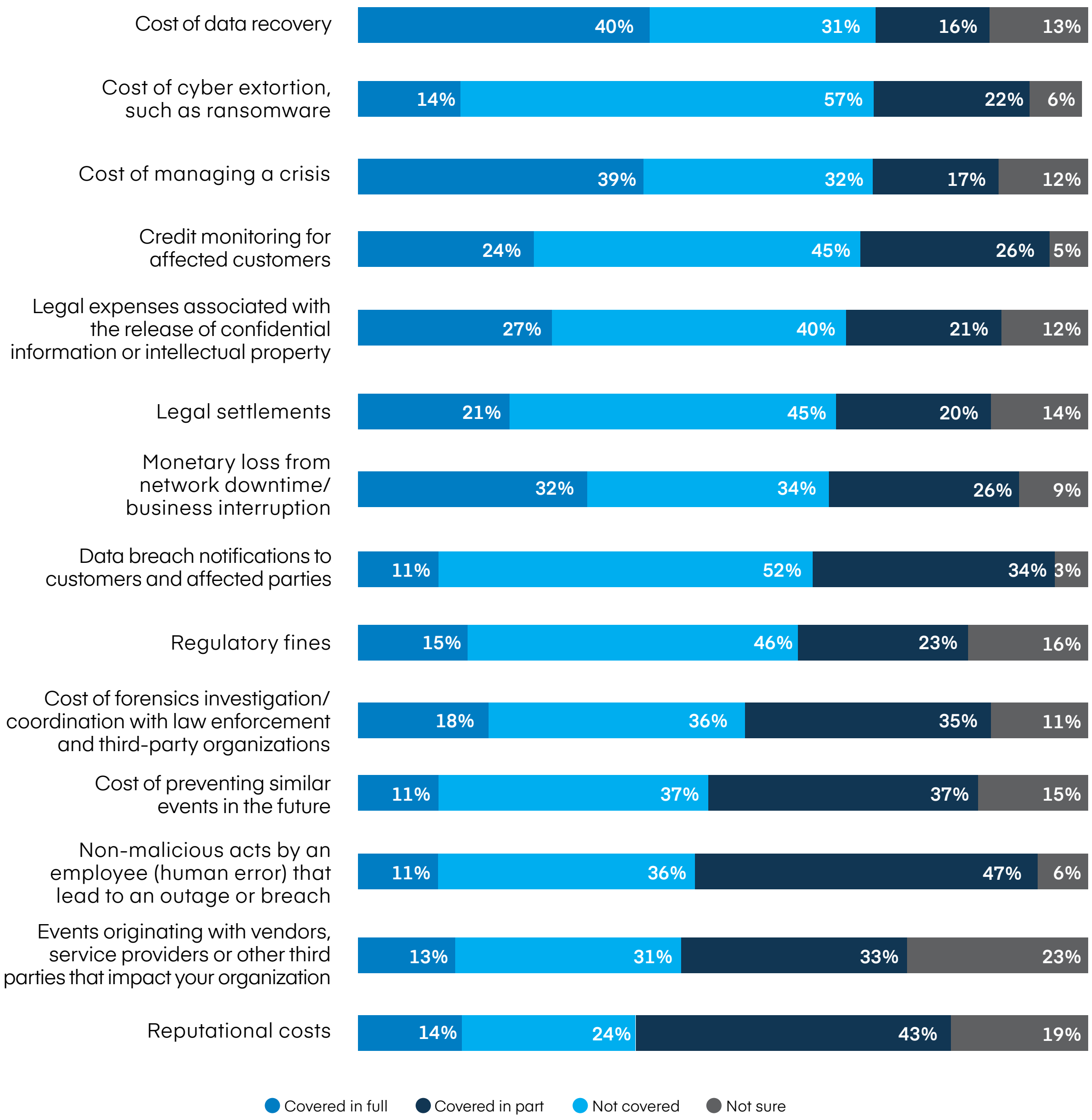
Among the executives who purchased cyber insurance, only four out of 10 believe that the costs of data recovery and crisis management are covered in full. Most executives recognize that their organizations would be on the hook for costs associated with legal expenses, regulatory fines, an outage caused by human error—traditionally the most common cause for an outage—and other common losses after a cyber event.

“There has been some disappointment in the marketplace sometimes because people thought they were buying a policy that gave them some protection only to find out it didn't,” says Ponemon. One potential perception gap comes from the self-assessment of cyber hygiene that insurers require. This is covered in the fine print, which can run to several hundred pages.

“If a CISO rates his or her organization highly and it turns out that assessment wasn't really true, coverage can be denied,” he explains. “If your data center is down a certain number of days, for example, it probably means you didn't have the right redundancy.” It gives the insurance company room to wiggle out or reach a settlement that's less than the full cost.

