Cyber-resilience during a crisis

how are Dutch Small and Medium businesses staying security-prepared in an unpredictable market?

kaspersky BRING ON THE FUTURE

Learn more: kaspersky.com

Introduction

The last three years have become a great stress test for businesses all over the world. Enterprises of all sizes were forced to pivot their priorities focusing on unlocking business value with a transition to remote working while fighting inflation, supply chain issues, or investing in new revenue streams.

Entrepreneurs and small businesses have always been a **very essential part of the economy**, not only because more that 99% of Dutch companies are SMBs, but also as they are able to innovate, bring products to market, or create jobs faster than large corporates. Also, in uncertain times, people traditionally turn to what and who they know – **usually trusted local businesses** or SMBs who can react faster to change.

However, as they charter unpredictable events beyond what is normally expected, change comes with additional stress or complications, requiring decision-makers to be prepared to quickly adapt and stay afloat. While it's hard to anticipate all risks, especially those that are not directly tied to financial losses, sometimes unseen gaps in the business can worsen a crisis.

This Kaspersky report explores some of the challenges SMB business leaders have been through in the last three years and to what extent they are ready for challenges of the future, the possible difficulties they see on the horizon, and potential cybersecurity risks that may arise as they navigate a post-pandemic, recessionary landscape.

Methodology

Kaspersky commissioned research consultancy, Censuswide, to undertake quantitative online research with 1,307 business owners and decision makers within small and medium-sized organizations (less than 999 employees) who are responsible for business development and strategy. The research was conducted across the UK, USA, Germany, France, UAE, KSA, Turkey, Indonesia, Thailand, India, Brazil, Mexico, Colombia, Belgium and The Netherlands.

Key findings

Business owners are concerned about potential cybersecurity incidents

40% perceive a cyberattack as a crisis

Four in ten (**40%**) Dutch SMBs would perceive a cyberattack as a crisis if it were to hit their business, followed by technology failure (**35%**) and dramatic employee outflow (**32%**).

Cyber-resilience must match growth and development

25% of medium businesses have faced a cyber security incident in the past

With **8%** of very small organizations (one to eight employees) and **25%** of mid-size firms (500 to 999 employees) reporting they faced a cyber-incident in the past, the probability of facing cyberattacks rises as companies grow.

SMBs value cybersecurity investment

13% would consider cutting cybersecurity costs in a crisis.

The majority of small businesses place value in cyber-resilience and security: **23%** of Dutch SMB leaders are more likely to cut advertising budgets than IT or cybersecurity, while just **13%** would consider cutting cybersecurity costs in a crisis.

But confidence in IT stability could improve

53% are not confident they could keep information security function stable

If hit by a crisis, companies need to rely on IT functions to keep transactions moving, customer data secure and suppliers connected with a business. However, **53%** of Dutch business managers or owners say they are confident they could keep their IT and information security functions stable if they would have to cut costs on IT.

Some measures aimed at reducing costs in times of a crisis can provoke additional cybersecurity risks

15% would be willing to use pirated software

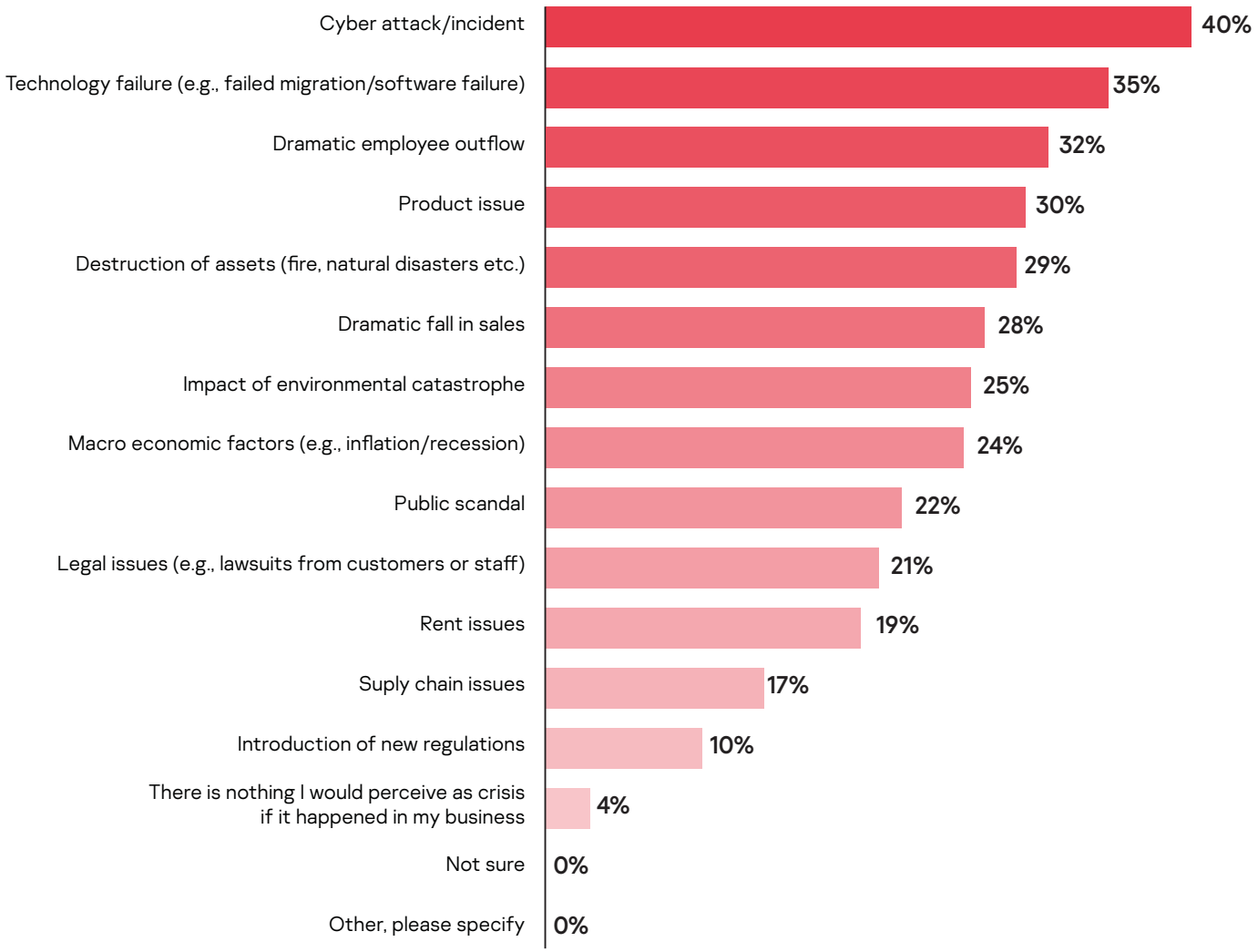
Speaking of staff reductions, companies may not have kept up-to-date with access restrictions to existing, new, or former employees. Of those surveyed, more than half could guarantee ex-employees can't access company data via cloud services (58%) or corporate accounts (**64%**). When it comes to reducing IT costs, more than one in ten (**15%**) respondents would be willing to use pirated software.

What defines a crisis?

