



# Why It's Critical for Businesses to Implement a Cyber Resilience Framework

An IDC eBook, sponsored by Carbonite and Webroot

WRITTEN BY:



**Michael Suby**  
Research Vice President,  
Security & Trust



**Katie Evans**  
Research Director,  
Worldwide Small and Medium  
Business Research



**Frank Dickson**  
Program Vice President,  
Cybersecurity Products

January 2022




**opentext™** | Cybersecurity

# Introduction

Cyber resilience, the ability to maintain business operations in the face of unending and evolving cyber threats, can be an intimidating topic for any business. Adding to the challenge is the complexity of companies' IT footprints — which today are often a distributed web of cloud applications, private servers, and employee devices. Critical data, the currency of business, is spread across this footprint and stored in documents, spreadsheets, electronic communications, and databases. This data powers business. When access to data is disrupted, as with a ransomware attack, the implications can be crippling.

Being cyber resilient doesn't have to be so intimidating. Rather than manage all aspects of cyber resilience in-house, companies of all sizes are turning to outside vendors who are experts in their fields for guidance, assistance, and implementation of cybersecurity technology. Often this is to compensate for internal limitations in time, expertise, and cybersecurity technologies that could leave these companies exposed to cyberattacks and unprepared to recover if an attack were to occur.

Still, some companies choose a riskier approach. Rather than recognize and offset their limitations in time, talent, and technology, they roll the dice and only partially address cybersecurity risks and the potential impact on their companies' cyber resilience. Unfortunately, but logically, this leaves them more exposed to cyberattacks, and, when unprepared, without a solid recovery plan. This often means the business consequences of cybersecurity incidents are more severe, and the time to return to normal business operations is longer.

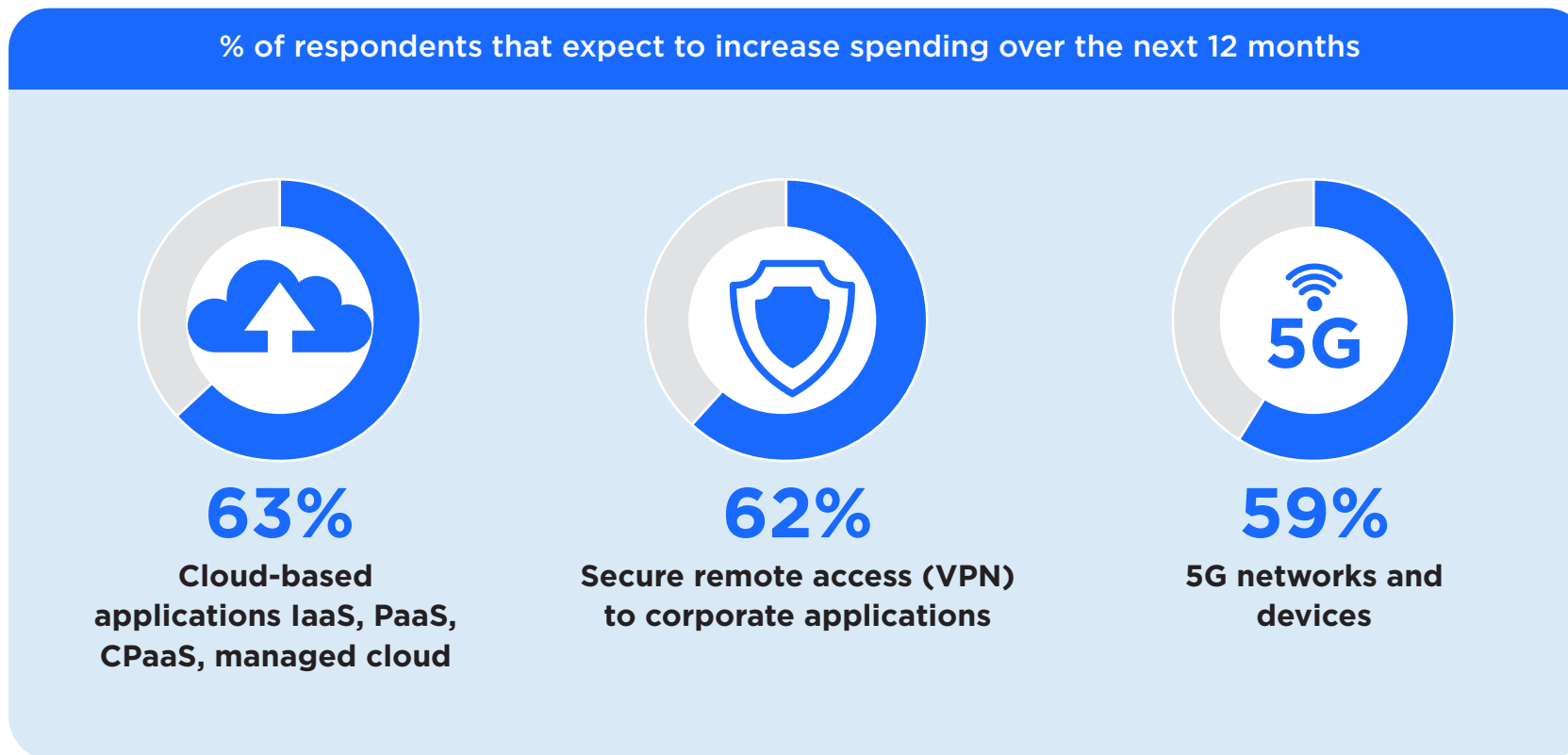


This does not have to be the status quo. There are steps that can strengthen your cyber resilience — internally or with the assistance of outside vendors. **These steps form the cyber resilience framework.**

# Why Should My Company Care About Cyber Resilience?

## A Distributed IT Footprint Brings Greater Risk

Before the pandemic, companies were already migrating to the cloud and operating with an at least partially remote workforce. With the pandemic, cloud migration accelerated and remote work shifted from pockets of employees to entire organizations. As a result of COVID-19, many organizations have increased their reliance on cloud services, and this is likely to continue. Additionally, many companies will continue to operate with a heavily remote workforce after the pandemic. Findings from IDC's 2021 *Future of Connectedness Survey* illustrate that more than 60% of companies plan to increase spending on both cloud-based applications and technologies to support secure connectivity for remote and mobile workforces.



