zivver

Secure Mail is On

To: Olly Watkins
Subject: Sensitive Material

Secure Sending

Remote working and data security in a digital world

→ 2021 survey findings

Table of contents

←
→

Introduction: The impact of remote working on data security

The phenomenon of remote working has been widely discussed for decades, particularly around the subject of digital transformation and dexterity.

However, until 2020, even a hybrid approach was rare; the office remained the heart of the business. In sectors such as education, government, and healthcare, working remotely was especially scarce.

The COVID-19 pandemic forced the hand of businesses worldwide to accelerate their digital strategies for the purpose of business continuity, during an unprecedented shift to remote working. Employees made home offices out of spare bedrooms and kitchens; office-based teams became remote workforces overnight - and so a flexible working culture began to evolve.

Now, nearly two years later, remote working is the norm. But with our new-found flexibility comes a variety of security challenges.

Can stakeholders still trust that their data is handled securely?

Do employees, business leaders, and IT professionals truly understand where security risks lie?

And to what extent can IT teams facilitate a remote workforce?

We set out to investigate how hundreds of IT and security professionals are combatting the challenges facing their organizations in a remote and increasingly digital world.

About the survey:

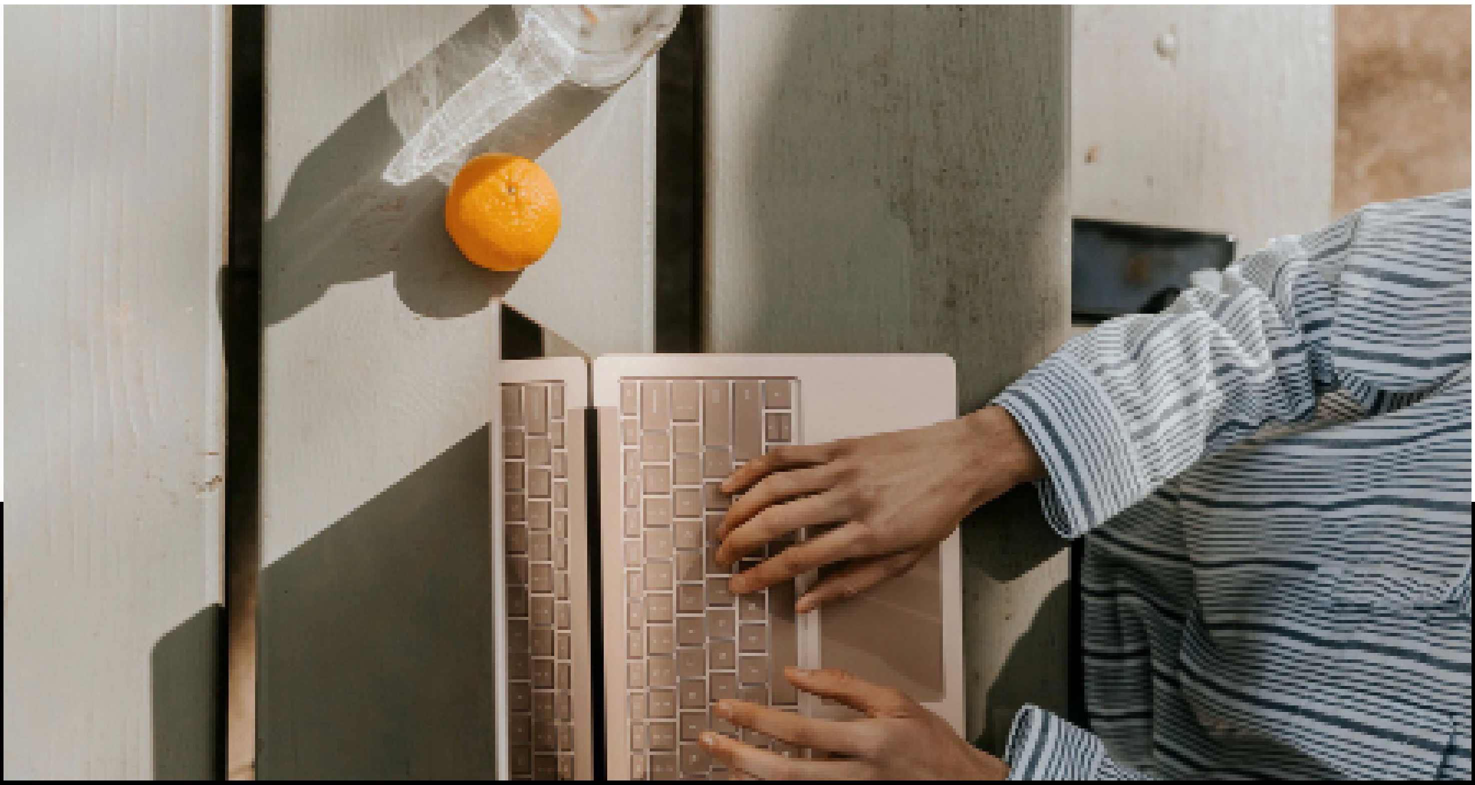
Zivver and IT platform, AG Connect, conducted a survey among 486 IT professionals in the first half of 2021 to investigate security challenges in relation to remote working, digital communications, and data security.

The majority of respondents work in government agencies, however, professionals from business services, financial enterprises, education, healthcare, and the communications sectors are also represented.

Respondents answered twenty questions on the requirements and resources for secure remote working in an increasingly digital world.

The purpose of this report is to indicate the current state of security and, above all, to identify areas in which there is still room for improvement.

We hope the findings will support business leaders in making informed decisions on the matter of digital communications and data protection across a remote workforce.



"Costs play an excessive role in the decision-making process" - Respondent

Executive summary

The phenomenon of working from home has been discussed for decades. However, due to the acceleration of digital communications, and the democratization of technology coupled with a global pandemic that forced teams to lock their office doors for an undetermined period of time practically overnight, many businesses have been caught short or are not prepared for a remote workforce.

There are many considerations raised by remote working, ranging from wellbeing and security, to information sharing and communication. But are business leaders focused on empowering individuals to work remotely? Is safeguarding communications, and the impact this can have, truly understood?

Zivver, in collaboration with IT platform, AG Connect, sought to explore this further, with a particular focus on the importance businesses place on creating an environment in which people can share information and communicate with confidence. Together, Zivver and AG Connect conducted a survey among 486 IT professionals across a variety of sectors to unpack the challenges and opportunities for working remotely.

This report paints a picture of the current landscape, and highlights the areas in which organizations can still improve in terms of understanding the impact of safeguarding digital communications.

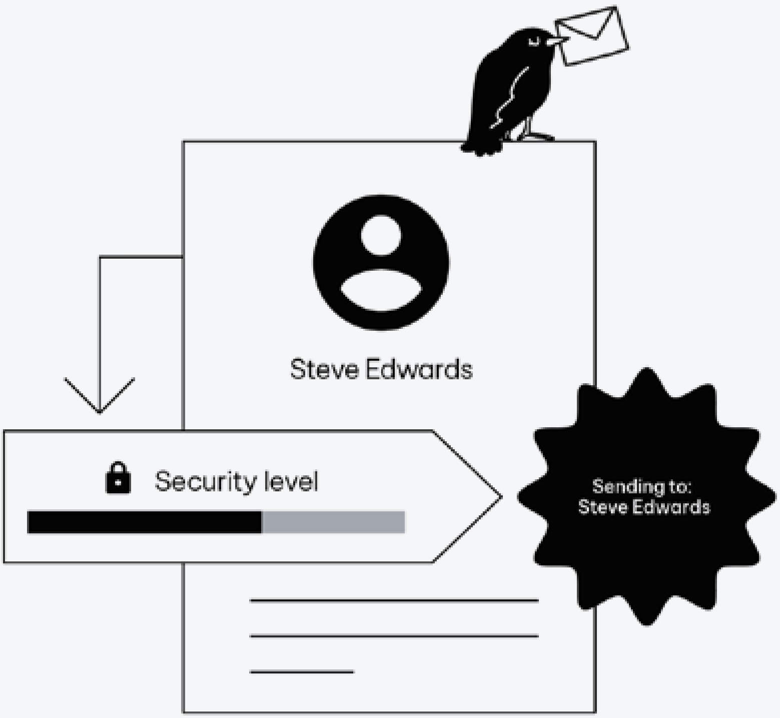
We hope that the insights in this report will help business leaders to empower their teams in making data driven decisions, drive action, and achieve results securely, all the while working remotely.

The main conclusions from the report center around the use of resources and tools, security challenges, unsafe communications and the causes of data leaks.