Managing small and medium businesses has never looked like an easy task, and the recent challenges have proved it once again. With all the experience SMB leaders have acquired during the last three years it is important to figure out what they perceive as a crisis, which difficult situations have they already faced, and how prepared entrepreneurs are for upcoming challenges on top of daily issue management.

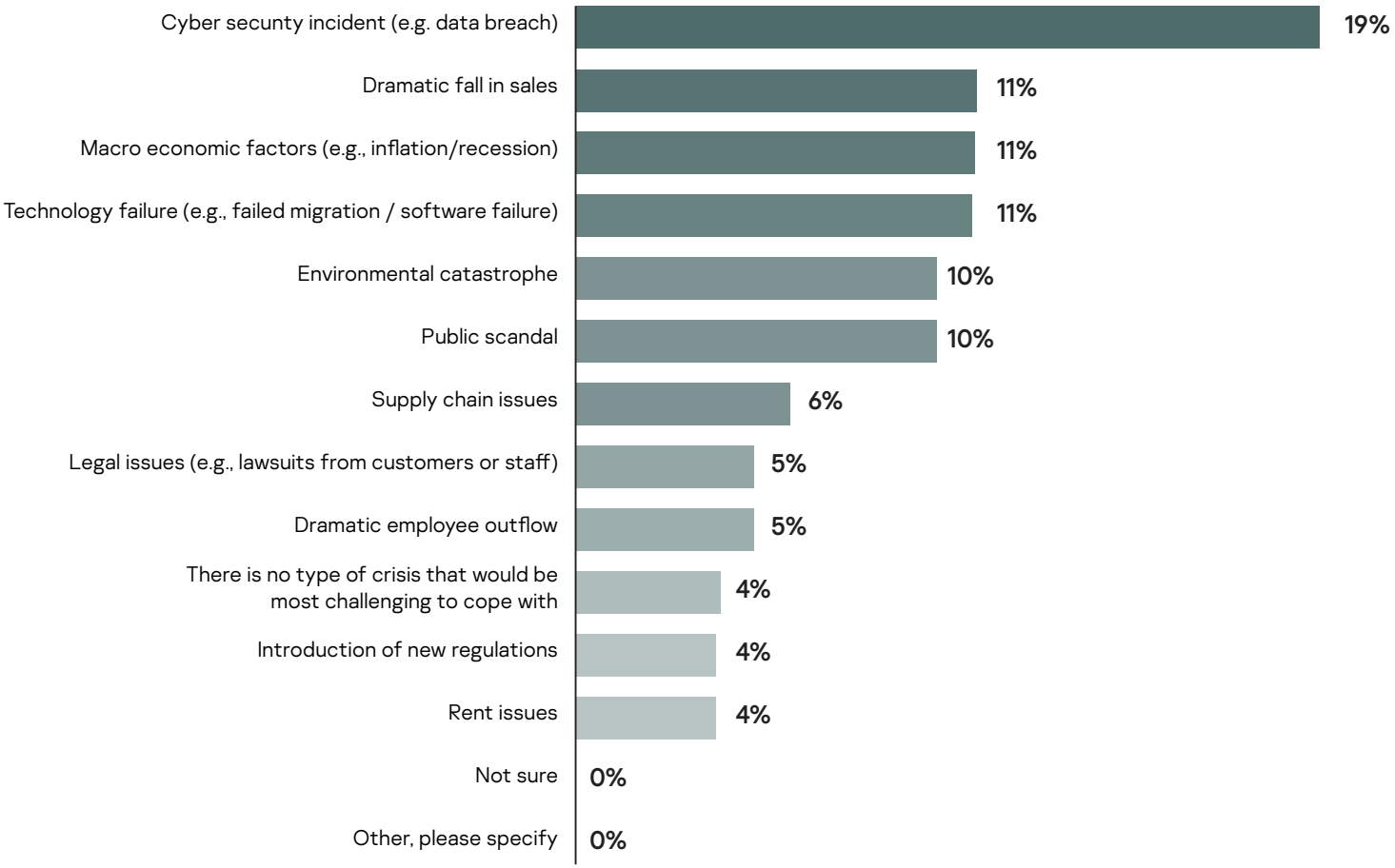
Four in ten (**40%**) SMB leaders agreed that a cyberattack would be seen as a crisis if it happened to their business. Supply chain issues (**17%**) and the introduction of new regulations (**10%**) were also seen as factors that would cause additional pressure. Other crisis factors include technology failure (35%), dramatic employee outflow (**32%**), destruction of assets (**29%**), dramatic fall in sales (**28%**), impact of environmental catastrophe (**25%**) and macro-economic factors (**24%**).

What, if anything, would you perceive as a crisis if it happened in your business?



Dutch SMBs have found that cybersecurity incidents (**19%**) are the most challenging to deal with. However, the loss of sales appears to be difficult to deal with for a substantial number of respondents too (**11%**). Macro-economic factors, such as fighting a recession or inflation, were seen as the hardest situations to cope with for **11%** of respondents. The dramatic outflow of employees, new regulations, or a sudden rent rise was seen as challenging for less than **5%** of respondents.

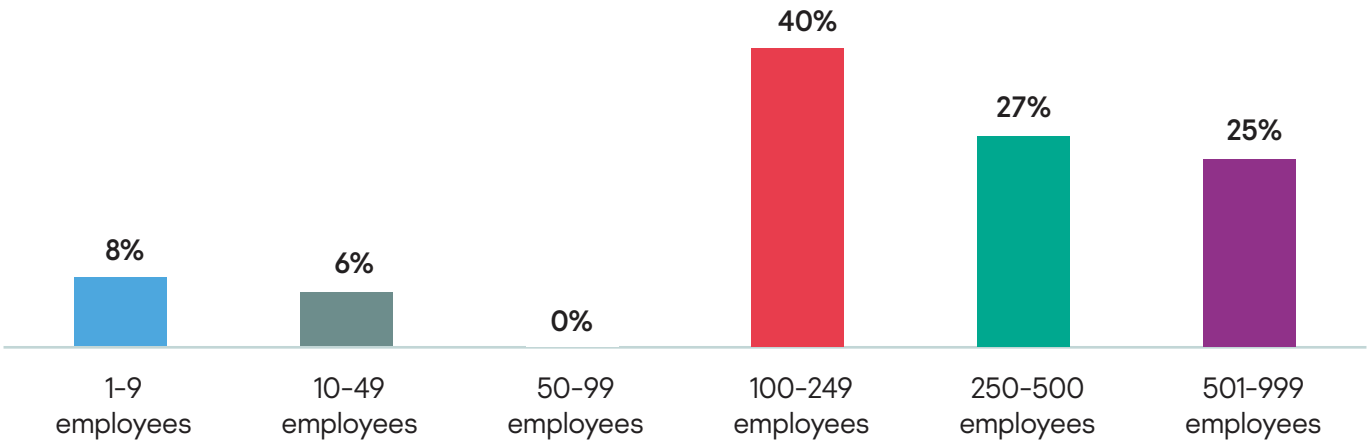
What, if any, type of crisis would be the most challenging for you to cope with?