This dispersed but highly connected workforce is a boon for cyberattackers, as it provides more entry points into companies' IT systems, critical applications, and sensitive data. In addition, remote employees work outside of cyberprotected offices. Each remote employee essentially operates as an office of one, connecting to business applications through a local network (a home network, for example) that is not managed by IT, opening up more vulnerabilities for businesses. As a result, protection against cyberattacks is only as strong as each connecting remote employee.

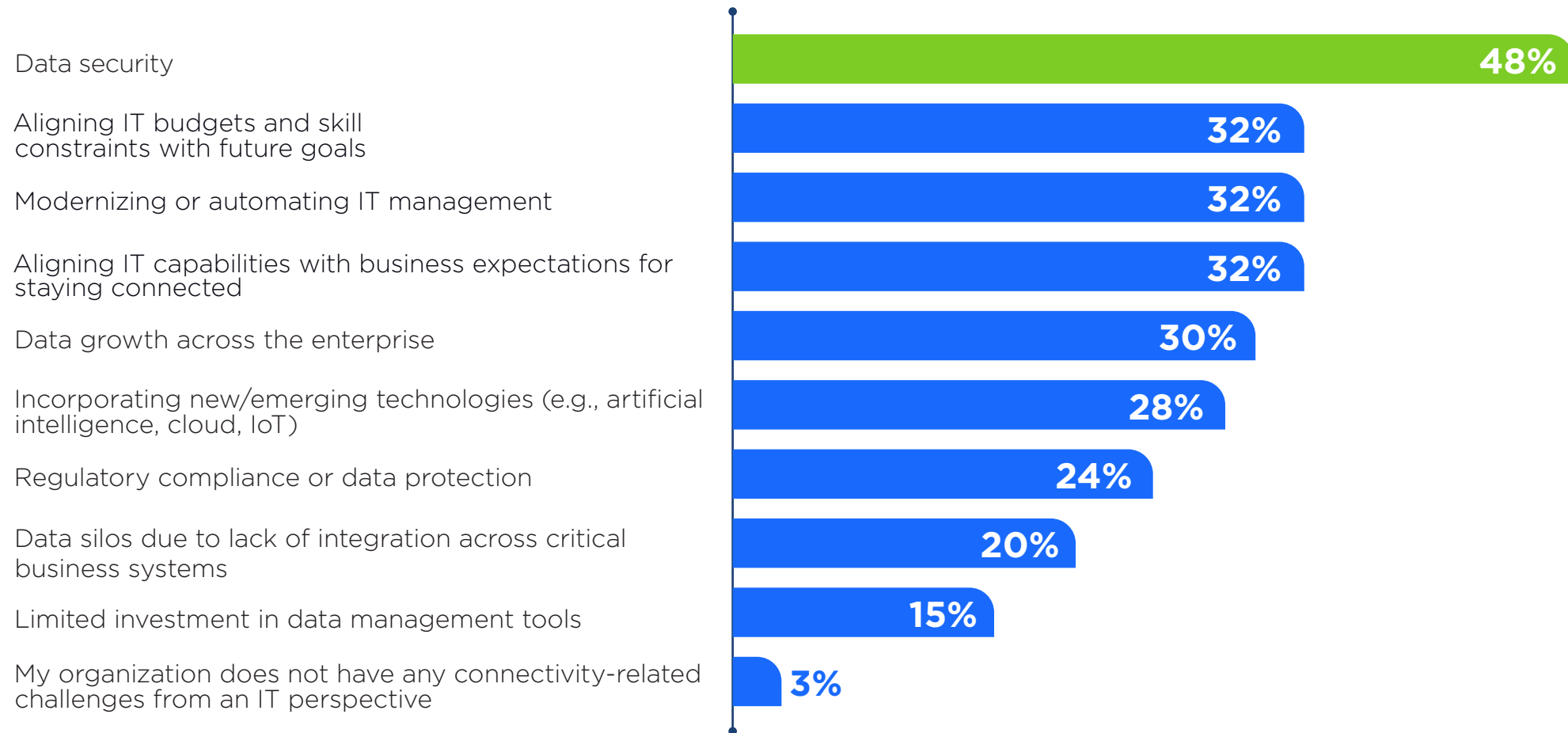
n = 607, companies with 500 or more employees

Source: IDC 2021 *Future of Connectedness Survey Findings: Agility and Resiliency Drive Investments Across All Areas of Enterprise Connectivity*

Most IT professionals are already aware that greater connectedness elevates security risk. And it's worth noting that data security and protecting the integrity of networks are among the top challenges faced by individuals in IT or networking roles, according to IDC's *2021 Future of Connectedness Survey*.

**Q: From an IT perspective, what are the top three connectivity-related challenges that your organization currently faces?**

(% of respondents)



n = 607, companies with 500 or more employees

Source: IDC *2021 Future of Connectedness Survey Findings: Agility and Resiliency Drive Investments Across All Areas of Enterprise Connectivity*



**Q: From a network perspective, what are the top three connectivity-related challenges your organization currently faces?**

(% of respondents)

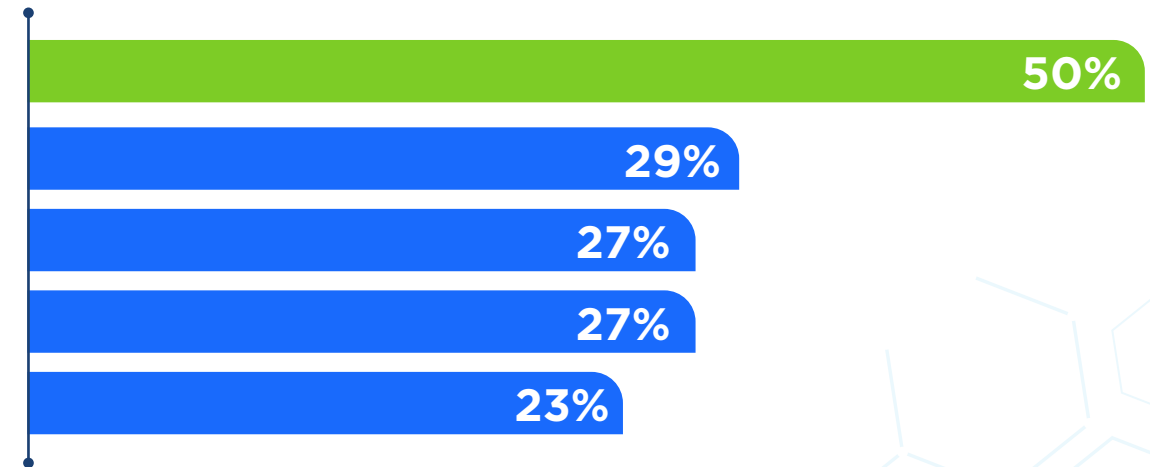
**Network security** — ensuring that corporate networks are protected against rogue actors, viruses, and DDoS issues