Use of resources to support secure digital communications

According to our respondents, the tools most implemented by their employers are antivirus software, access control and backups. In addition, the report reveals that there is an uplift in people considering the introduction of endpoint monitoring and policies for flexible working.

Despite 80-90% of data leaks occurring in outbound communications, our research shows that a staggering 70% of those surveyed are not worried about the information being shared. Immediate awareness is required to empower workforces to be able to communicate, succeed, and share sensitive information with confidence.



Challenges of security

What are the main security challenges people experience as they evolve to a remote working culture?

- 46% of respondents claim that more emails are being sent with an increase in remote working
- Preventing data leaks is acknowledged by 74% of respondents as being the largest challenge with remote working
- Additionally, security awareness among employees urgently requires attention, with nearly 72% of respondents stating that the awareness level of security issues amongst their employees is one of the main challenges with remote working.

Causes of data breaches

There is a discrepancy between the actual causes of data breaches and the data breaches known to many organizations. Almost 75% view hacking, malware and phishing as the main causes of data leaks, despite the Dutch Data Protection Authority showing that only 5% of data breaches are actually caused by said malicious attacks, with outbound communication the cause of 85% of data breaches.

Not only are the causes of data leaks misunderstood, but keeping track of security issues seems to be a challenge for many organizations. A large proportion of respondents indicated that they are not aware of whether there has been a data breach in their organization.

Five key take-outs:

01 Full 360 degree security review: securing all paths of digital communications is what's key. Focusing only on inbound (what's coming into your systems, for example) is the equivalent of locking your windows but leaving your front door wide open.

02 Empower users: enable individuals to securely do their jobs through smart technology whilst lessening the need for training.

03 One size does not always fit all: consider solutions that offer right sized levels of secure communication supportive of use-case and recipient technology capabilities (not all situations require tight security and vice versa).

04 Technology is powerful - maximize it whenever possible: having powerful machine-learning detection and automation wherever possible is key,

05 It's not just about where information is coming from: being able to smartly detect the status of the recipient's/user's set-up provides a critical layer of security.

01 Remote working has had a positive impact on IT security

Many organizations had strong IT security systems in place before the pandemic.

We asked respondents to consider the change in focus on IT security: have they witnessed an adjustment in security since remote working became the norm prior to the global pandemic?

The majority of respondents believe that their organization's security procedures were strong prior to the pandemic and remained that way throughout lockdown.

STATEMENT: There were good IT security systems in place before the pandemic

Completely agree	Partly agree	Partly disagree	Completely disagree
53.36%	39.58%	4.59%	2.47%

STATEMENT: There were strong IT security systems in place for core processes and applications prior to the pandemic

Completely agree	Partly agree	Partly disagree	Completely disagree
63.6%	28.62%	6.01%	1.77%

"It was the sudden scale of remote working that posed a challenge to us" – Respondent

Furthermore, respondents feel their workplace has improved IT security for core systems and processes since their workforce became remote.

STATEMENT: There were good IT security systems in place across the entire organization

Completely agree	Partly agree	Partly disagree	Completely disagree
54.77%	38.52%	5.3%	1.41%

STATEMENT: There were good IT security systems for core processes or applications in my workplace

Completely agree	Partly agree	Partly disagree	Completely disagree
67.49%	27.21%	3.89%	1.41%

“All our focus is now on remote working and more measures are in the pipeline.” – Respondent

Almost 70% of respondents agree that their organization’s approach to cyber security has improved since the start of the pandemic. We can therefore conclude that the pandemic, and resulting shift to remote working, has had a positive effect on IT security across the majority of sectors.

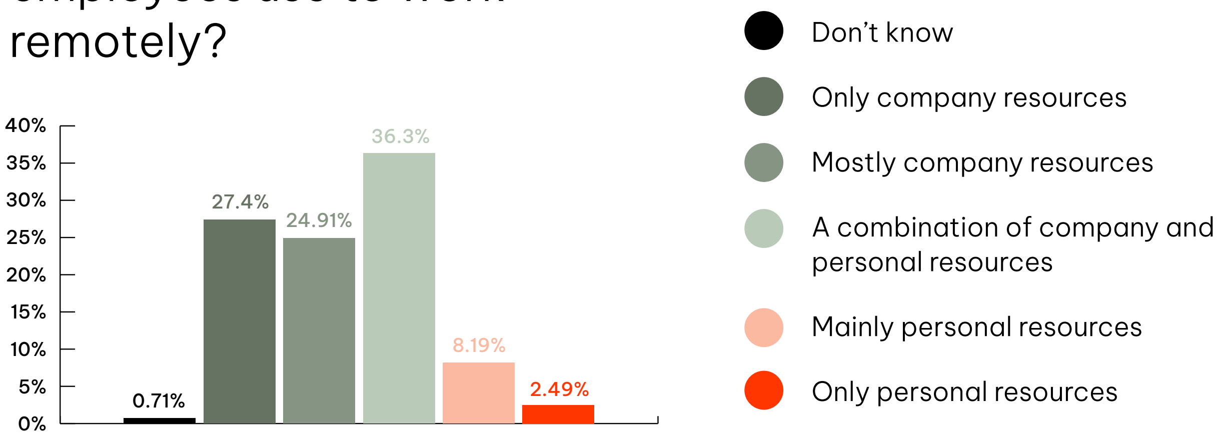
STATEMENT: Our cybersecurity has improved since the pandemic

Completely agree	Partly agree	Partly disagree	Completely disagree
14.84%	53.36%	18.02%	13.78%

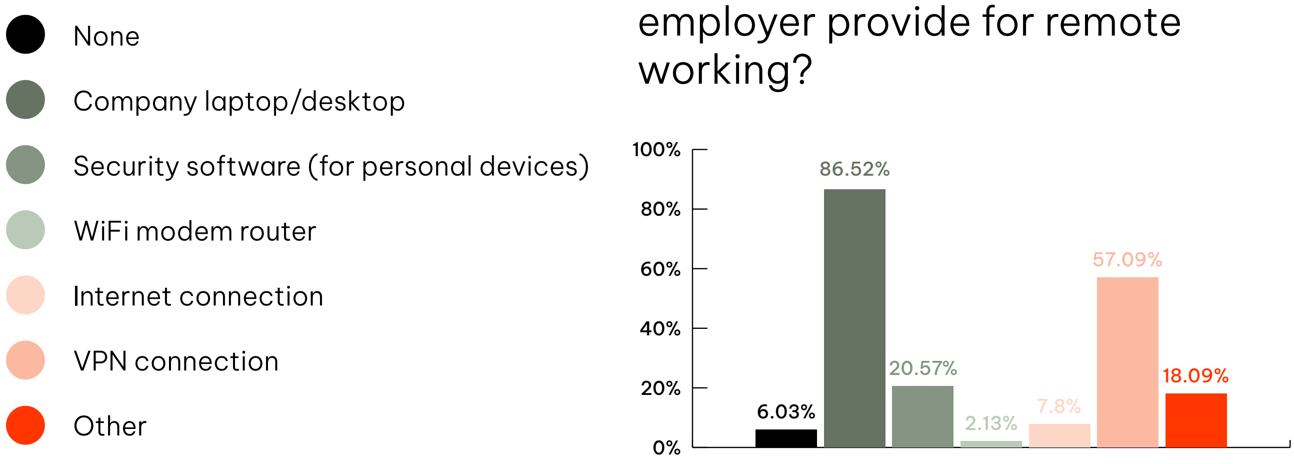
Remote working resources

Over 70% of workers utilize their own resources to operate remotely. With personal devices a very real security threat for businesses, and a significant lack of ‘bring your own device’ policies in place to log the use of personal items, this number is surprisingly high.

What resources do employees use to work remotely?



What resources does your employer provide for remote working?



Resources provided by employers tend to primarily be laptops and a VPN to enable a secure connection with the corporate network. Only 21% of respondents received security software for their personal devices from their employer; for respondents in business services (20%) and government institutions (17%), the distribution of security software for personal devices was more prevalent.

This survey did not consult on office furniture. However, many respondents indicated that their employer had provided such resources.

02 New resources to counter modern challenges

New challenges call for the deployment of innovative tools.

