

WHITEPAPER

TOP SMB IT PAIN POINTS & SOLUTIONS

WHAT DOES THE RESEARCH SAY?

JUNE 2021





contents

Document

Executive Summary	3
Key Findings	3
Recommendations	3
Introduction	4
Survey Methodology/Demographics	4
Top IT Pain Points in SMBs	5
Security and Data Protection Challenges	5
Challenges Around Adopting New or Emerging Technologies	7
Operational Employee Challenges	11
Obstacles Around Communications and Collaboration	11
Connectivity/Business Continuity Issues	12
Other Work-From-Home Issues	13
Opportunities to Address Pain Points	15
Security Solutions	15
IT Security/Cybersecurity	16
Printer Device Security	16
Information Security Consulting	17
Video Security	17
Digitalisation Solutions	17
Document Capture and Management Paired with Enterprise Search	17
Digital Contract Management	18
Digital Mailroom	19
Operational Employee Solutions	19
Communication and Collaboration Tools	19
Connectivity/Business Continuity Solutions	20
Remote Work Solutions	20
Opinion	22



Tables

Table 1: Percent of Respondents Experiencing Different Security Issues Over Last Two Years 6

Table 2: Impact of COVID-19 Pandemic on Level of Digitalisation and Electronic Approvals 10

Figures

Figure 1: How many computer-based employees work at your company?..... 4

Figure 2: What are your company's current major IT challenges? Please select the top 5. 5

Figure 3: What, if any, are the IT challenges around employees working remotely from home? 7

Figure 4: In which technologies or capabilities, if any, did your company acquire or upgrade as a result of the COVID-19 7

Figure 5: What are the main reasons your organization maintains paper documents? 8

Figure 6: What percentage of your company's business content remains on paper? 9

Figure 7: Why is there an increased level of digitalisation at your company? Please select all that apply..... 10

Figure 8: What are the business operations challenges resulting from employees working remotely? 11

Figure 9: What have been the IT challenges employees have experienced due to the COVID-19 pandemic? Please select the top 5..... 12

Figure 10: What are your company's priorities around data storage and backup? Please select all that apply. 13

Figure 11: How challenging has managing remote work been for your organization's IT staff? 14

Figure 12: Konica Minolta 360-View of Security is an Example of a Comprehensive Security Approach..... 15



Executive Summary

IT decision makers within small and medium-sized businesses (SMBs) are tasked with many responsibilities, but some of their greatest concerns relate to security, adopting new technologies, and ensuring employees are properly equipped to do their jobs. These challenges are often associated with past experience: For example, two-thirds of SMBs surveyed said their company has experienced a malware incident in the last two years. They are also tied to the potential stakes of not addressing these issues. Indeed, a security breach can result in comprised customer relationships as well as large regulatory penalties, while manual processes and/or poorly executed technology projects can result in many headaches, demoralized employees who may leave the company, and significant financial waste. The good news is that technology solutions and services exist to address these challenges, including security products, software to digitize key processes, platforms and tools for improved employee communication and collaboration, business continuity, and remote working.

Key Findings

- ♦ As of Q1 2021, SMBs' top IT obstacles included security and data protection, adopting new or emerging technologies, and enabling workers to adequately perform their daily jobs.
 - Many of these challenges were exacerbated by the COVID-19 pandemic and its numerous ramifications.
- ♦ SMBs with 50-199 employees (versus those with 200-250 employees), as well as those in Western Europe mainland countries, appear to be facing a higher level of IT pain points.
- ♦ Underlying reasons for putting off technological investments include concerns around affordability, systems integration, and privacy.

Recommendations

- ♦ Determine how your organization's top IT pain points compare to those most commonly being experienced by SMBs.
- ♦ Assess the extent to which your IT roadmap addresses the top challenges and priorities; adjust accordingly.
- ♦ Invest in the right technology and services to alleviate your top pain points as well as fulfil your leading business objectives.
 - A wide range of affordable and customizable security, digitalisation, communication and collaboration, network optimization, and business continuity solutions exist to address differing concerns.