**Incorporating new technologies** — determining business needs and benefits of emerging networking technologies (e.g., WiFi 6, SD-WAN, cloud)

**Geographic connectivity** — ensuring adequate connection between offices across our geographic footprint

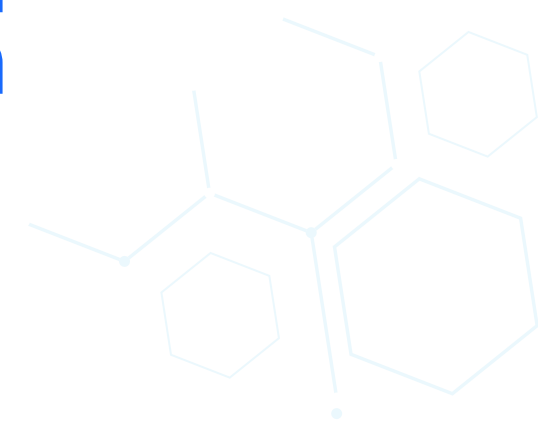
**Agility** — transforming network to be more virtualized, scalable, and agile

**Speed/performance** — managing latency issues with WAN (i.e., 4G/5G, SD-WAN)



n = 607, companies with 500 or more employees

Source: IDC 2021 Future of Connectedness Survey Findings: Agility and Resiliency Drive Investments Across All Areas of Enterprise Connectivity



# IT Is Stretched Over a Lengthy List of Priorities

Businesses of all sizes grapple with lengthy lists of technology priorities. Case in point, IDC's *Worldwide Small and Medium Business Survey, 2020*, reveals a range of technology priorities for small and medium businesses (SMBs) — spanning multiple disciplines including security, networking, device management, employee helpdesk, and cloud migration. With so many priorities, many of which are compounded by increased reliance on the cloud, a larger remote workforce, and few dedicated IT personnel, many SMBs struggle to develop and maintain strong cyber resilience.

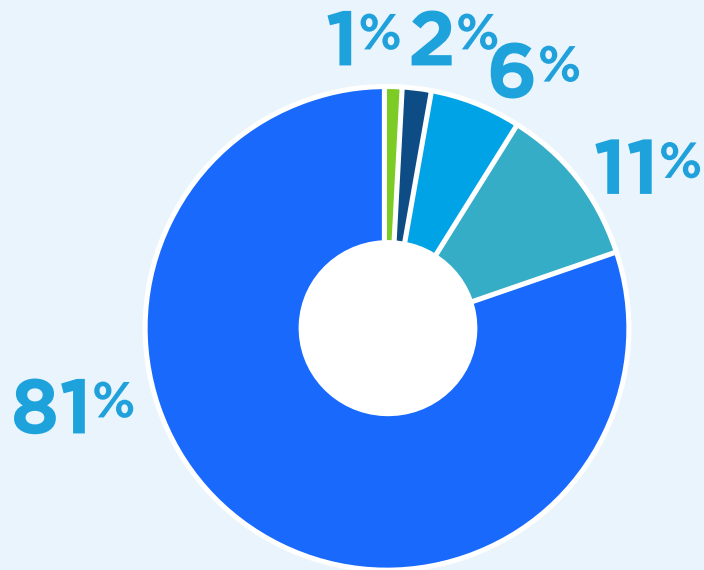


## Did You Know:

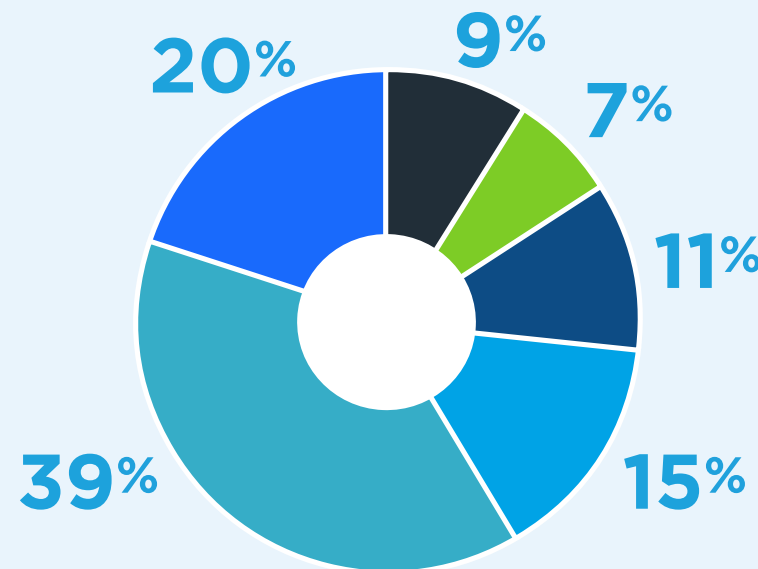
The number of full-time IT staff members available to support these priorities averages less than 2% of an SMB's total employee base.

**Q: Approximately how many full-time people (or equivalents) are in your IT department, including managers?**  
(% of respondents)