> “
> **There has been some disappointment in the marketplace sometimes because people thought they were buying a policy that gave them some protection only to find out it didn't....If a CISO rates his or her organization highly and it turns out that assessment wasn't really true, coverage can be denied. If your data center is down a certain number of days, for example, it probably means you didn't have the right redundancy.”**
>
> **LARRY PONEMON,**
> FOUNDER, PONEMON INSTITUTE

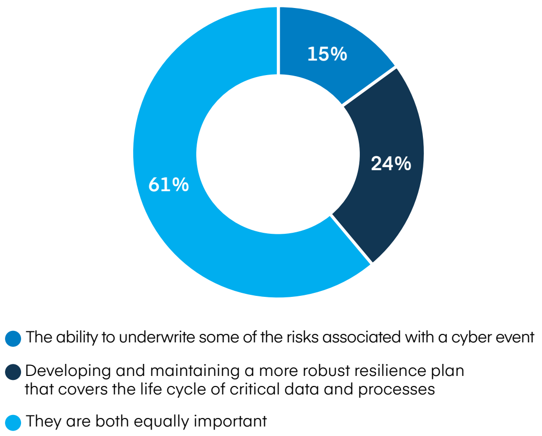
Figure 16. Which costs and incidents do you believe are covered by your cyber insurance policy?



One recent case involved a massive data breach. The insurance company did a postmortem on the breach and discovered that customer data was not properly encrypted. In this case, the company at fault displayed a distressing complacency toward encryption, in part because it was insured against losses. The insurance company refused to pay.

There is a need for greater transparency on the part of insurers, but organizations must also be honest about their standards and practices. Ironically, Ponemon's research shows that companies with a strong security posture are more likely to buy insurance. "Philosophically, they see it as a complement to current security rather than an

Figure 17. Which do you believe is most important to minimizing the impact of a cyber event?



alternative," he explains.

Most executives (61%) believe that developing and maintaining a robust resilience plan is just as important as the ability to underwrite some of the risks associated with a cyber event. A quarter believe that when it comes to minimizing the impact of a cyber event, resilience is paramount.

CONCLUSION

In the hyperconnected organization, cyber resilience needs to be as diverse, dynamic and dispersed as the data and systems that run that organization. Blind spots when it comes to shadow IT, maintaining resilience in the cloud and cyber insurance coverage may be creating a false sense of security for decision makers and hindering the development of a more robust, life-cycle plan for resilience.

To cover the blind spots and perception gaps in cyber resilience, organizations must develop a clear understanding of who is responsible for what.

Better communication: When it comes to shadow IT, users and line-of-business managers need to be part of an overall resilience plan. Turf issues could put the organization at risk.

Trust but verify: Migrating to the cloud involves a certain level of trust when it comes to a cloud provider's security controls. But organizations should not be dependent on vendors to provide all necessary controls or some responsibilities could fall through the cracks. Organizations must recognize the extent of their provider's responsibilities by first understanding their provider's security operating model and then enforcing a clear view of who is responsible for cloud security among users, developers and anyone who has access.

Know your risks: Insurance is no substitute for a strong resilience posture. Insurers can—and will—refuse to cover events that could have been avoided. No organization can avoid all cyber risk, but they can prepare for a number of what-ifs by creating adequate redundancies, practicing disaster scenarios and ring-fencing critical systems. For specific risks that cannot be avoided, cyber insurance may be a good option—but read the fine print.

METHODOLOGY

In the fourth quarter of 2018, Forbes Insights surveyed 353 executives across the globe about their outlook on cybersecurity and resilience at their organizations. Three out of five are from the C-suite (including 17% CIOs, 9% CTOs and 8% CISOs), while 40% are at the VP-level in functions related to IT operations, business continuity or disaster recovery. A wide range of industries are represented, including 10% from banking; 9% from telecom, media and entertainment; 7% from automotive; 7% from insurance; and 7% in healthcare. All organizations have at least $500 million in revenue, while three-quarters have at least $1 billion in annual revenue. This report was published in 2019.

ACKNOWLEDGMENTS

Forbes Insights and Kyndryl would like to thank the following individuals for their time and expertise:

- **James Kaplan,** Partner and Co-Leader of IT Infrastructure and Cybersecurity, McKinsey & Co.
- **Larry Ponemon,** Founder, Ponemon Institute

Forbes insights

Forbes Insights is the strategic research and thought leadership practice of Forbes Media, a global media, branding and technology company whose combined platforms reach nearly 94 million business decision makers worldwide on a monthly basis. By leveraging proprietary databases of senior-level executives in the *Forbes* community, Forbes Insights conducts research on a wide range of topics to position brands as thought leaders and drive stakeholder engagement. Research findings are delivered through a variety of digital, print and live executions, and amplified across *Forbes*' social and media platforms.

EDITORIAL & RESEARCH

Erika Maguire
EXECUTIVE EDITORIAL DIRECTOR

Kasia Wandycz Moreno EDITORIAL DIRECTOR

Hugo S. Moreno EDITORIAL DIRECTOR

Ross Gagnon RESEARCH DIRECTOR

Scott McGrath RESEARCH ANALYST

Deborah Orr REPORT AUTHOR

Zehava Pasternak DESIGNER

PROJECT MANAGEMENT

Tori Kreher
PROJECT MANAGER

Brian Lee
PROJECT MANAGER

Todd Della Rocca
PROJECT MANAGER

SALES

North America
Brian McLeod VICE PRESIDENT
bmcleod@forbes.com

Matthew Muszala EXECUTIVE DIRECTOR
mmuszala@forbes.com

Europe
Charles Yardley SVP MANAGING DIRECTOR
cyardley@forbes.com

Asia
Will Adamopoulos
PRESIDENT & PUBLISHER, FORBES ASIA
wadam@forbesasia.com.sg