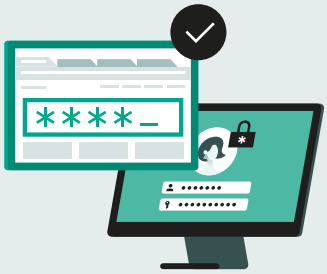
In the Netherlands, **89%** of small business leaders have navigated through at least one crisis in the past, with **19%** experiencing a dramatic employee outflow and 19% enduring technology failure like failed migration. Almost one in five (**18%**) have experienced a cyber security incident, for example a data breach. Meanwhile, environmental catastrophe and rent issues are the least common crises for SMBs, with only **7%** contending with this.

While cybersecurity incidents have affected **18%** of all respondents, this number seems to increase in relation to the number of employees at the company. Only **8%** of organizations with one to eight employees faced such a situation, while **25%** of companies with more employees (501-999) and larger IT infrastructure experienced a cyber-incident.

Proportion of companies that had to navigate cyber secutity incident in the past



To keep business protected and reduce the likelihood of a cybersecurity incident Kaspersky recommends the following:



- Eliminate the probability of a brute force attack when an adversary attempts to gain access to your digital entry point by submitting many passwords or passphrases in hopes of eventually guessing correctly. Implement a strong password policy for all your and your employees' digital assets. A secure password should consist of at least eight letters, one number, uppercase and lowercase letters, and a special character. In case there is any suspicion that the password have been compromised, change it immediately. A security solution, such as **Kaspersky Small Office Security** with a built-in password manager will help effortlessly put this approach into practice.

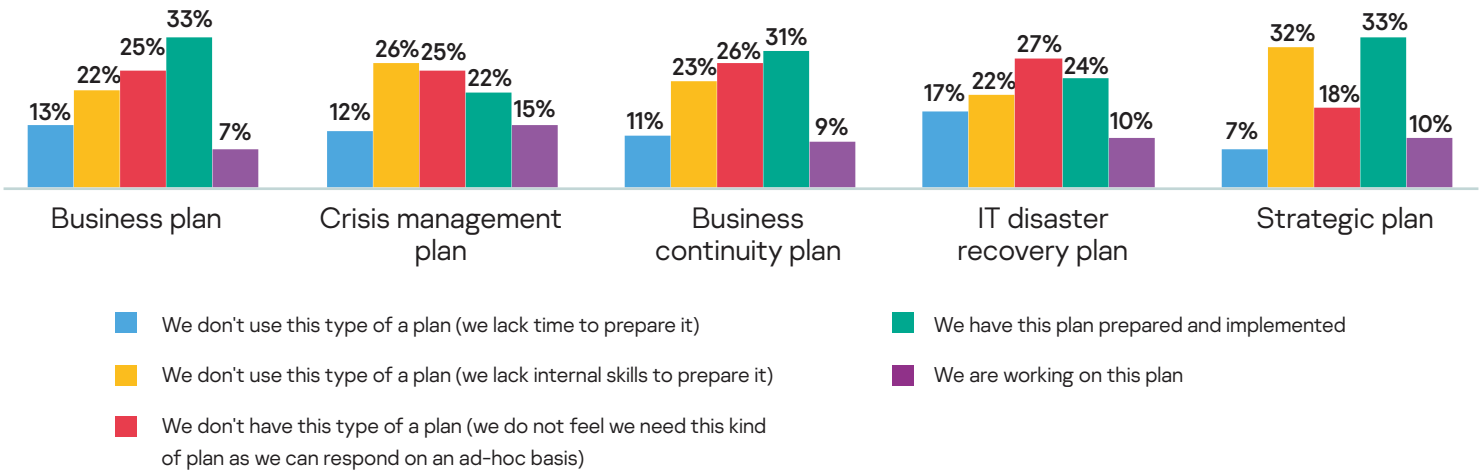
- Don't let adversaries get advantage of your software vulnerabilities. These are low-hanging fruits for attackers which use vulnerabilities to get initial access to a corporate data. Don't ignore updates from a software and device vendors. These usually not only bring new features and interface enhancements, but also resolve uncovered safety gaps.

- Protect against ransomware attacks, when an intruder encrypts corporate data and extorts the ransom for its decryption. Besides keeping all devices updated, another important step is to set up offline backups for your data so that you can quickly access them if any of your organization's files are encrypted. Since this threat is on the rise, the security solution for your business needs to be able to provide **100% protection** against ransomware. Its functionality should include identifying and blocking unknown malware before it is executed, and initiating automatic backup copy creation in the event of an attack;

- Maintain a high level of security awareness among employees. Encourage your workers to **learn more** about current threats and ways to protect their personal and professional life and take relevant **free courses**. Another way is effective third-party training programs for employees, such as **Kaspersky Automated Security Awareness** program which helps to build concrete cyber-hygiene skills and practices.

Do you have a crisis management plan?

While almost a quarter (24%) of SMBs do have an IT disaster recovery plan prepared or implemented, many are better prepared for growth than security: more have a business plan (56%), strategic plan (33%) or business continuity plan (31%). Active crisis management plans were only in place with 22% of businesses questioned.



One warning issue is that **27%** of SMBs believe they don't need an IT disaster recovery plan and intend to deal with this kind of problem on an ad-hoc basis, perhaps because they assume they would not be the target of a cyberattack. In addition, more than one in five respondents admit they lack the skills to prepare a crisis management (**26%**) or IT disaster remediation plan (**22%**).

What steps might help mitigate an IT disaster impact? – recommendations from Alexey Vovk, Head of Information Security at Kaspersky

An IT security incident is always a stressful situation. To make sure that you'll be able to react quickly and won't waste time in case of emergency, we recommend the following:

1. Identify your critical business assets and systems. Make sure that these assets are protected and you make a regular backup of crucial information.

2. Know the risks - understand the nature of potential threats. Monitor relevant cybersecurity news to understand what kind of attack your company should be aware of. This knowledge also will allow you to understand if your security solution provides the necessary protection.

3. Make a list of key contacts. Think about who you can turn to in case of a cyber incident, including partners, suppliers, banks, IT providers, and incident response services.

4. Inform your employees how to spot an incident. Such signs as computers running slowly, users being locked out of their accounts or users being unable to access documents, ransom demanding notifications, and any unusual computer behavior can be an indication of this.

5. Regularly conduct internal emergency drills (including testing the shutdown of a number of IT systems and testing restoring data from backups).

6. Information on action plans and communications in emergency situations should also be stored offline, as IT systems may not be available.

7. Implement a system for prompt secure communication of key people in an emergency, for example, a messenger independent from the main one, not connected to other corporate systems and therefore won't be compromised.

8. Develop and approve in advance PR-statement templates for various types of incidents and emergencies.

How are small businesses managing the oncoming crisis?

The pandemic has been the **perfect storm for businesses** globally, of the likes no one has ever seen. Long-term strategies pivoted to cost saving and cutting plans. As recessions, rising interest rates, staff retention and hybrid working models continue to impact SMBs, how are they able to balance business operations with security?