**All Small Business (1-99)**



**All Medium Business (100-999)**



**Number of full-time people in IT department:**

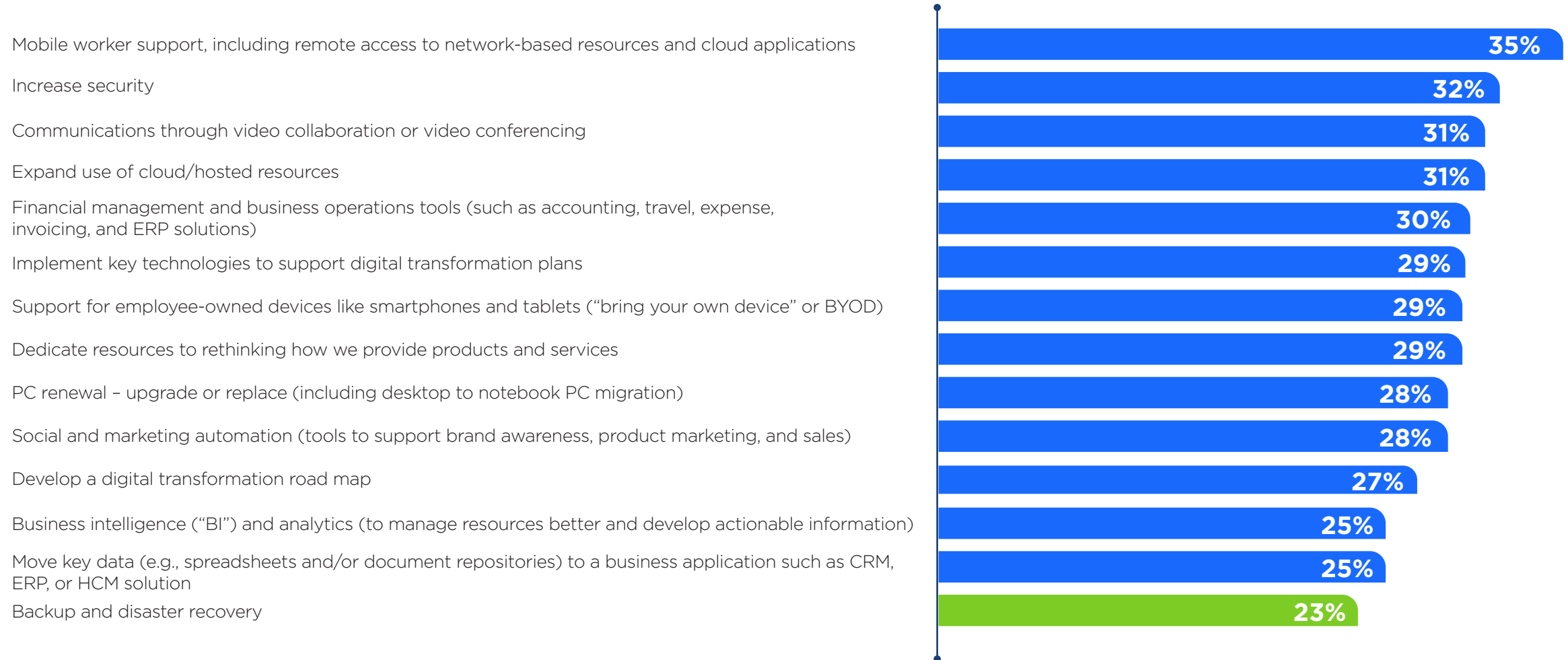
- 1
- 2
- 3
- 4
- 5
- 6-10

n = 1,383 (494 small businesses (fewer than 100 employees) and 889 mid-sized businesses (100-999 employees))  
Source: IDC 2020 WW SMB Technology Buyer Survey, 2021

While security is the second most popular technology priority for SMBs, listed as a priority by 32% of SMBs, only 23% of SMBs specifically listed backup and disaster recovery as a technology priority for the next 12 months — showing there's still room for cyber resilience improvement.

**Q: Which of the following will be technology priorities for your company in the next 12 months?**

(% of respondents)



n = 2,463 (1,520 small businesses (fewer than 100 employees) and 943 mid-sized businesses (100-999 employees))

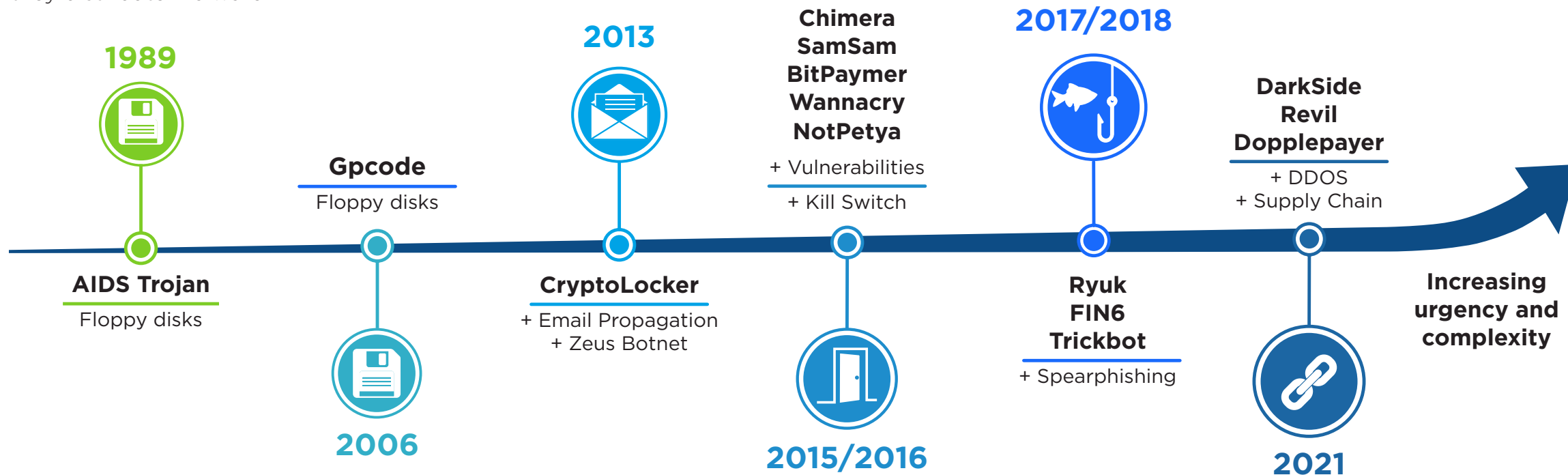
Source: IDC 2020 WW SMB Technology Buyer Survey

# Crippling Cyberattacks Are on the Rise

Increased cloud adoption, disparate workforces, and the many changes necessary to undergo digital transformation put today's business leaders in a precarious position. Digital transformation has deepened companies' digital dependencies, and the distributed and connected network of employees and IT systems that represent critical business operations are companies' Achilles heel. Disruption to just one of a company's many digital connections can produce devastating business consequences.

What's more, savvy threat actors are also aware of and are leveraging the precarious positions companies find themselves in. Ransomware attacks are a prime example. Through ransomware attacks, bad actors extort payments from companies by holding their digitized operations and, more recently, exfiltrated sensitive data, hostage.