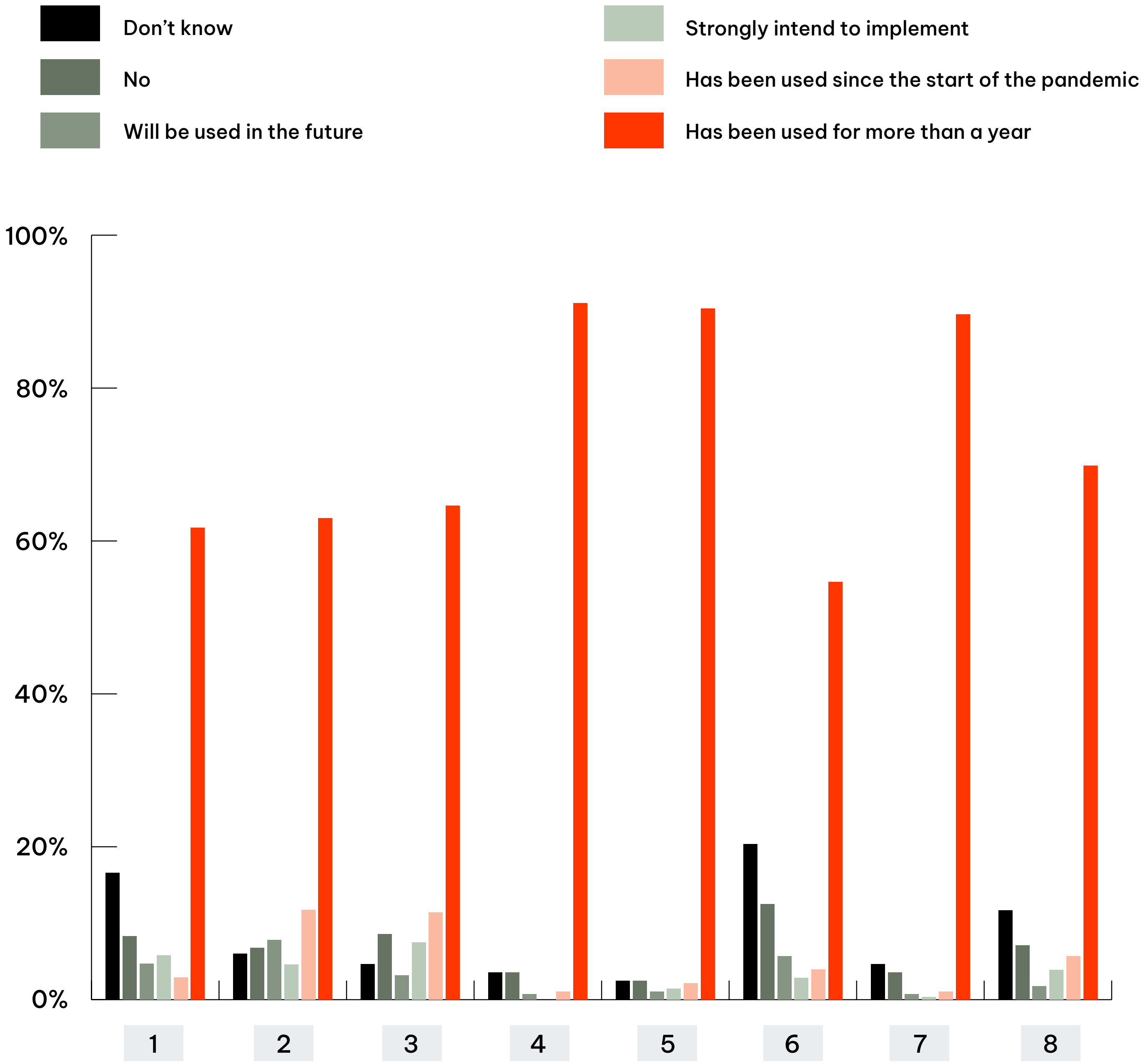
The resources most frequently introduced by employers are, according to our respondents, anti- virus software, access control, and back-ups. However, a remote working culture necessitates a shift in security protocols. Our survey found that employers have also implemented endpoint protection, awareness campaigns, and remote working policies.

Security awareness is an integral aspect of data security. Furthermore, with employees working outside of the office environment, organizations have increased the use of secure outbound communication technologies.

Technology alone is not a security silver bullet. Organizations have found that a combined approach, with security awareness training embedded as a core function within secure communications software, instils best practice, ensuring employees have the skills and knowledge required to handle data correctly.

Please indicate whether your employer is using, or will start to use, the following resources:

1	Endpoint	4	Antivirus	7	Backups
2	Remote working policies	5	Access control	8	Secure outbound communication
3	Awareness campaigns	6	Whitelisting		



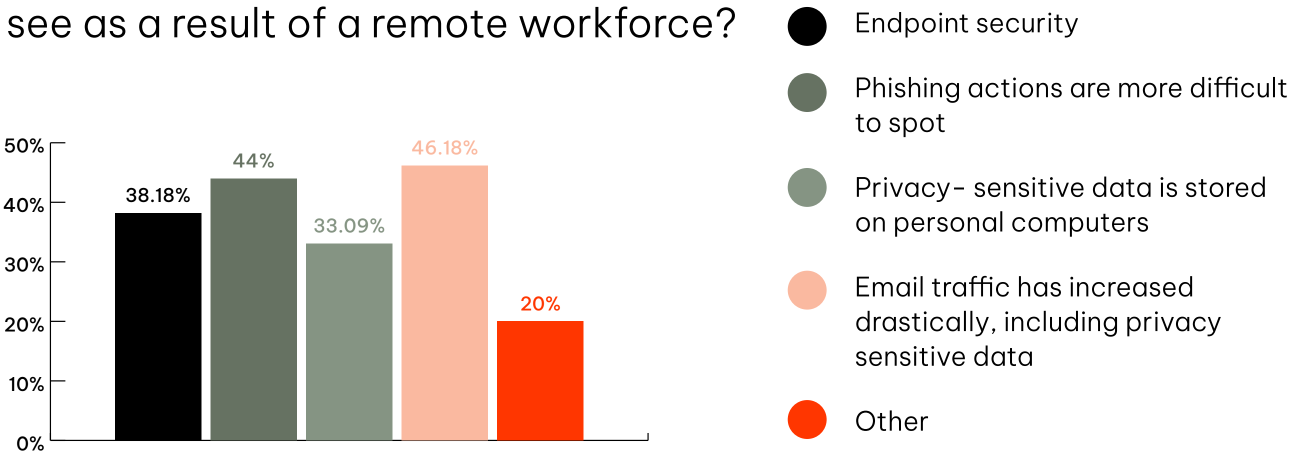
Security challenges for a remote workforce

With employees spread far and wide, we asked respondents about the challenges they experience concerning outbound and/or internal communications, remote working, and data security.

More than 46% of respondents referred to concerns regarding an 'increase in email traffic, including sensitive data'. Additionally, as many as 44% stated that phishing activities are more difficult to prevent across a remote workforce; the ability to avoid social engineering attacks was also frequently mentioned. Employee awareness plays a decisive role here.

Endpoint security (38%) also appears to be an important factor. Naturally, with such a sudden and vast shift to remote working, it has become more difficult for security professionals to secure access to remote networks.

What security challenges do you see as a result of a remote workforce?



The results showcase the very real challenges confronting security professionals across different sectors today. Over 72% of respondents indicate that their employer has a good system in place or is working towards it. However, while the general consensus is, 'We are doing our best but could do better', there remains a certain amount of unclarity, with many stating, 'I expect my employer has taken care of this, but am unsure'.

It is no secret that human error remains the leading cause of data incidents today, iterated by an increasing focus on security awareness across the workforce. Also of great importance is the usability and practicalities of security measures, processes, and platforms, with user-experience mentioned several times by respondents. 'If you ask me, no one can ever have security 100% covered, as you have to consider usability.' - Respondent

Almost 28% of respondents feel less confident about their employer's initiatives. One respondent states: 'Costs play an excessive role in the decision-making process.' Others state that, while their organization is aware of the risks, they fail to take appropriate action: 'Only knowledge and insight, no real actions or resources'.

STATEMENT: How strongly do you agree with the statement, 'My employer has put the appropriate systems in place for secure remote working'?