- To best implement and maintain these solutions, it may be worth partnering with a reputable managed services provider with deep IT expertise.

Introduction

With IT the backbone of many SMBs, it's imperative that it functions smoothly to maximize worker productivity and satisfaction. While a simple application or new piece of hardware may be fairly easy to integrate into the organization, as more components are added the potential for challenges increases. This is especially true in the ongoing COVID-19 landscape, with more work environments and technological elements in place. This white paper will discuss the top IT pain points that today's SMBs are facing as well as potential solutions for alleviating these difficulties.

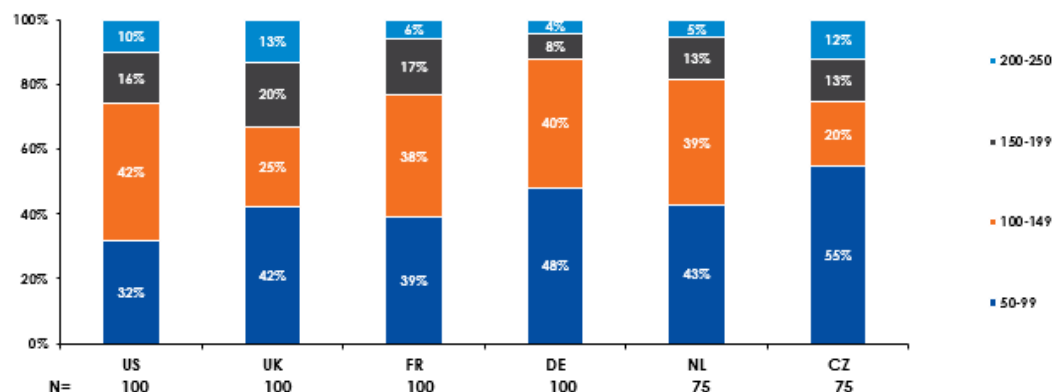
Survey Methodology/Demographics

In February-March 2021, Keypoint Intelligence (on behalf of Konica Minolta) conducted a web survey of 550 SMB IT decision makers spread across the Czech Republic, France, Germany, the Netherlands, the United Kingdom, and the United States. These individuals came from a mix of companies with 50-99, 100-149, 150-199, and 200-250 computer-based employees (with the average company size at 119 computer-based employees), as well as a variety of economic sectors—with professional services, manufacturing, and healthcare most represented. Most were the main decision maker for the most recent IT-related decisions (67%), while the rest were heavily involved in the decision-making process (29%) or somewhat involved in the decision making (5%). In line with this finding, the large majority were very or extremely familiar (89%) with their company's IT and held roles like president/CEO/owner (34%) and IT manager (37%). As SMBs, on average they had 2.5 internal company staff dedicated only to managing or maintaining IT.

550

Number of IT decision makers surveyed in Keypoint Intelligence and Konica Minolta's 2021 SMB IT and Business Operations Pain Points Study.

Figure 1: How many computer-based employees work at your company?



Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

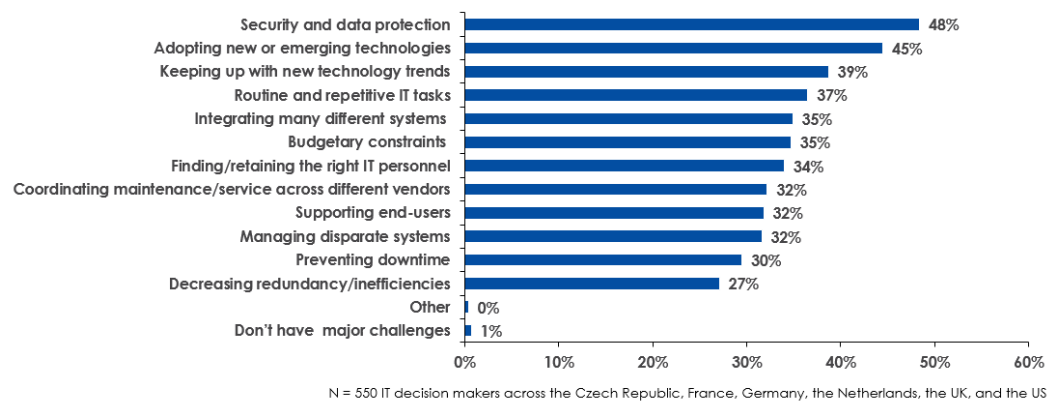


Top IT Pain Points in SMBs

Security and Data Protection Challenges

The study revealed that the top IT challenge facing SMBs is security and data protection (48%), followed by adopting new or emerging technologies, and keeping up with new technology trends. This leading challenge does vary a bit by country, however, with Germany and the Netherlands more likely to cite adopting new or emerging technologies as the number one priority. We also saw some differences by company size category, with the 150 to 199 employee size segment seeing the adoption of new or emerging technologies as the leading IT obstacle. When viewing these results in conjunction with other survey results, however, it becomes clearer that security is a major pain point in every single region and company size category surveyed.

Figure 2: What are your company's current major IT challenges? Please select the top 5.



Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

For instance, more than 40% of respondents in each company size category have experienced what they consider a security breach (48% in total), while even more have experienced specific issues over the last two years—such as a malware incident (67% in total) or lost/exposed passwords (56% in total); these issues are particularly prevalent in Germany and the Netherlands as well as SMBs with fewer than 200 employees.

67%

Of respondents report their company has experienced a malware incident in the last two years.



Table 1: Percent of Respondents Experiencing Different Security Issues Over Last Two Years

Attack Type	No Incident	Not aware	Mild Incident	Severe Incident
Phishing	29%	20%	38%	13%
Ransomware	30%	19%	35%	17%
Internal (employee) intentional damage	27%	22%	30%	21%
DDoS	26%	22%	32%	20%
Malware/virus	16%	17%	47%	20%
Employee leaving with company data/trade secrets	34%	24%	33%	9%
GDPR data issue	32%	19%	30%	19%
Endpoint compromised	30%	22%	27%	21%
Passwords lost/exposed	23%	23%	34%	22%
Other data Leak	32%	23%	29%	16%

N = 550 IT decision makers across the Czech Republic, France, Germany, the Netherlands, the UK, and the US

Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

It appears the COVID-19 crisis has exacerbated security-related issues within many organizations, with 37% of respondents citing a virus/malware/security threat as an IT challenge experienced by employees due to the pandemic (see Figure 9 below). There wasn't much variety between countries on this question, with the exception of the Czech Republic, which was much less likely (18%) to identify security as a pandemic-caused issue. In terms of company size, organizations with fewer than 200 employees were more likely to cite security as a pandemic-triggered issue.