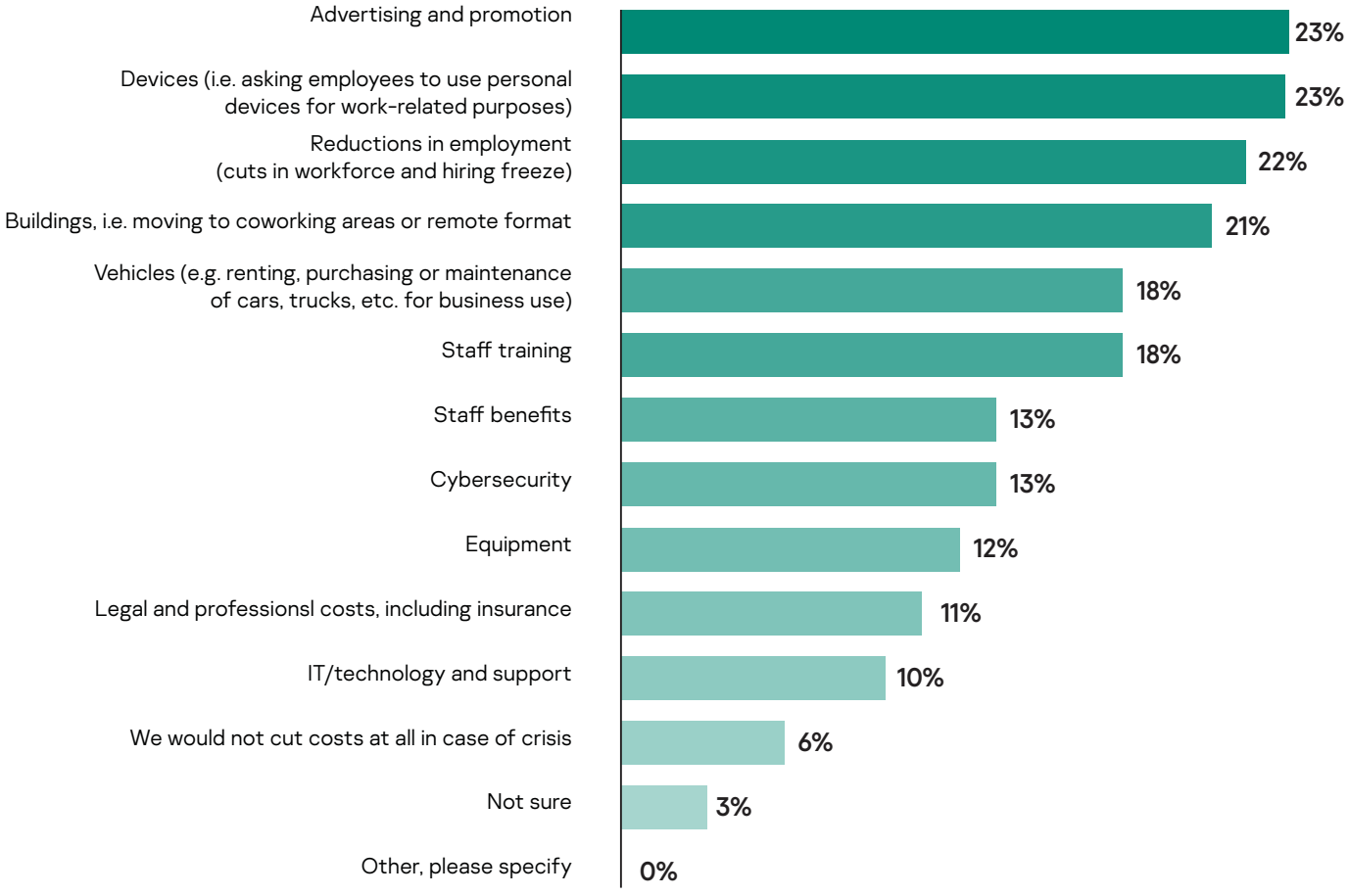
In section two, we examine the attitudes of SMBs towards crisis management, how they have changed, cope under pressure and who – if anyone – they turn to for advice.

Managing operational costs

Operational costs have been a challenge for businesses, particularly SMBs, over the previous years – according to the last year's Kaspersky report almost four-in-ten (**38%**) SMBs admitted to cutting budgets to survive. Of those, **35%** reduced pay for working hours; over a third (34%) closed physical locations; a quarter (**24%**) cut their spend on IT and tech support – one-in-five (**19%**) for cybersecurity and **12%** had to lay off staff.

While this is no surprise, our survey confirms cost-cutting is still a business priority as **91%** of SMB leaders would try to do so in case of a crisis. To optimise costs SMBs would be willing to reduce advertising (**23%**), devices (**23%**) and employment (**22%**) spending. However, most were not prepared to cut their cybersecurity costs, even in hard times. In fact, cuts to IT technology and cybersecurity spending were only considered by **10%** and **13%** of businesses, respectively.

Where, if anywhere, would you cut costs in case of a crisis?

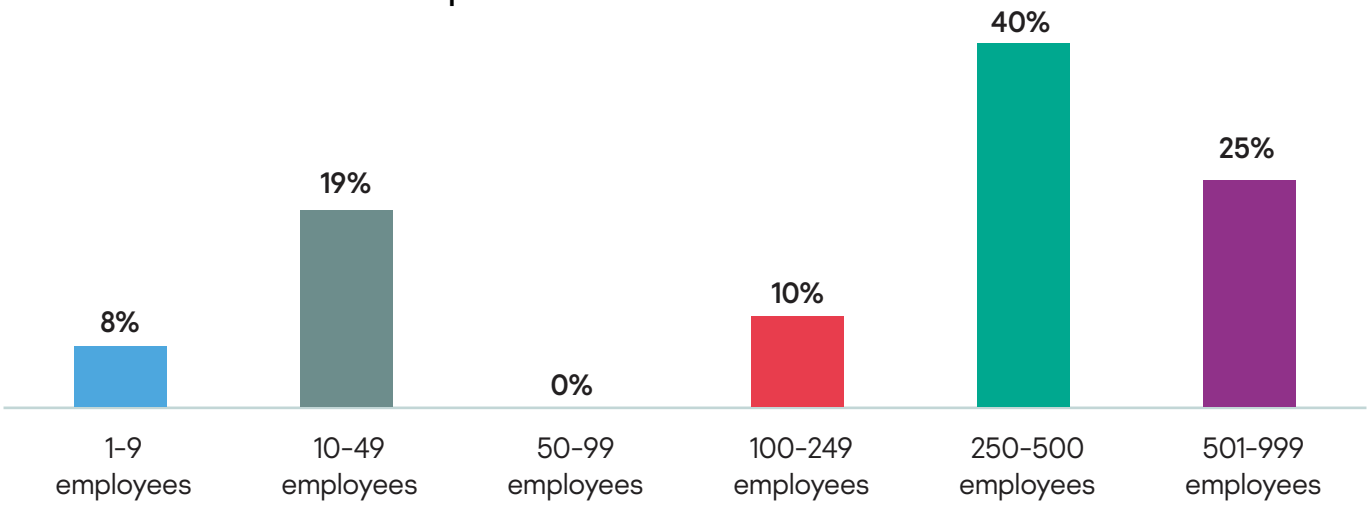


With every aspect of a business being under pressure in the current climate, it is no surprise business leaders are playing it safe and being more cautious than ever: **61%** are opting to bring in lower-cost contractors, while another **61%** track special offers or discounts that might help cut operation costs.