3.91

Strongly disagree

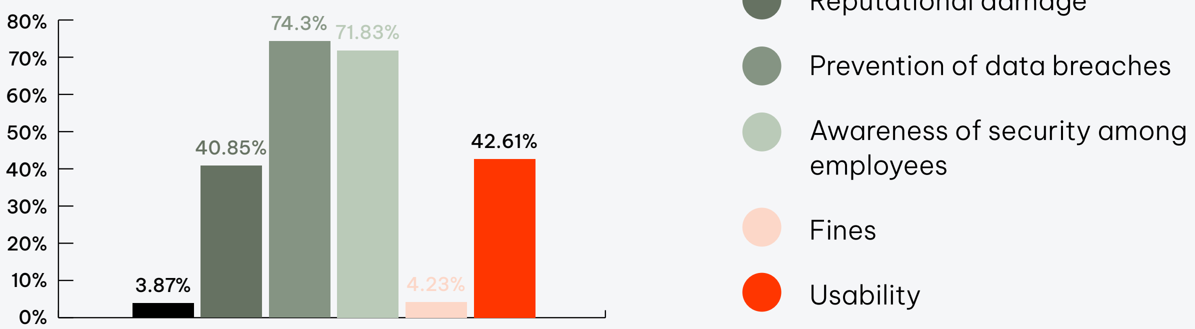
Strongly agree

1	2	3	4	5
2.52%	3.6%	21.58%	44.6%	27.7%

Current and future challenges concerning communication security

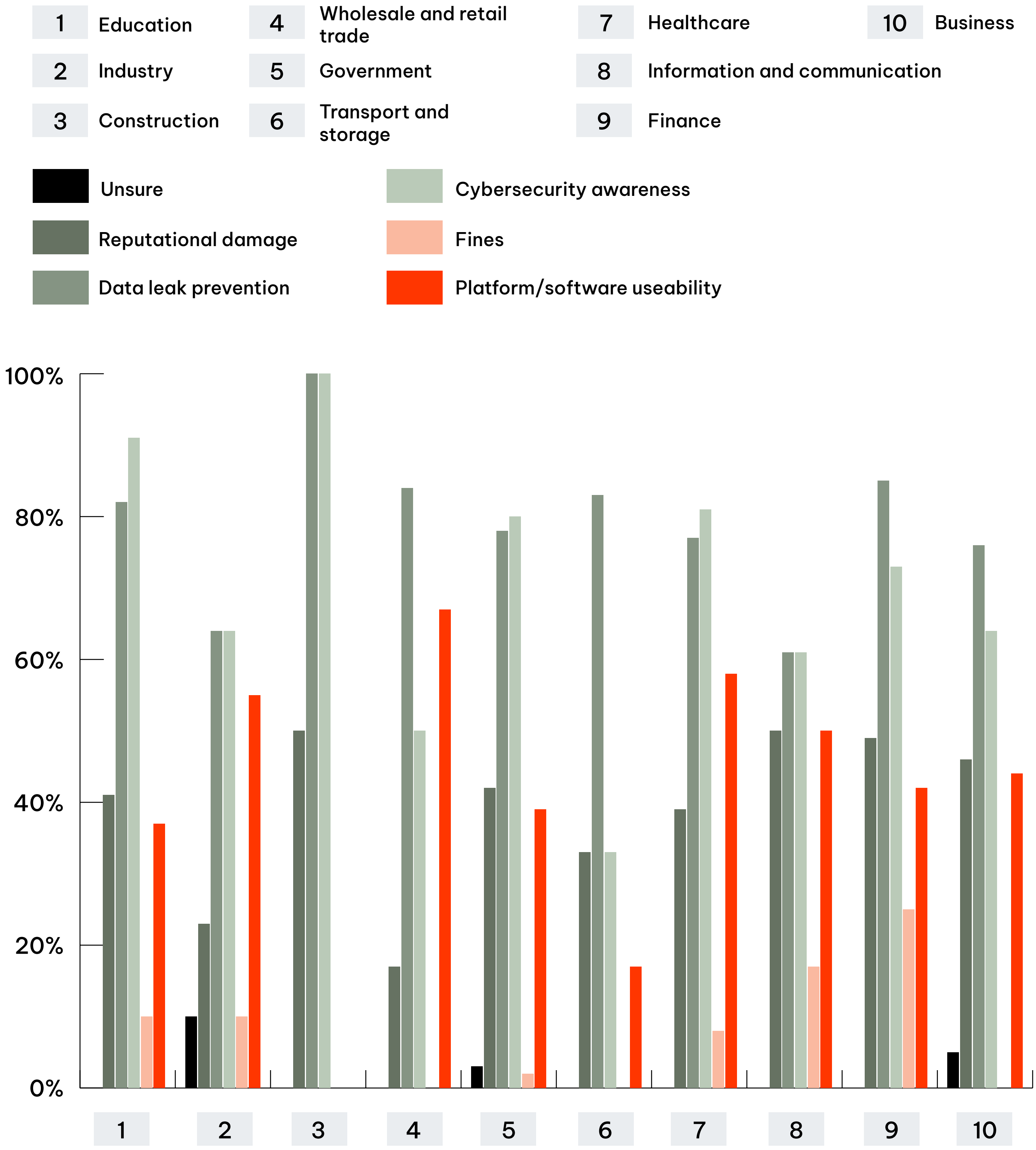
We asked respondents to consider the challenges they expect to encounter in the near future on the matter of communication security and remote working. More than 74% of respondents referred to the 'prevention of data breaches' and 72% raised 'security awareness among employees' as an ongoing challenge. Also frequently mentioned were both usability and reputational damage.

What challenges do you foresee in the near future regarding communications security?



Usability of security software and platforms is a particular issue in the healthcare (58%), wholesale and retail (67%) sectors.

What challenges do you foresee in the near future regarding communications security?



At just 5%, very few respondents see the imposition of a fine as a factor of concern.

03

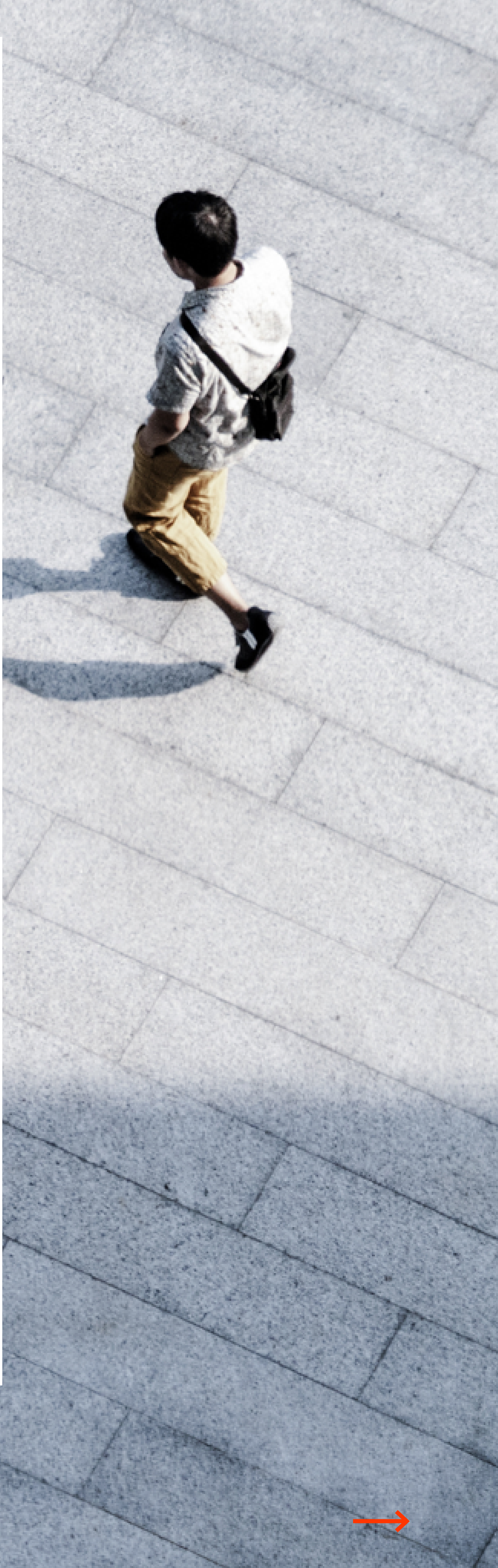
Security awareness and education

Raising awareness among employees is a top priority for security professionals.

According to respondents, effectively raising awareness across a remote workforce remains a great challenge in ensuring secure communications. Unless a security policy is mandatory, people are unlikely to comply with it. And, inevitably, if employees are unaware that a security issue exists, they are unable to act appropriately.

But just how effective is compulsory training, mandatory policies, procedures, and approved software lists?

The ways in which employees manage communications with stakeholders must be secure, if only to ensure compliance. Respondents agree that striking the balance between usability and security is key in achieving this – arguably this is one of the most complex challenges facing security and IT professionals today.