Ransomware attacks have a lengthy and infamous history. Since their debut in 1989, these attacks have evolved, becoming more sophisticated in how they distribute malware.



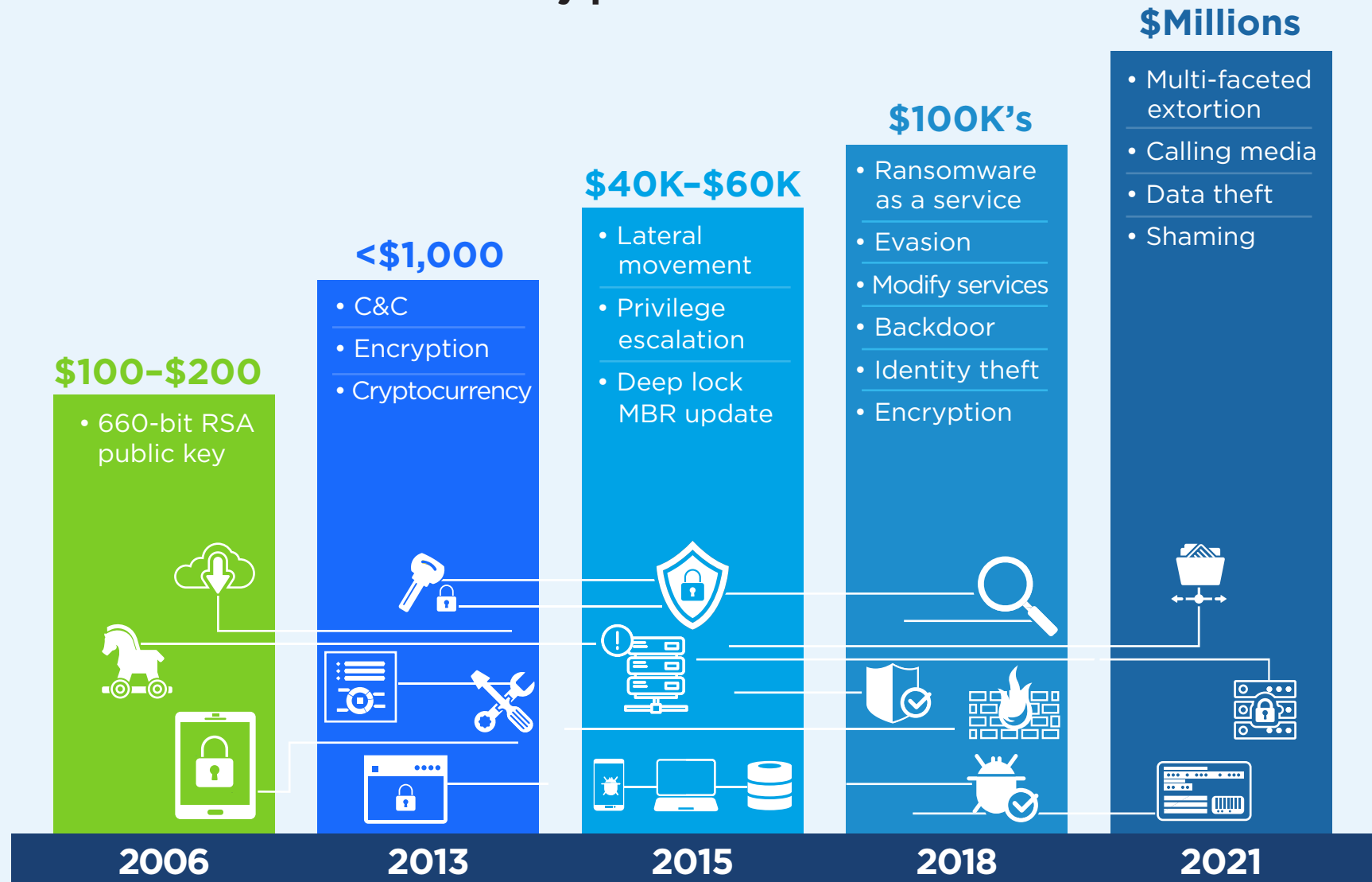
Source: IDC Market Analysis Perspective: Worldwide Data Security, 2021



The pace of innovation in the targeting and distribution of ransomware has been equaled by the technical innovation of the malware itself. Early improvements to malware, including stronger encryption, have been key to ransomware's effectiveness. Additionally, cryptocurrency introduced anonymous monetization. Stronger and more effective encryption and anonymous monetization have enabled ransomware's evolution.

Cyber miscreants later discovered that the willingness of the victim to pay a ransom and the amount that the victim is willing to pay is tied to the encrypted data's importance to the victim's operations, regulatory requirements, and brand. Thus, ransomware attackers began increasing their use of techniques such as lateral movement attacks, credential harvesting, and privilege escalation to find, exfiltrate, and take control of the targeted victim's high-value data. As a result, ransom demands and payment amounts have increased, particularly over the last three years.