In 2022, expanding customer reach is still important, with **19%** of SMBs willing to buy or consider purchasing customer databases as a way of growing client leads.

To make further operational savings, **28%** of SMBs would replace their current software with a free alternative. Worryingly, 18% would replace their current software with a pirated version to optimize budget spending. Of this figure, the share is different for small and medium businesses. Up to **19%** of small businesses say they would take this step, compared to up to **40%** of medium-sized companies.

Would you replace current software with a pirated version to cut or optimise costs in the event of a crisis?

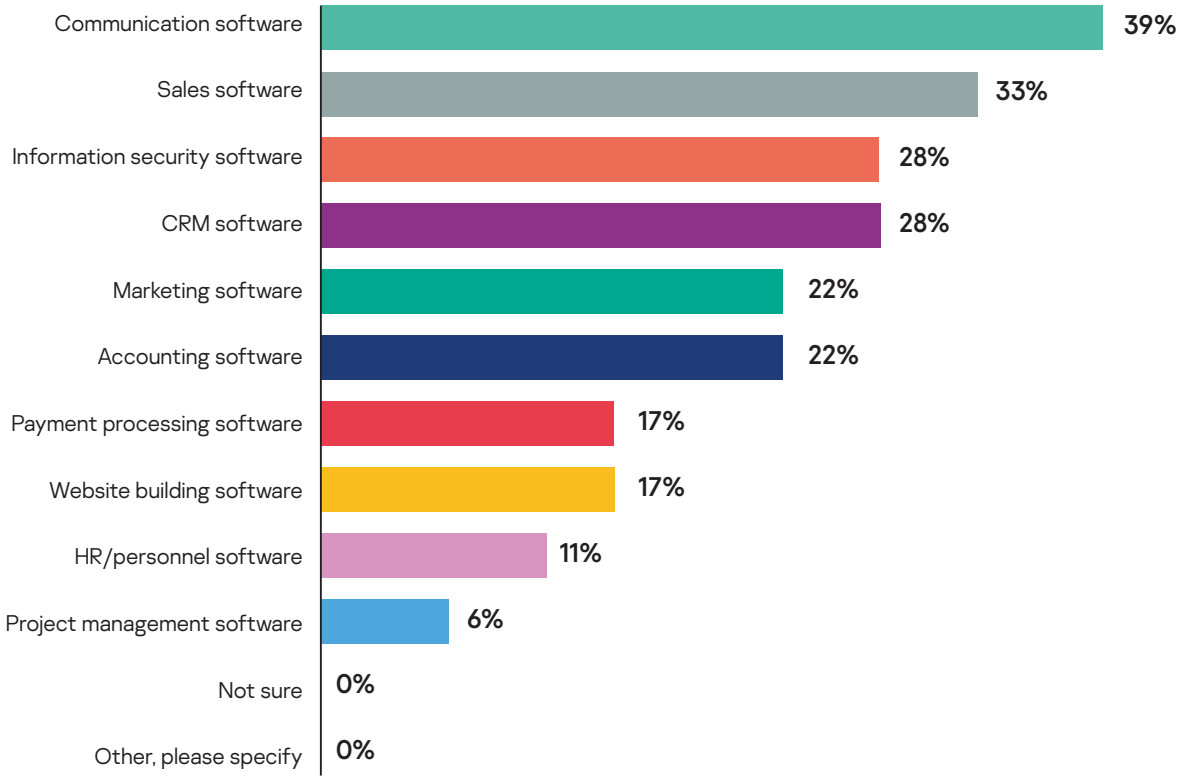


To access information on the threats related to the SMB sector, Kaspersky experts analyzed the most popular software used by small and medium businesses. We used the titles of the software, such as MS Office, MS Teams, Skype, and others as keywords and ran these against Kaspersky Security Network (KSN)* telemetry to determine the prevalence of malicious files and unwanted software related to these programs, as well as the number of users attacked by these files.

For the period from January 2022 ,1, to August 2022 ,30, the total number of users who encountered malware and unwanted software hiding in software products for SMB was 9,685, with 4,525 unique files distributed under the guise of SMB-related software.

When asked what type of pirated alternative software they would bring into their organization, the most sought after was communication software (**39%**), followed by sales (**33%**) and CRM software (**28%**), while another concerning **28%** say they are ready to use a pirated alternative of cybersecurity software in their organization.

You said that in the event of a crisis, you would replace current software with a pirated alternative. What types of software would you do this with?



*Kaspersky Security Network (KSN) is a system for processing anonymized cyberthreat-related data shared voluntarily by Kaspersky users.

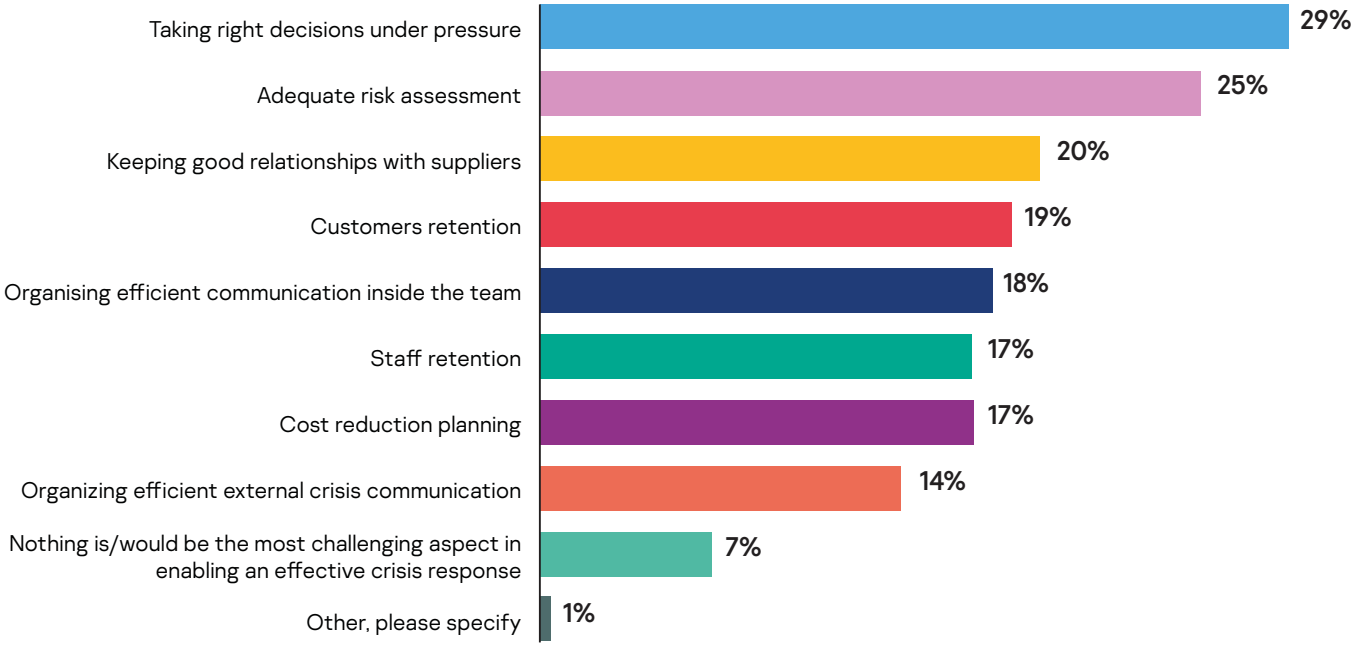
How to avoid infected software installation?