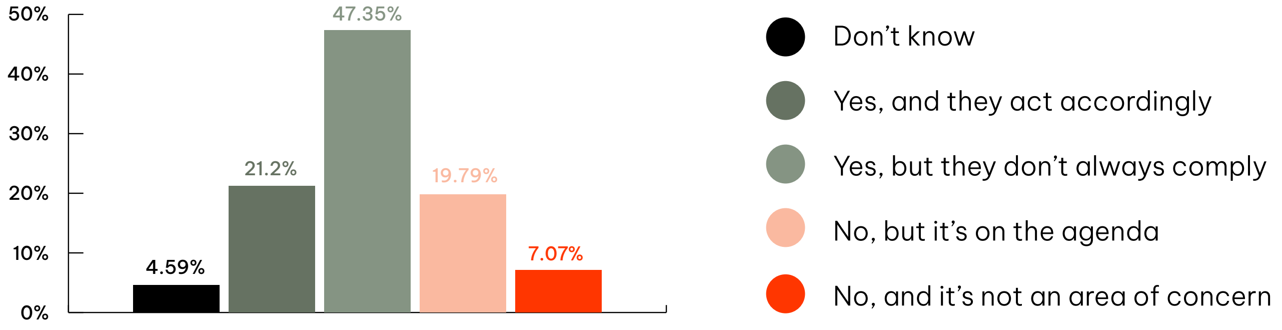
An analysis of the results:

Employees recognize the importance of cybersecurity but do not act accordingly

On the matter of awareness, the results highlight a distinction between employees and managers. According to respondents, employees are aware of security requirements, but often fail to comply with recommended (or mandatory) security policies and procedures. Often, this is due to a misconception of their importance. 52% of respondents state that employees somewhat understand the seriousness of unsecure file sharing, and only 21% of employees take action to secure sensitive communications, according to respondents.

47% of employees occasionally comply with requirements, leaving a large segment managing sensitive data and communications in a less than secure way.

Do you think employees are aware of IT security requirements when working away from the office environment?



In particular, respondents in the business services and construction sectors indicated that employees do not fully appreciate the severity of unsecure communications. It is striking that respondents in more traditional sectors, such as transport and healthcare, indicated that their employees are particularly careful when handling sensitive data while working remotely.

STATEMENT: In your opinion, do employees understand the seriousness of unsecured file sharing and communication when working remotely?

No, not at all	No, not really	Yes, a little	Yes, absolutely
0%	20.92%	52.84%	26.24%

In your opinion, do employees understand the seriousness of unsecured file sharing and communication when working remotely?

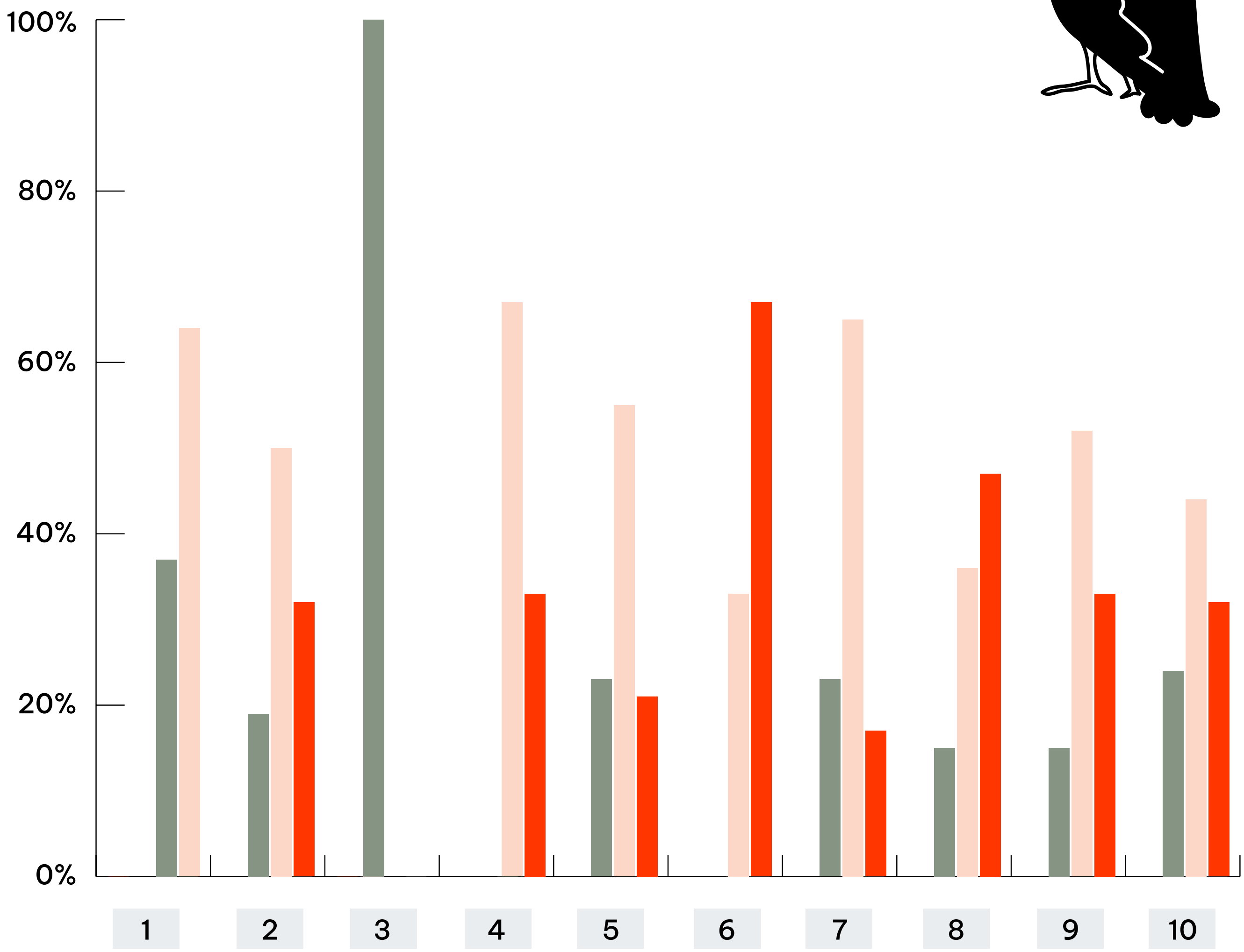
1	Education	4	Wholesale and retail trade	7	Healthcare	10	Business
2	Industry	5	Government	8	Information and communication		
3	Construction	6	Transport and storage	9	Finance		

■ Not at all

▨ Not particularly

□ Yes, somewhat

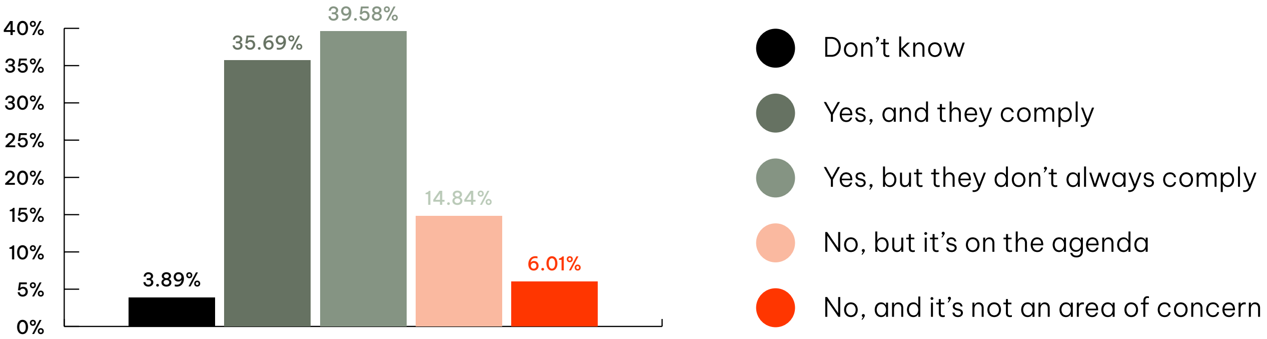
🟥 Yes, absolutely



Managers may be setting a bad example for employees

At 36%, the number of managers complying with security requirements is considerably higher than employees. However, this leaves an enormous 60% of managers still regularly failing to act according to security requirements.

In your opinion, are managers aware of IT security requirements for remote working?



Raising awareness is not a priority

Our survey also found that 6% of managers believe that communications security awareness is not a priority; 4% of managers indicate that they do not know whether employees are even aware of how to communicate securely.

No matter how small the segment, a lack of focus on data security is concerning, particularly in an increasingly digital world.

Are security professionals worried about the security of digital communications?

The short answer is 'no': an enormous 70% of security professionals are not concerned by digital communications security.

However, this stands in contrast to other responses. Respondents emphasised the ongoing security challenges they are facing, particularly in relation to remote-working employees and their repeated failure to comply with imposed security measures.

What can we conclude from this? It seems that there is a widespread misconception of where hazards lie on the matter of communication security. While respondents referred to risks in relation to both outbound and inbound communication, attention is primarily focussed on inbound (e.g. phishing, hacking, malware etc), leaving much room for error in outgoing emails and file sharing.