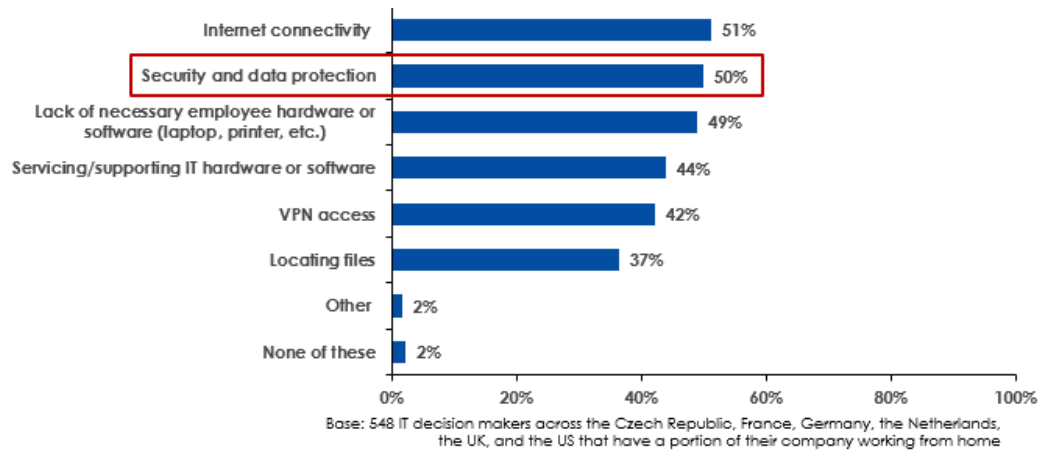
It is not surprising that COVID has prompted security-related challenges in many companies, given that it resulted in so many people working from home—in environments that weren't necessarily as secure as the traditional office. On average, about 46% percent of workforces were working from home at the time of the survey—without all that much variation by country or company size. Of the respondents stating at least some of their company's employees work from home, a whopping 50% cited security and data protection as an IT challenge around associated with home-based working—making it second in importance only to Internet connectivity. Once again, the Czech Republic appears to be seeing these kinds of problems at a lower rate.

1/2

One in two companies that support working from home identified security and data protection as an IT challenge.



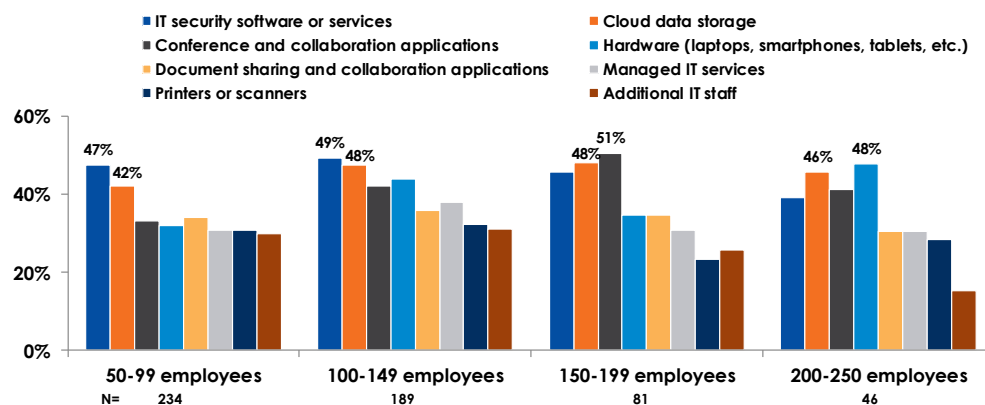
Figure 3: What, if any, are the IT challenges around employees working remotely from home?



Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

As a result of COVID-19-related challenges, 47% of all respondents acquired or upgraded IT security software or services—making it the top area of investment. Respondents in the Netherlands (58%) and United States (50%) were most likely to be spending on security, while those in the Czech Republic (33%) least commonly did so. In terms of company size, the largest of SMBs (200-250 employees) were the least likely to have invested in security.

Figure 4: In which technologies or capabilities, if any, did your company acquire or upgrade as a result of the COVID-19



Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

Challenges Around Adopting New or Emerging Technologies

As mentioned above (and shown in Figure 2), the number two and three IT challenges facing SMBs surveyed are adopting new or emerging technologies (45%) and keeping up with new technology trends (39%). These two challenges are very much related, as they both are centered on organizations identifying and implementing new and beneficial