- Make sure your employees can't install programs on their own. Usage of standard accounts without admin rights will prevent them from accidentally installing a Trojan mistaken for productivity software.
- You can use free security solutions. They usually have less functions than paid products but still might be very helpful. Choose a solution based on the independent tests' results, and download it directly from the developer's site.
- To avoid paying a hidden electricity bills, constantly monitor your devices efficiency. If your gadget is slowing down, overheats and makes a lot of noise even when no one is using it, someone might have installed a miner on the device which is overloading the processor and video card. Use a security solution that detects not only malicious programs, but also potentially unwanted installments.
- Update your operating system, antivirus, browser and all the programs you work with as soon as a new update comes out.
- Implement regular backups of important files in a cloud service and on alternative hardware. That will allow you to have a copy, even if ransomware encrypts your data. A security solution with remediation features, such as Kaspersky Endpoint Security Cloud will let you roll back actions performed by malware in the operating system, delivering protection against cryptolockers.

Overcoming pressures and challenges

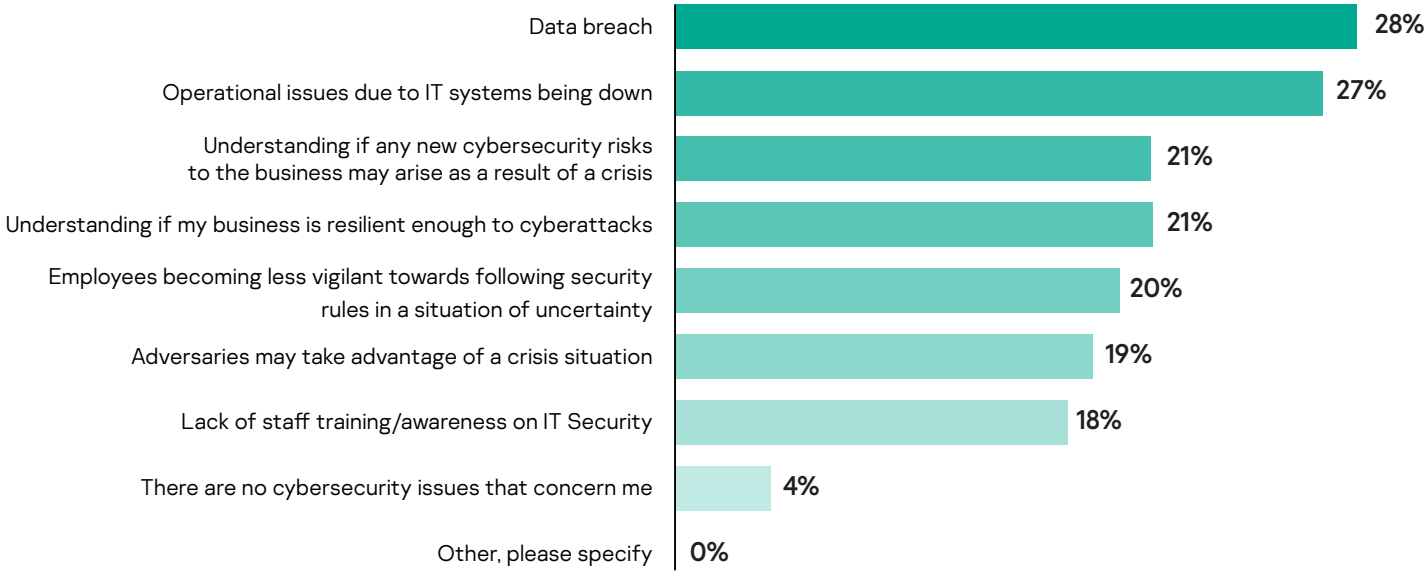
Navigating a stressful market is challenging for any business. This is even tougher for SMBs who don't always have the capital or reserves of their larger, enterprise peers. So how can they deliver an effective crisis responses or make decisions under pressure? Almost three out of ten (**29%**) of SMBs say retention of staff is the most challenging aspect in enabling their business to operate an effective crisis response. Organizing efficient communication inside the team (**25%**) and customer retention (**20%**) are also among the top three issues facing SMBs.

According to your experience or assumptions what are/would be the most challenging aspects in enabling an effective crisis response, if any?



Despite **96%** of respondents having concerns about their company's cyber-resilience during a crisis, **53%** say they could keep their IT system and data stable if they had to cut IT staff. Speaking of the most challenging aspects of keeping their company cyber resilient during hard times, data breaches (**28%**) were the most significant issue for SMBs. This was followed by operational issues due to IT systems being down (**27%**) and understanding if any new cybersecurity risks to the business may arise as a result of a crisis (**21%**) as well as understanding if the business is resilient enough to cyberattacks (**21%**).

What are the cybersecurity issues, if any, that concern you when speaking about your company's resilience to a crisis?



Managing a team through a crisis

Even if a business is strong, keeping morale up and employees on board is a challenge in turbulent times. Our research shows that the majority of SMBs agree that communication and transparency with team members is key to encourage staff retention and dedication.

When a crisis, such as a cyber-incident, sales loss, or strikes hit, most business leaders in the survey view transparency as key to staff trust and retention and, as such, look to strengthen team relations (**31%)** and offer flexible working schedules (**27%**). This approach is seen as a more effective way to keep employees during a crisis than a salary increase, which was the tactic for **24%** of business leaders.

How, if at all, would you try to retain your employees during a crisis?

Considering the talent risks

Being up front is the best policy choice for **65%**, who prefer to communicate openly with employees regarding a crisis. However, most employees (**57%**) are worried that sensitive information could provoke staff turnover and **50%** believe this could lead to staff negligence of their responsibilities.

Julian Robinson, Director of CruxPoint crisis management consultancy shares his recommendations on the best approach regarding communications with employees during a crisis::

Pre-prepared templates providing the foundational structure and content for communication (regardless of the nature of the event) can assist to streamline communication processes; Crux Point advocates the following structure for crisis communications:

Dr Michael Ryan (WHO Health Emergencies Programme) at a press briefing on COVID-19 in March 2020 quoted Voltaire when talking about the lessons learned from previous Ebola outbreaks: **"Perfection is the enemy of the good when it comes to emergency management… you need to be coordinated, you need to be coherent… be fast, have no regrets"**.

Speed is a critical communication principle in a successful response to an emerging crisis event. Another critical communication principle is acting on decisions which are based only upon available facts (not information gaps). Leaders should follow the principles when communicating during a crisis event, for all (internal and external) communications.

Awareness: Demonstrated knowledge of the facts surrounding the event and information gaps that key people are addressing.

Empathy: Demonstrated understanding of the potential or actual impacts of the situation on those affected with a primary focus on safety and wellbeing.

Cooperation: Reassurance that the right people and resources are engaged to respond both to the event and the continuation of business activities where safely practicable.

Commitment to communicate: Reassurance that leaders will continue to inform employees of any developments in a timely manner.