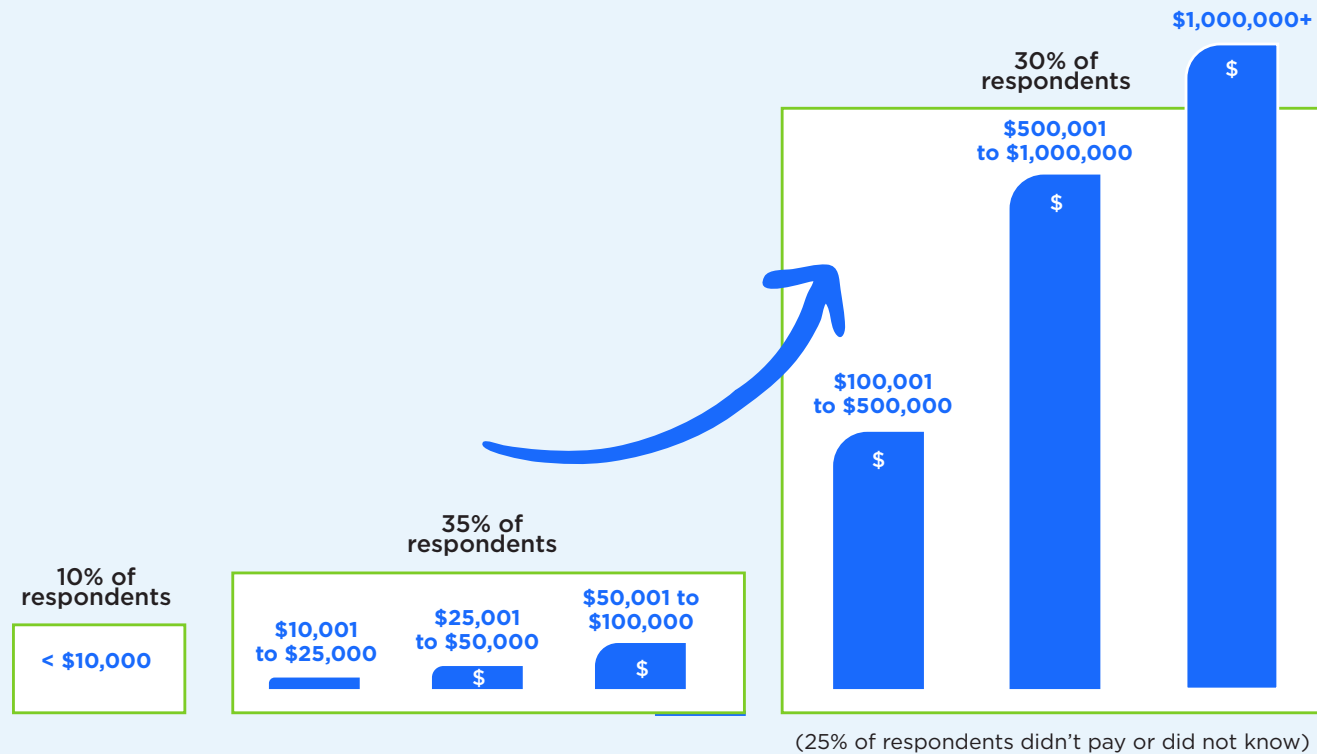
## Growing sophistication driven higher by profit motive



Source: IDC Market Analysis Perspective: Worldwide Data Security, 2021

**Q: If your organization paid one or more ransom payments in the past 12 months to regain access to systems or data, how much was paid in total?**

(% of respondents)



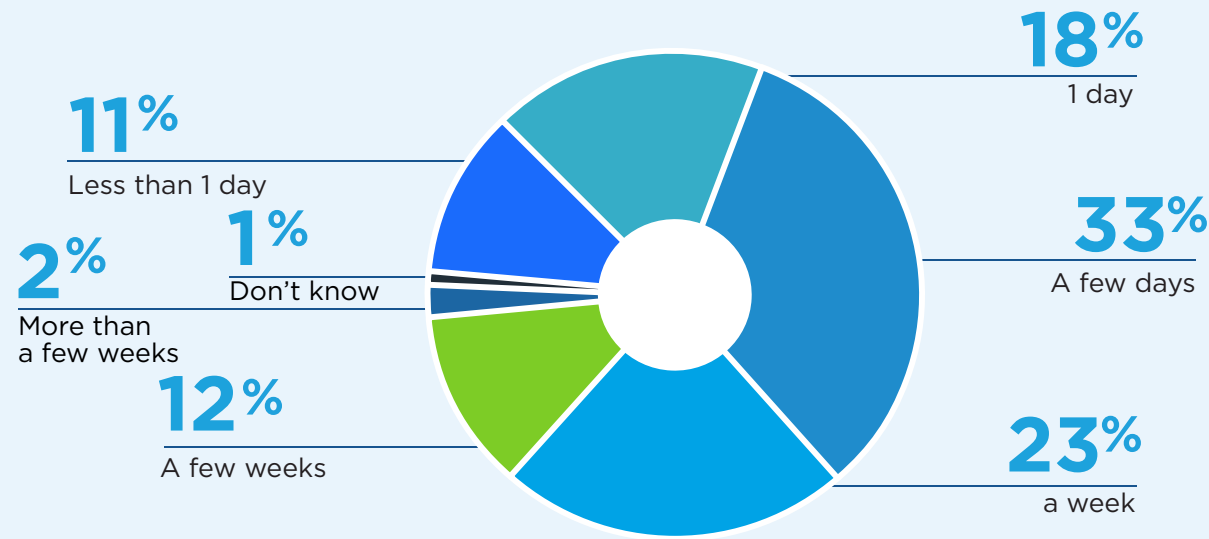
**Did You Know:**

Combining IDC's survey findings on the frequency of ransomware attacks with the distribution of ransom payments, 13% of businesses with 500 or more employees experienced a ransomware attack and paid a ransom of between \$50,000 and \$1 million to regain access to their data and systems.

n = 292, Sources: IDC, *Future Enterprise Resiliency & Spending Survey Wave 6*, July 2021, IDC's *2021 Ransomware Study: Where You Are Matters!*

Ransom payments, however, provide only a partial picture of the total business cost of ransomware attacks. Businesses also often incur significant costs related to the direct and indirect expenses of business disruption. According to IDC's *Future Enterprise Resilience & Spending Survey Wave 6*, more than a third of companies that experienced a ransomware incident reported business disruption of a week or longer.

**Q: For your most recent ransomware incident, how many days was business disrupted?**  
 (% of respondents)



n = 199, Sources: IDC *Future Enterprise Resiliency & Spending Survey Wave 6*, July 2021, IDC's *2021 Ransomware Study: Where You Are Matters!*

It's also important to understand that paying a ransom doesn't guarantee that the company will regain full access to its data or that business operations will be quickly restored. In addition, single ransomware incidents are actually rare. In many instances, a company sustains one or more ransomware attacks and must invest significant time and money to recover.