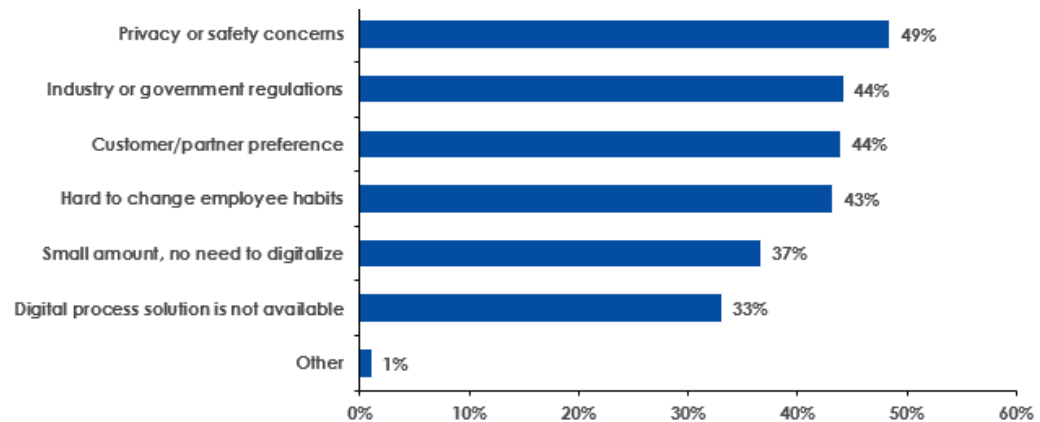
49%

Of organizations maintain paper documents (versus adopting digital processes and technology) due to privacy and safety concerns.

technologies. It is interesting to see that larger SMBs (those with 150-199 and 200-250 employees) are more likely to consider these obstacles—possibly reflecting the larger scale involved with new IT projects in their organizations.

These challenges may be intertwined with other noted pain points, including budgetary constraints (35%), integration issues (35%), and privacy/safety concerns—the latter of which 49% of respondents say this is the main reason why paper documents are maintained. If IT decision makers are concerned about the impact new digital technologies may have on the privacy or safety of employees, clients, and even suppliers, it makes sense they are hesitant to spend money on these products and services. While paper-based processes may be old-fashioned and time-consuming, they are perceived by many as proven methods of privacy protection.

Figure 5: What are the main reasons your organization maintains paper documents?



N = 550 IT decision makers across the Czech Republic, France, Germany, the Netherlands, the UK, and the US

Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

That said, it's also clear there are tradeoffs associated with legacy systems. For example, 37% of respondents cited routine and repetitive IT tasks as a major IT challenge (which could potentially be solved by increased automation), and 37% also indicated that locating files is an IT challenge associated with working from home (which could be addressed with more modern and user-friendly cloud-based document management systems). It appears routine and repetitive tasks are especially an issue in Germany (44%), the Netherlands (43%), and companies with fewer than 150 employees (39%), while locating files while working from home is most challenging in France (45%), the Netherlands (43%), the United Kingdom (42%), and companies with fewer than 200 employees (38% vs. 24% in companies with 200 to 250 employees). It is very possible the largest of SMBs already have more technology in place to address these kinds of problems.

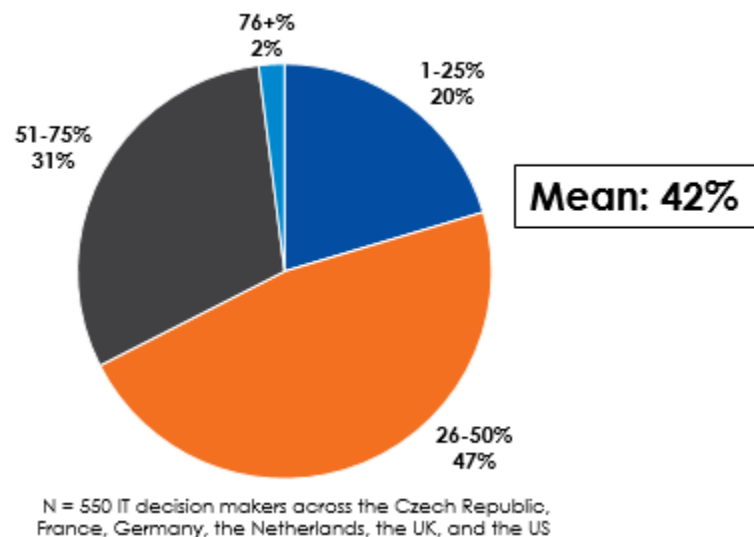


42%

Of business content still remains on paper, on average.