STATEMENT: How concerned are you about the security of transmitted data and sensitive information?

Not at all concerned

Very concerned

1	2	3	4	5
38%	33%	19%	8%	2%

04

Data breaches: prevention is better than cure

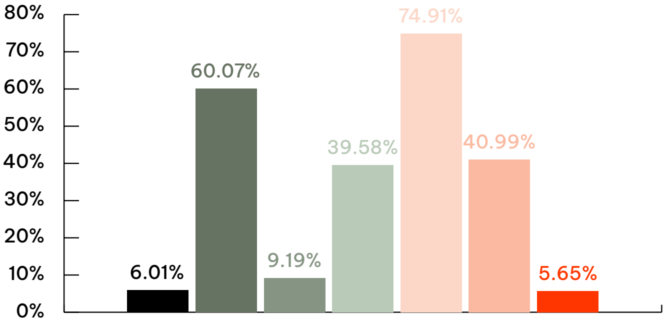
Causes of data breaches

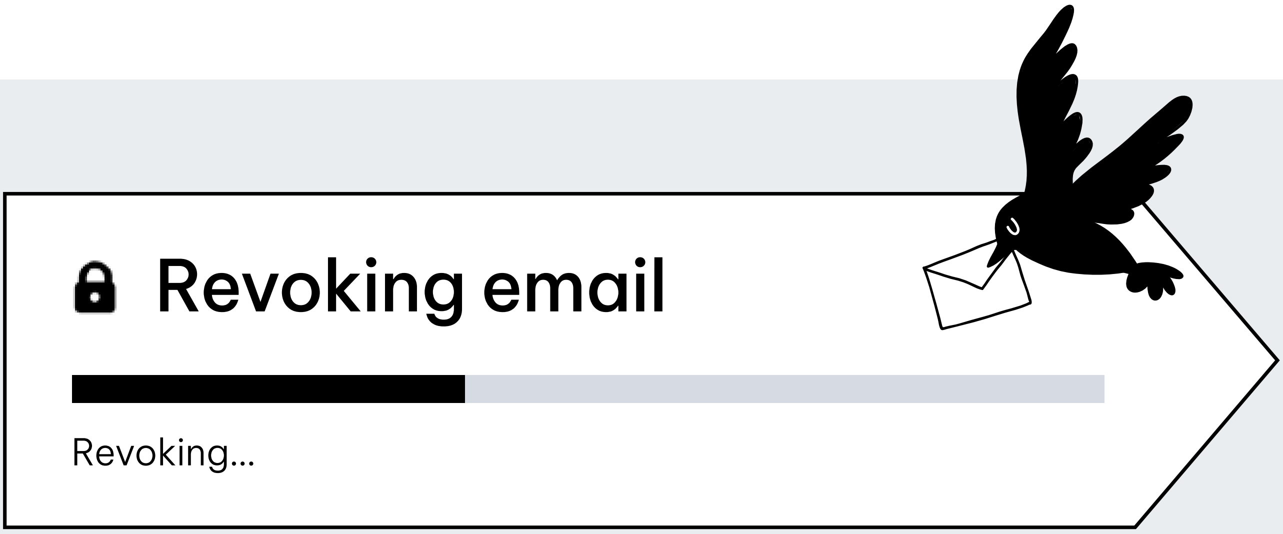
Outbound communications account for the majority of data breaches.

There is a discrepancy between the actual and perceived causes of data loss incidents. While nearly 75% of respondents see hacking, malware and phishing as the primary threats to their data, the Dutch Data Protection Authorities annual report shows such inbound threats account for the smallest percentage of data breaches, at just 5% of all cases.

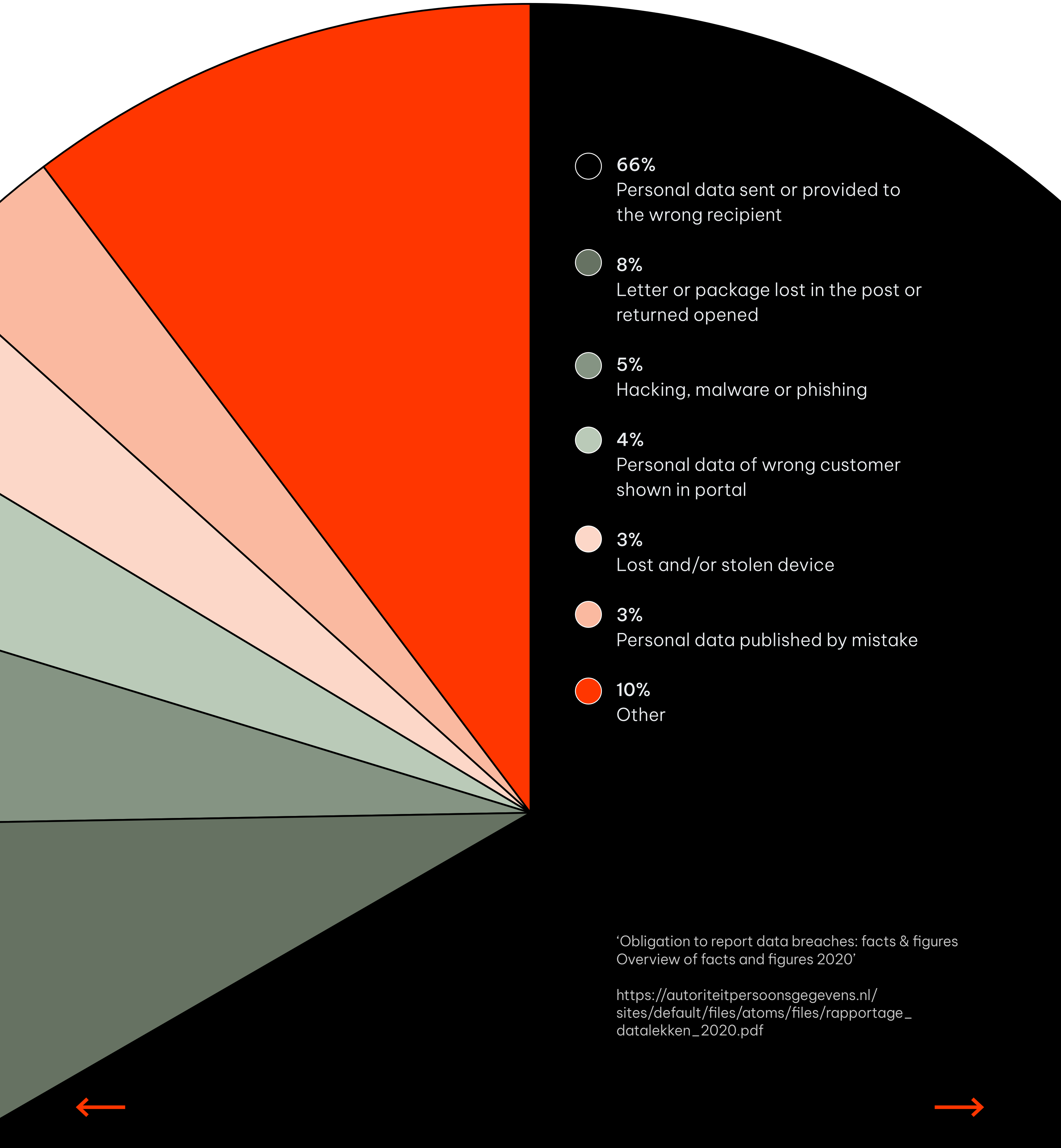
What possible causes of data breaches do you perceive to be a threat to your organization in the near future?

- ● None
- ● Personal data sent or provided to the wrong recipient
- ● Letter or package lost in the post or returned opened
- ● Device, data carrier (USB stick) and/ or documents lost or stolen
- ● Hacking, malware, and/or phishing
- ● Personal data shown to an unauthorized person
- ● Other, namely





Causes of data loss incidents



‘Obligation to report data breaches: facts & figures Overview of facts and figures 2020’

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf

While the causes of data breaches remain misunderstood, resources to improve communications security will continue to be channeled in the wrong areas. The key question for security professionals, therefore, should be: “Is your outbound communication as secure as your inbound communication?”