**Q: Over the past 12 months, which statement best reflects your organization's experience with exposure to and defense against ransomware?**  
 (% of organizations that encountered ransomware)

We experienced 10 or more ransomware incidents requiring significant extra resources to rectify

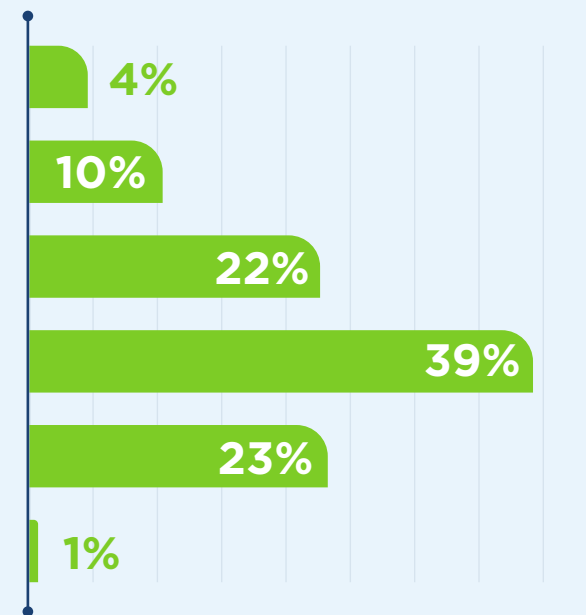
We experienced 5-9 ransomware incidents requiring significant extra resources to rectify

We experienced 3-4 ransomware incidents requiring significant extra resources to rectify

We experienced 1-2 ransomware incidents requiring significant extra resources to rectify

We experienced only minor ransomware incidents: remediation was handled by internal staff and did not involve spending significantly on extra resources to rectify

Don't know/unable to respond



n = 156, Sources: IDC Future Enterprise Resiliency & Spending Survey Wave 6, July 2021, IDC's 2021 Ransomware Study: Where You Are Matters!

Furthermore, the impacts of ransomware attacks do not end when a business recovers its data. Seventy-five percent of companies that encountered a highly visible ransomware incident required post-incident steps to assess and, as warranted, improve their company's data protection and recovery practices.

**Q: Over the past 12 months, which statement best reflects your organization's experience with exposure to and defense against ransomware?**

(% of respondents)

We conducted an organization-wide review of our current security and data protection/recovery practices based on publicly available lessons learned, and initiated product/process changes

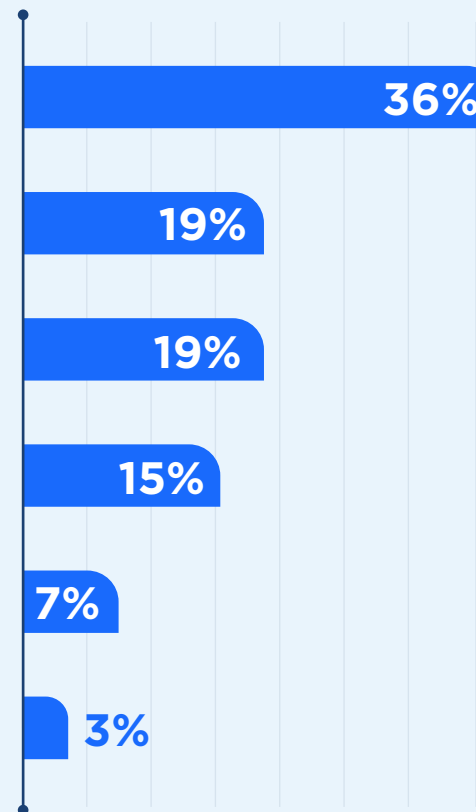
We conducted a formal organization-wide review of our current security and data protection/recovery practices based on publicly available lessons learned, but no changes were required

We contracted with an external services provider to audit and update our security and data protection/recovery practices

We haven't considered/taken any actions

We decided that there was no need to review or update our current security and data protection/recovery practices

Don't know



n = 296, IDC Future Enterprise Resiliency & Spending Survey Wave 6, July 2021  
 Source: IDC's 2021 Ransomware Study: Where You Are Matters!



**Did You Know:**

SMBs are recognizing the need to step up their defense against ransomware attacks so that they don't need to take such time-consuming post-attack actions.

Twenty-seven percent have implemented ransomware protection including prevention, detection, and remediation, and 11% plan to add these capabilities in the next 12 months, according to IDC's *Worldwide Small and Medium Business Survey*.



# The Cyber Resilience Framework

The business impact of cyber incidents like ransomware attacks make it critical for companies to take action to lower their cyber risks and to avoid becoming the next victim. Companies must also be pragmatic and develop a strategy for dealing with the ramifications of a cyber incident should one occur. Reducing cyber risk, while imperative, does not guarantee that persistent threat actors will always be blocked. The potential of a cyber incident still exists. Therefore, companies should adopt a cyber resilience framework that includes multiple elements of prevention and the ability to recover.

IDC has developed a six-step cyber resilience framework based on the principles detailed in the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*. This IDC framework is designed to help companies assess and achieve cyber resiliency, and includes six interlocking steps.



Source: IDC, 2021

CA48731722BRO



### Step 1: Identify

Companies cannot protect what they have not first identified. Therefore, they should periodically scan their entire IT footprint to identify assets (endpoints, servers, cloud applications, etc.), map relationships to digital-dependent operations, and assess risk. Ironically, scanning for connected assets and relationships is what threat actors do as they seek to uncover vulnerabilities. Skipping this step cedes an advantage to threat actors.



### Step 2: Protect

A company's employees and their devices are often threat actors' first targets (the first point of compromise) in establishing a foothold in a company's environment. To offset this risk, the Protect step is the first of multiple layers of cyber defense. Optimally, this step is transparent to employees, so their work routines are undisturbed. A strong Protect strategy also entails an endpoint protection solution that automatically blocks a wide array of cyber intrusions, preventing threat actors from accessing data. This step also includes systematic file and system backup.



### Step 3: Detect

Threat actors are relentless. When they encounter a closed door, they try another. Plus, they employ tactics to evade Protect defenses. Threat intelligence and experience-based detection (a second layer of defense) is essential to prevent an initial compromise from turning into a major cybersecurity incident.



#### Step 4: Respond

Understanding threats that are already within (as with the Detect step) is essential, but companies must also stop the attackers' advances before real harm occurs. Predefined playbooks and workflows are immensely more effective than responses that are defined and executed during a period of panic. Responses also must account for business impact. The homework done in the Identify step helps avoid an unintended business-affecting outcome.



#### Step 5: Recover

The foothold threat actors first create frequently includes backdoors so they can return. Cleaning up infected devices is critical to prevent actors' easy return. In addition, bad days are still possible (when a ransomware attack encrypts critical files, for example). You need a mechanism to recover your damaged/out-of-commission assets. The good news is your systematic file backup (Protect step) is your file-recovery lifeline.



#### Step 6: Educate

A cyber aware employee base forms a citizen army of cybersecurity checkpoints. Periodic, easy-to-digest awareness and response education can instill confidence within this army to fulfill its mission of helping the company avoid devastating cyber incidents. However, despite the importance of cybersecurity education, only 26% of SMBs have implemented security training for staff, according to the IDC *Worldwide Small and Medium Business Survey*, with 11% planning to do so in the next 12 months. Education is the critical first and last step of the cyber resilience framework. Employees must understand how they can keep systems and data secure as well as the actions that they must swiftly take if an attack occurs. Strong cybersecurity starts with knowledgeable employees.