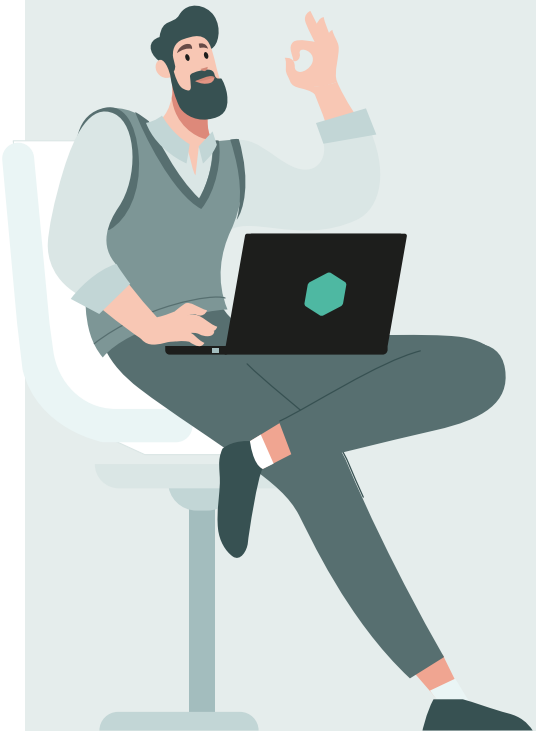
Communication during a crisis should come from a carefully selected leader whose seniority identifies them immediately as a credible spokesperson for the organization and possesses appropriate character traits of calm and control. This demonstrates that the organization is giving an appropriate level of attention to the situation and reduces the chance of panic or loss of confidence.

Following a disruption event, the critical principle of communication with employees is candour. Regardless of whether the disruption event was unavoidable or not, it is important for employees to understand that the organization demonstrates ownership of the situation as it builds trust in leadership, as opposed to avoidance.

Further, **51%** also could not guarantee internally shared information would not be disclosed publicly. Still, in the event of staff reductions, **55%** felt confident of maintaining good relations with former employees.

Taking into account that reduction in staff employment is a common measure to reduce operational costs in crises, the negligence towards access restrictions to former employees may be seen as a worrying situation - of those surveyed, just over half could guarantee ex-employees can't access company data via cloud services (**58%**) or corporate accounts (**64%**). Apart from the risk of corporate data damage, this situation may lead to financial losses for business - 59% of respondents believe ex-employees may still be able to use corporate information to launch their own business and **67%** are worried that workers would share their consumer bases or other important corporate information from the former workplace with their new employers.

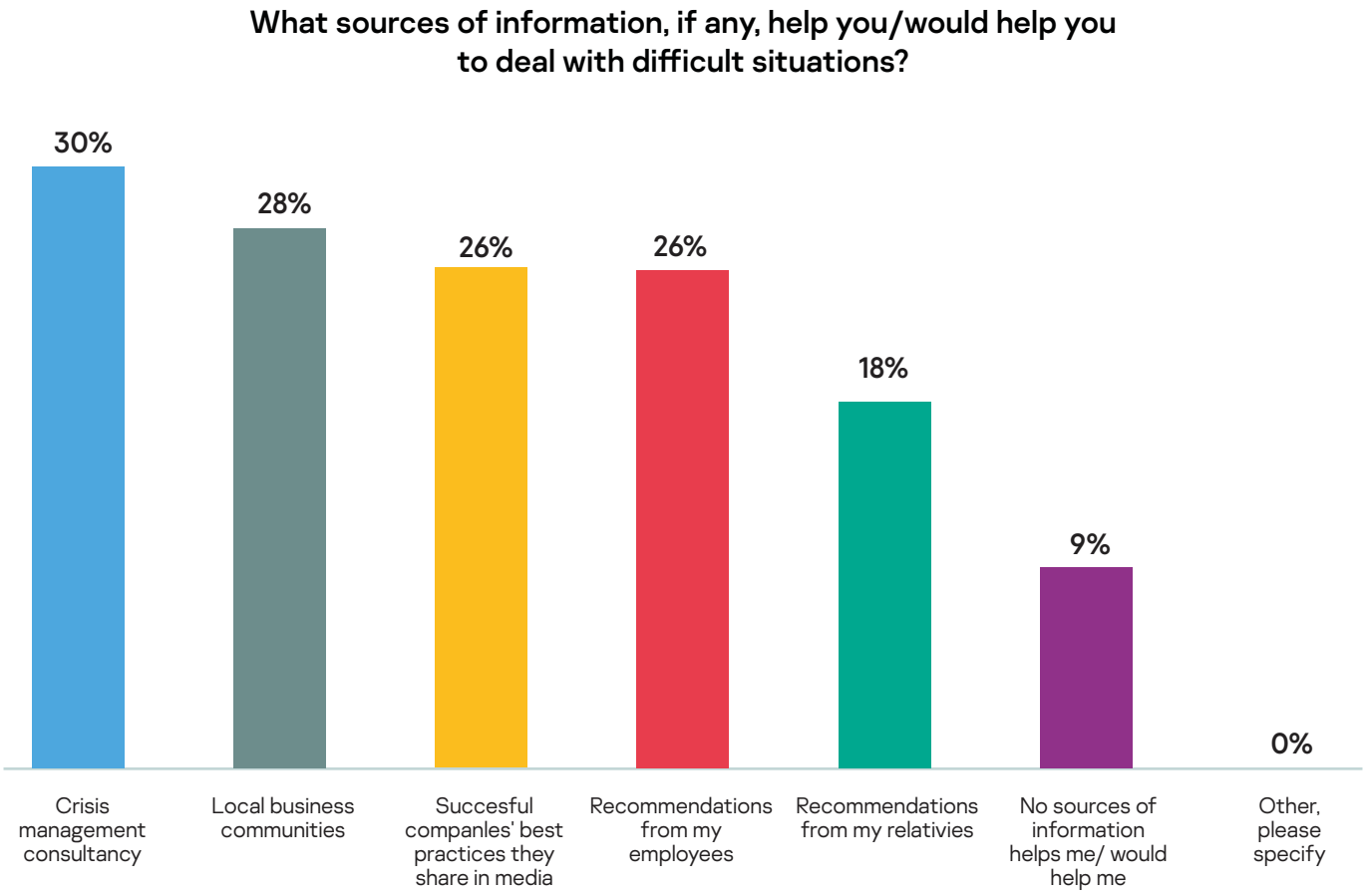
To ensure accurate corporate data usage by employees, Kaspersky recommends taking the following steps:



- If possible, decrease the number of people with access to crucial corporate data, reducing the amount of data available to all employees. Breaches are more likely to occur in organizations where too many employees work with confidential valuable information that can be sold or somehow used.
- Set up an access policy for corporate assets, including email boxes, shared folders, and online documents. Keep it up to date and remove access if an employee leaves the company. Use cloud access security broker software that helps manage and monitor employee activity within cloud services and enforces security policies.
- Make regular backups of essential data to ensure corporate information stays safe in case of emergency.
- Provide clear guidelines on the usage of external services and resources. Employees should know which tools they should or shouldn't use and why. When switching to any new software for work, there should be a clear procedure of approval with IT and other responsible roles.
- Encourage employees to have strong passwords for all digital services they use and to change passwords regularly.
- Regularly remind staff about the importance of following basic cybersecurity rules relating to safe account and password management, email security, and web browsing.;
- Employ dedicated cybersecurity services which provide visibility over cloud services used by employees, such as **Kaspersky Endpoint Security Cloud**.