Another drawback of not implementing new and emerging digital technologies is the sheer amount of paper that is still being used, cutting into budgets and resulting in more manual work for employees. According to the survey, 42% of business content still remains on paper—across all companies represented. Hardcopy penetration rates are particularly high in France (47%), Germany (45%), and the Netherlands (44%) as well as companies with fewer than 200 employees (42%). Consistent with other survey results, the largest SMBs (those with 200 to 250 employees) have the lowest portion of business content on paper (35%).

Figure 6: What percentage of your company's business content remains on paper?



Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

65%

Of organizations saw increased digitalisation due to the COVID-19 pandemic.

All that said, some investments certainly have been made as of late (see Figure 4 above). In addition to IT security software or services (47%) mentioned earlier, the survey showed that quite a few organizations acquired or upgraded cloud data storage (45%), conference and collaboration applications (40%), and various other technologies and IT resources. This helps explain how most companies have been able to increase the level of digitalisation (65%) and electronic approvals (68%) occurring since the start of the COVID-19 pandemic. In the Czech Republic, however, fewer than half of respondents noted increased digitalisation (41%) and electronic approvals (48%); as for company sizes, digitalisation was less likely to have occurred because of COVID in companies with 200-250 employees (57%)—most likely because they had already achieved significant digitalisation pre-COVID. We also saw that digitalisation and electronic approvals were most likely to have increased in companies in France (76% and 82%, respectively) and the Netherlands (72% and 79%, respectively), as well as those with 150 to 199 employees (72% and 75%, respectively).

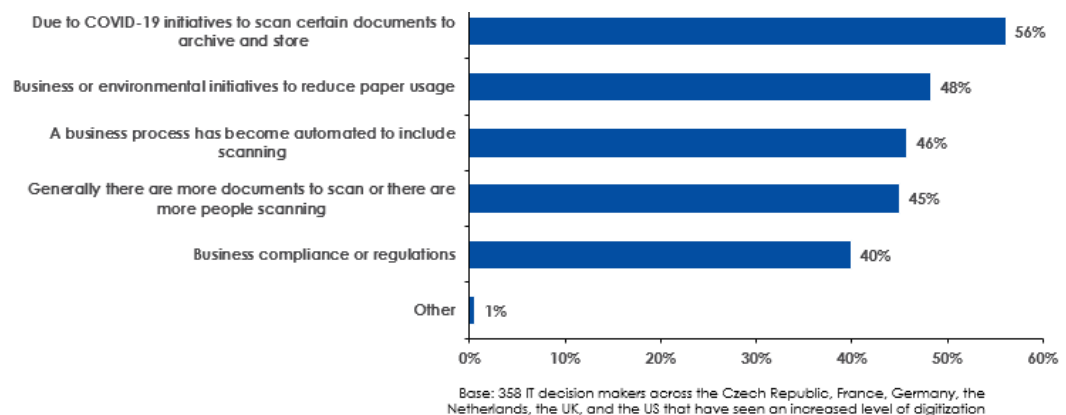
**Table 2: Impact of COVID-19 Pandemic on Level of Digitalisation and Electronic Approvals**

	Increased	Same level	Decreased
Level of digitalisation	65%	33%	2%
Quantity of electronic approvals	68%	30%	2%

N = 550 IT decision makers across the Czech Republic, France, Germany, the Netherlands, the UK, and the US

Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

To better understand the factors driving increased digitalisation, respondents were asked to indicate why this is taking place. Clearly, scanning initiatives prompted by COVID were a key driver (56%); factors like environmental initiatives, business process automation, the existence of more documents, and compliance requirements were also cited by many companies. Scanning initiatives were particularly prevalent in the United States (65%) and France (65%), while environmental factors were most frequently cited by French respondents (53%). While IT decision makers in the Czech Republic were least likely to identify COVID-19 scanning initiatives (26%), business or environmental initiatives to reduce paper (36%), or business compliance or regulations (23%) as factors for increased digitalisation, they were most likely to cite the increase in documents (52%) as a reason.