## From Framework to Action

Unless implemented, a framework is just a blueprint. Companies must convert this blueprint into structure. But not all companies have the time or internal talent to effectively accomplish this conversion. Moreover, it's important that businesses don't underestimate the value of cyber criminal experience. Often, criminals use tactics that have worked many times over. This is how threat actors make their nefarious businesses profitable.

As time, talent, and experience will vary from one company to the next, we offer two options companies can follow in their pathway to cyber resilience: a do-it-yourself one, and one in partnership with a managed services provider. These pathways are not mutually exclusive. **In fact, the winning formula may be a combination of the two.**



# From Framework to Action: Options

## Option 1: Do-It-Yourself

Business leaders and employees assigned cybersecurity oversight should leverage this cyber resilience framework as a confidence assessment guide. Answering the questions below will provide clarity about what your organization can accomplish on its own versus what should be accomplished with the assistance of a managed service provider.



### **Does my company have the technologies and internal processes in place to complete each of these steps?**

It's critical for companies to understand where they stand in terms of executing on each step. Companies should address the steps where they fall short with internal taskforces. For example, if a company has not formalized cybersecurity employee training, it should establish an education curriculum and ensure employees complete it.



### **When was the last time these technologies and processes were evaluated for effectiveness?**

Companies should regularly assess each step in the framework to ensure it is suitable with changing conditions. For example, for the Detect step, companies should take note of new forms of attacks and update their systems and processes so that they are prepped to respond if attacked.



### **If a cybersecurity incident or incidents have occurred, what was learned about our company's state of cyber resilience, and were there any deficiencies?**

If an incident occurs, companies should have a debriefing process to uncover how the adversary succeeded and the systems and processes the company needs to put in place to strengthen cyber resilience.







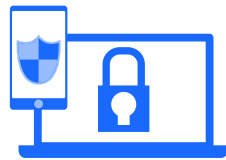
**If cyber resilience deficiencies were identified, what has been our company's track record in closing these deficiencies in a timely manner?**

Once a company has identified deficiencies and the steps to erase them, follow-up should occur to confirm the steps produced the intended outcome. As an example, systematic backup is crucial but the process is incomplete unless restoration is also tested.



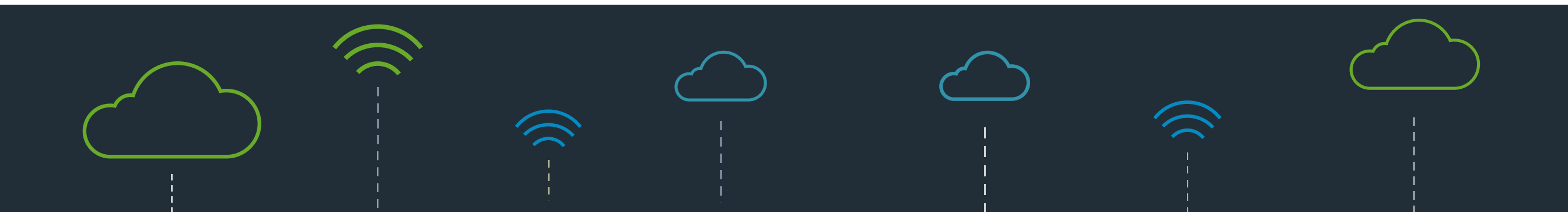
**What is our level of confidence in critically evaluating our current set of cyber reliance technologies and alternatives?**

Internal confidence can sometimes be excessive. With the considerable knowledge, processes, and technologies required for effective cyber resilience, bringing in a third party to assess your state of cyber resilience can assist in identifying deficiencies and provide a point of view that might otherwise be missed by internal staff.



**If new or replacement technologies are needed, can our company manage the end-to-end process of evaluating and implementing change in a reasonable period of time and minimize impact on employees?**

The more transformative new or replacement technology is, the greater the likelihood that bumps will be encountered on the road to deployment. Conduct a technology gap analysis on your company's cyber resilience and keep in mind that the larger the gap, the more your internal project management capabilities will be tested. Remember, threat actors are not waiting for you to deploy new and better technology to strengthen your cyber resilience before they pounce.



## Option 2: Managed Services Providers

Managed services providers should conduct the assessment above in collaboration with their customers and prospects. But before you can get to an actual assessment, education on cyber resilience is critical and should cover the following:

1. What cyber resilience entails
2. How your customers and prospects can use your talent, services, and technology to achieve it
3. The potential ramifications if customers do not follow a cyber resilience framework



## How you communicate with SMBs is equally important.

- To illustrate that your firm has real-world experience, present clear and relevant examples from existing clients about the benefits of investing in your security technologies.
- Explain in straightforward terms — using examples such as ransoms that may need to be paid or business disruptions — the risks that SMBs face if they do not invest in cyber resilience supporting technologies and processes.
- Detail the specific implementation steps and timelines involved in strengthening cyber resilience and how your firm can ease the burden to internal staff, minimize interference to business operations, accelerate implementation, and ensure a higher level of cyber resilience is achieved.
- Explain how your firm helps other SMBs implement effective cyber resilience technology and, as applicable, service tiers for SMBs of various sizes, across industries, and with differing levels of in-house technical expertise.
- Be clear on all-in costs and how those might change as the size and scope of the SMB's business and digital footprint changes.
- Tailor your word choice to the audience and avoid acronyms and jargon that SMBs may not understand.
- Highlight success stories of similar businesses.
- If it applies to the conversation, describe how your engagement supports SMBs with compliance requirements.

### Key Consideration:

Each service or product a business supplies to clients and customers must be thoroughly vetted to ensure it is secure. Integration with outside suppliers can introduce new risks. Additionally, any software that may be preloaded onto a product a business sells, such as a laptop or tablet, should be checked to ensure it doesn't contain malicious ransomware or malware.

## Message from the Sponsor

# opentext™ | Cybersecurity

### **OpenText is Committed to Simplifying Cyber Resilience**

Through diverse product offerings spanning data security and backup applications.

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

Learn more at [go.zixcorp.com/Email-Security.html](https://go.zixcorp.com/Email-Security.html)