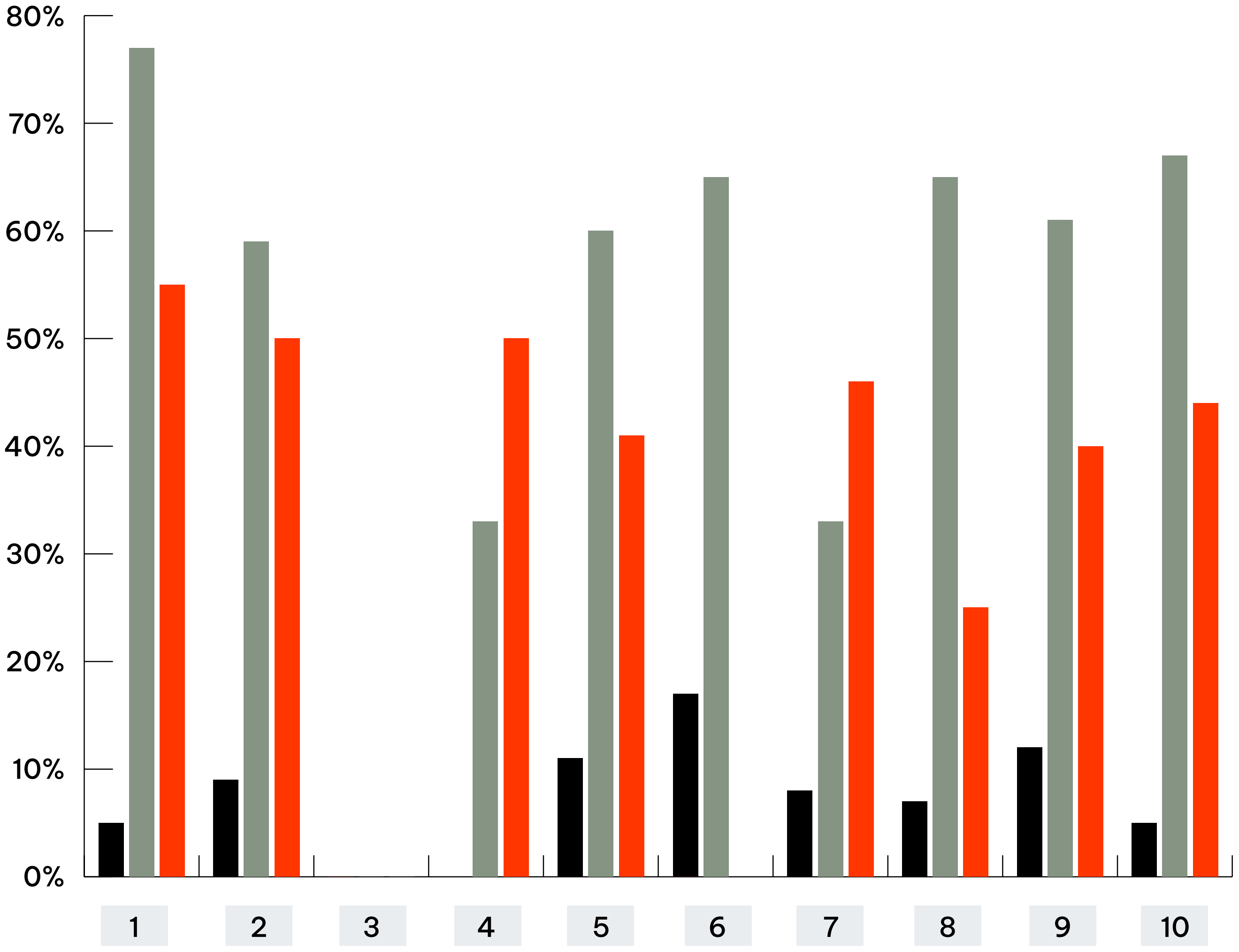
Which sectors consider outbound communication to be a major risk for data breaches?

1	Education	4	Wholesale and retail trade	7	Healthcare	10	Business
2	Industry	5	Government	8	Information and communication		
3	Construction	6	Transport and storage	9	Finance		

⬛ Letter or postal package lost or opened returned received

▨ Personal data sent or provided to the incorrect recipient

🟥 Personal data shown to the incorrect individual



Increase in data breaches caused by hacking, malware and/or phishing

Reports of data breaches caused by hacking, malware and/or phishing are on the rise, according to the Dutch Data Protection Authority in March 2021: "The Dutch Data Protection Authority is detecting an explosive increase in the number of hacks aimed at capturing personal data. The number of reports rose in 2020 by no less than 30% compared to the previous year."

At the same time, chair of the Dutch Data Protection Authority, Aleid Wolfsen, has sounded the alarm. The advice seems simple, but according to Wolfsen, a large number of organizations still do not utilize multifactor authentication: "When people share their personal data with organizations, they assume their data will be treated confidentially. Unfortunately, this is not always the case. Often, proper security measures could have easily prevented a great deal of harm. Although multifactor authentication is a simple security measure that is compulsory when processing sensitive personal data, it should be compulsory in organizations as standard, to prevent harm."

> "Because of the proliferation of links and the failure to put proper procedures in place for identity and access management, a lot of data is still available to, or retrievable by, groups of people who, in my opinion, should have no access or restricted access. I do have to point out that we are doing a lot of good work here. We are also running an IGA (Identity Governance and Administration)"
>
> – Respondent

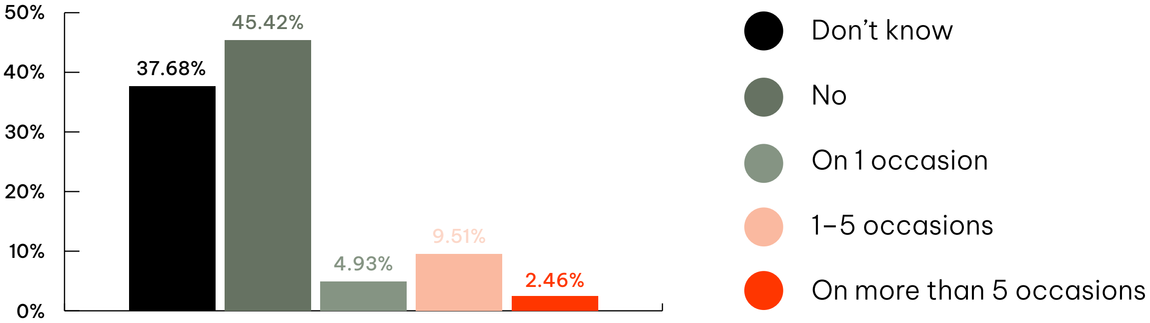
Has your organization experienced any data breaches since remote working has become the norm?

Alongside misconceptions concerning the leading causes of data breaches, gaining a complete overview of data security also appears to be a challenge for many organizations. Nearly 40% of respondents are reportedly unsure whether there has been a data breach in their organization since their workforce became remote.

> “Lack of security awareness due to a focus on speed and efficiency was the reason for a data breach in our company.” – Respondent

Although this is cause for concern, almost half of respondents reported zero data breaches in their organization during the pandemic. This is a positive outcome. Despite drastic changes to our way of working, many organizations appear to be managing security procedures effectively.

Did your organization suffer a data breach during the pandemic?



05 What does the future hold?

Security investments in 2020 compared to 2021

We asked respondents to what extent they expect security budgets to change as a result of remote working. Over 82% of respondents expect an increase in 2021.

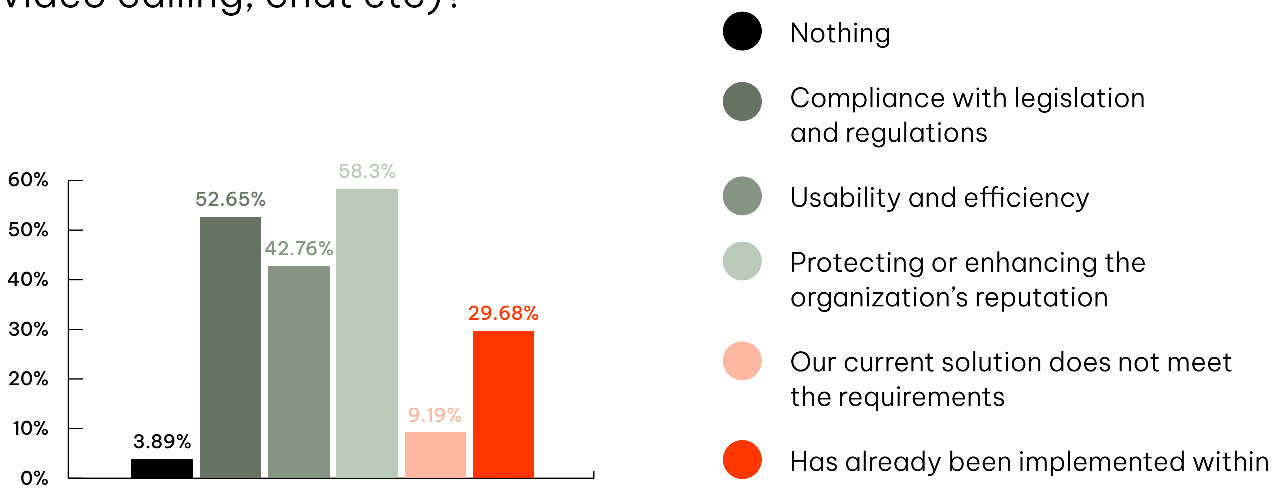
STATEMENT: Cybersecurity budgets will increase in 2021 compared to 2020

Completely agree	Partly agree	Partly disagree	Completely disagree
32.75%	49.65%	10.92%	6.69%

We also asked respondents to share their motivations for investment in secure communication solutions. Compliance with data legislation and regulations plays an important role in the decision making process; in the healthcare and information and communication sectors, this is the most important driver.