Figure 7: Why is there an increased level of digitalisation at your company? Please select all that apply.

Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)



51%

Of respondents identify communication with managers or other employees as a business operation challenge resulting from work-from-home arrangements.

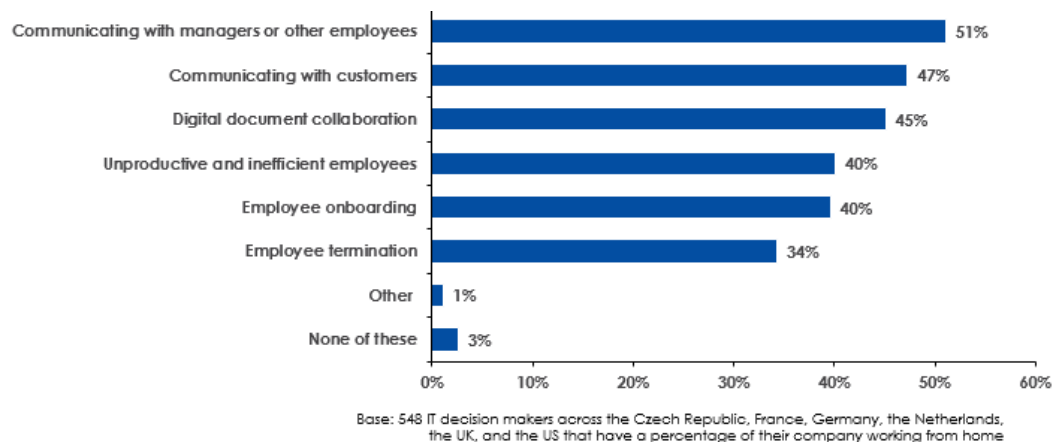
Operational Employee Challenges

Other top IT issues relate to how employees are able to go about their daily jobs. The survey revealed, for instance, that quite a few challenges exist around enabling employees to communicate and collaborate with others; access their work materials without issues; and have the appropriate training, technology, and support to do their jobs.

Obstacles Around Communications and Collaboration

When asked about the business operations challenges resulting from employees working remotely, IT decision makers were most likely to cite communicating with managers or other employees (51%), communicating with customers (47%), and digital document collaboration (45%). Once again, these issues seem less common in the Czech Republic (39%, 42%, and 30%, respectively).

Figure 8: What are the business operations challenges resulting from employees working remotely?