Where can business leaders get support?

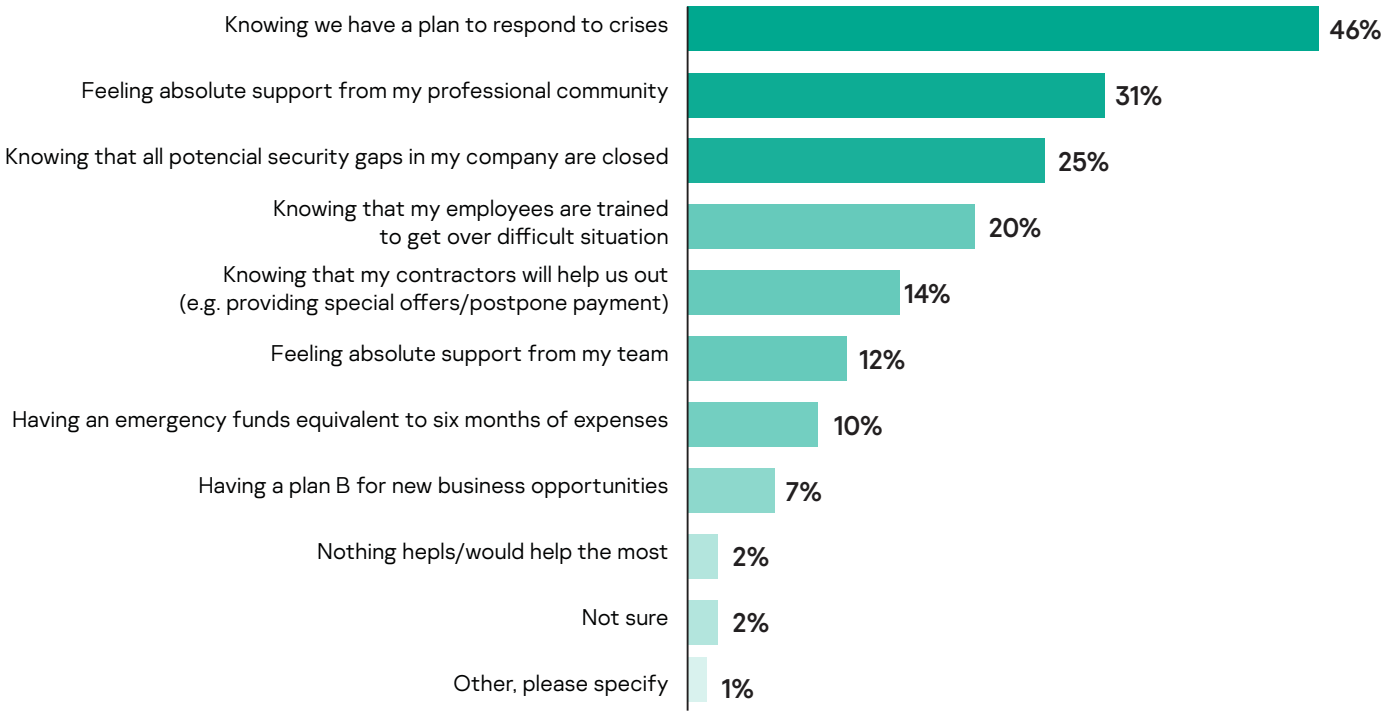
While people may turn to their local weather service in changeable climates, there are few networks or services for SMBs to turn to when their organization faces a new or unexpected challenge. Who do they turn to and what can small business owners learn – if at all – from a crisis? For most small businesses, business leaders are happy to apply for support or seek professional advice in a crisis, with almost a third to bring in a consultant or expert (**30%**).



Looking to the strategies or 'best practices' of successful companies shared in the media (**26%**) is seen as an effective and quick solution. The majority are willing to talk about their own experience or best practices with peers inside the organization (**79%**) or with friends (**60%**), but **47%** would not feel comfortable sharing insights with competitors and **45%** would never share with networks.

Good planning, a trusted team and closed cybersecurity gaps help business leaders feel less stressed during times of difficulty. Most respondents chose knowing they have a plan to respond to crises, feeling absolute support from their team and knowing all potential security gaps in their company are closed as the top-3 factors that would help them feel less stressed in case of a crisis. These options are more important for entrepreneurs' peace of mind than having emergency funds equivalent to six months of expenses (**10%**) or having a plan B for new business opportunities (**7%**).

What, if anything, helps/would help you the most to feel less stressed when/if your company is going through difficulties?



How can business owners at least to some extent be sure that cybersecurity gaps in their organization are closed? - explains Konstantin Sapronov, Head of Global Emergency Response Team at Kaspersky.

Due to budget limitations, small and medium businesses sometimes cannot afford to adopt cutting-edge cybersecurity solutions or hire skilled security specialists. That is why these organizations may question the probability of achieving a sufficient level of cyber resilience.

However, as our **study exploring the nature of cyber incidents**, shows, even basic and simple measures still can significantly contribute to a company's security. Thus, since 54% of cyberattacks started on public-facing applications, such as Microsoft Exchange with published vulnerabilities, timely software updates alone can reduce the likelihood of an incident by half.

To give attackers even less chance to steal your company's data or money, introduce a robust password policy and teach your employees to distinguish phishing emails. These steps mitigate the likelihood of an incident by another third, even for large corporations because usage of compromised accounts and malicious emails are also among the top-3 adversarial methods to get into the corporate infrastructure.

Fraudsters usually look for low-hanging fruits and obvious cybersecurity gaps because they need their operations to be

cost-effective. If the revenue from an attack is less than its cost or requires too much effort, it is usually of no interest to them. The basic measures mentioned above are not exhaustive but in combination with implementing a cybersecurity solution would help to reduce the appeal of your business for bad guys.

After navigating a crisis, the successes and failings offer an opportunity to reflect on how the situation was managed and protect the business from similar challenges. Can a crisis be useful for the company? Of **30%** of respondents who have experienced a crisis, they gained a better understanding of how to manage future events, and **27%** indicated it allowed them to implement new technology. Only **3%** of business leaders said going through a difficult situation did not help or strengthen them in any way.

What, if anything, has going through a serious crisis or difficult situation helped you with?

Navigating the cybersecurity landscape during a crisis

Almost all SMBs that responded to Kaspersky have faced some form of a crisis in the past. And, while some SMBs are prepared for a crisis – only 22% have a crisis management plan in place - the results show that among small businesses and enterprises there is still work to be done.

This mainly can be attributed to the informational security gaps. Facing a cybersecurity incident or business crisis connected with large or small-scale cybersecurity incidents, most firms have concerns regarding their business safety while going through hard times.

It is also important for small and medium business leaders to consider that some anti-crisis measures, such as cutting costs for IT or staff reductions may also introduce new risks.

However, the fact that SMBs care about cybersecurity and understand how challenging IT security incident remediation can be is a good tendency that hopefully will result in reliable protective measures implemented within these organizations.