58% of respondents also referred to protecting and enhancing their organization's reputation. Customer expectations around the use of their data is increasing; no organization can afford a data breach today. Of equal importance, however, is customer communications. Ensuring customers have a positive experience when managing and accessing communications from an organization, particularly when said communications include sensitive and personally identifiable information (PII), is imperative.

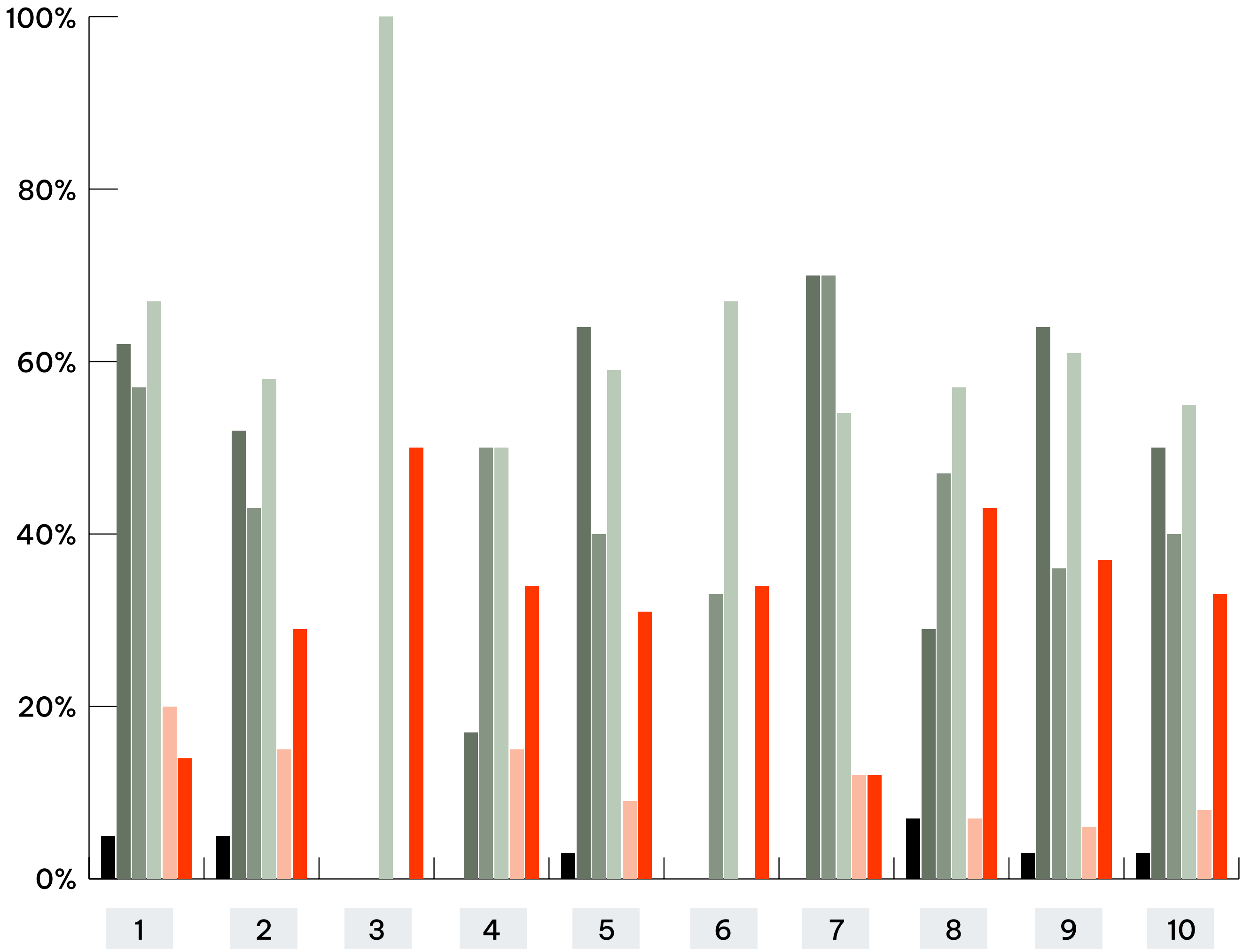
What would motivate you to invest in an additional layer of security within digital communication (e.g. email, file transfer, video calling, chat etc)?



What would motivate you to invest in an additional layer of security within digital communication (email, file transfer, video calling, chat etc)?

1	Education	4	Wholesale and retail trade	7	Healthcare	10	Business
2	Industry	5	Government	8	Information and communication		
3	Construction	6	Transport and storage	9	Finance		

- ⬛ Nothing
- 🟩 Compliance with legislation and regulations
- 🟩 Usability and efficiency
- 🟩 Protecting or enhancing the organization's reputation
- 🟧 Our current solution does not meet the requirements
- 🟥 Has already been implemented within



06 Five recommendations for security success

01 Outbound is the new inbound

In recent years, inbound communication has dominated the conversation around cybersecurity. While hacking, malware and phishing clearly have a place in the narrative around communication security, business leaders must reconsider 'traditional' security measures in light of a new remote working culture.

Employees are handling more data than ever, and email traffic is on the rise; with 80% of data incidents resulting from human error (incorrect recipients, misuse of Bcc/Cc etc) it is time to shift focus to outbound communications. Fortunately, industry experts, including Gartner, foresee a rising interest in securing outbound communications in 2021 and 2022.

02 Find the balance between security and usability

Prioritize usability when it comes to security tools. If the imposed security measures only serve to inconvenience employees, they are unlikely to use them, undermining security efforts in the long term. Make security accessible and employees will be empowered to work securely and efficiently.

03 Master the basics and share best practice

Establish a strong groundwork and build from there. Consider patching vulnerabilities, training employees, and implementing zero-trust access with multi-factor authentication (MFA). And, of course, secure endpoints, cloud, and applications. With a solid security infrastructure in place, establishing additional platforms, policies and procedures to empower a remote workforce will be simpler and successful.

04 Do not over-complicate

Work with security vendors who can help to simplify existing security infrastructure. Integrating new security measures into current working methods guarantees uptake amongst end users, promising greater efficiencies in the short and long term. For example, integrating software for secure communication in your organization's preferred communications solutions (e.g. Outlook, Gmail, Salesforce, the Zaaksysteem or Electronic Patient Files) will streamline processes, improve stakeholder experiences, and drive efficiencies.

05 Listen to your people

Security professionals and business leaders must reevaluate the role of people in data protection. Employees must not be viewed as a security risk; instead, they should be empowered with the appropriate tools and awareness to be their organization's greatest security defence.

About Zivver

Since 2015, Zivver has supported more than 4,000 organizations to make secure email the standard with every message and file sent. Known for our innovative and user-friendly approach to outbound security, we enable employees to be their business's greatest security defence.

Zivver protects outbound emails before, during and after hitting 'send', with unbeatable security measures, advanced encryption, and machine learning technology to alert users in real-time to potential errors. Flawless integration with Gmail, Outlook and O365 enables users to share confidential information without leaving the comfort of their familiar email client.

Designed to deliver an effortless user-friendly experience for both the sender and recipient, we make receiving secure emails easy; recipients needn't battle with account creation, and senders can maintain control once their message is received, with simple and effective recall and expiration functionality.

Featured on the esteemed Cybertech 2021 list for innovative tech providers, ranked second in the Deloitte Technology Fast 50 for 2020, and with a 99% renewal rate, our platform is recognised for its usability and seamless integrations - making it one that employees want to use, every day

Trusted by

de Rechtspraak

nationale nederlanden

Foundation Home Loans

NHS West Suffolk NHS Foundation Trust

zivver

Zivver
Kon. Wilhelminaplein 30
1062 KR Amsterdam, Netherlands

+31 85 016 0555
contact@zivver.com

www.zivver.com

linkedin.com/company/zivver facebook.com/zivver @zivver_en