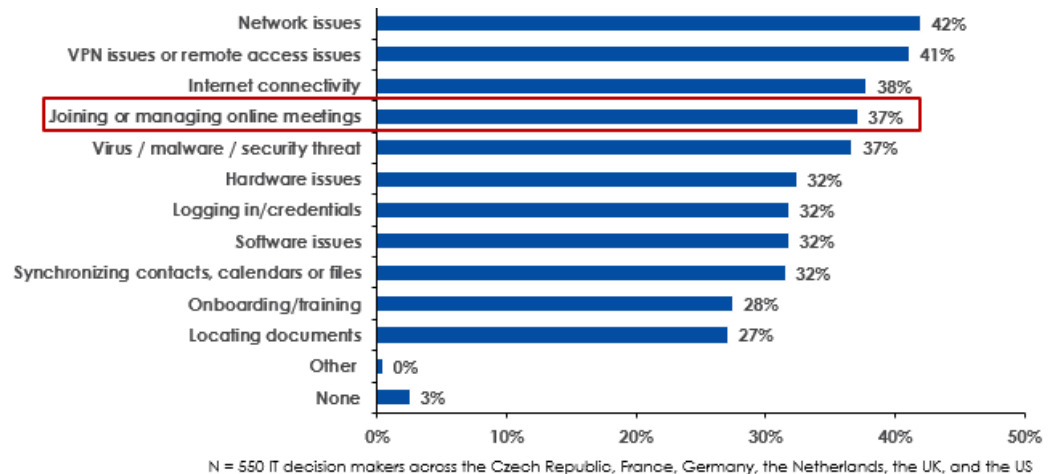


Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

Issues around communication are reinforced by the fact 37% of respondents identified joining or managing online meetings as a top IT challenge that employees have experienced due to the COVID-19 pandemic. Joining or managing online meetings appears particularly problematic in France (46%) and in companies with 50 to 99 employees (41%).



Figure 9: What have been the IT challenges employees have experienced due to the COVID-19 pandemic? Please select the top 5.



Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

These organizations may not have had top-notch conferencing and collaborations systems in place pre-COVID to ensure that business could be satisfactorily conducted once COVID hit. While many organizations (40%) (see Figure 4 above) acquired or upgraded their conference and collaboration applications as a result of the COVID-19 pandemic, this was especially the case in Germany (45%), the United States (44%), and companies with 150 to 199 employees (51%). As for document sharing and collaboration applications, 35% acquired or upgraded these solutions during the pandemic; this was most common in the United States (42%).

Connectivity/Business Continuity Issues

Being able to connect to the network and work resources is clearly another pain point in SMBs. As shown in Figure 9 above, network issues (42%), VPN issues or remote access issues (41%), and Internet connectivity (38%) are the top three IT challenges facing employees as a result of the COVID-19 pandemic. As a whole, these issues appear to be impacting the United States and the United Kingdom the most, possibly reflecting weaker Internet infrastructures in these regions (the United States in particular faces challenges related to its size and many rural areas), as well as the largest of SMBs. Indeed, SMBs with 200 to 250 employees must guarantee that their full range of employees—across all of their work locations—can access the Internet and company network with minimal issues.

Another issue being experienced by a decent portion of companies surveyed is challenges around data backup and disaster recovery. The survey showed that 21% of companies back up and recover data manually, while another 14% simply do not practice data backup and disaster recovery. Companies in the Netherlands (23%), France (19%), and those with 150 to 199 employees (19%) are the least likely to be practicing data

42%

Number of employees experiencing network issues due to the COVID-19 pandemic.



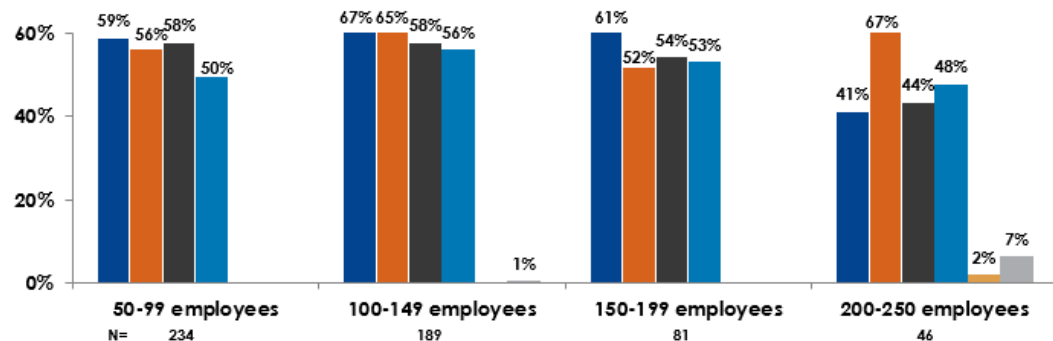
61%

Of respondents say improving disaster recovery capabilities is a data storage and backup priority.

backup and disaster recovery—suggesting there are ample opportunities to serve customers in these segments with data backup and disaster recovery solutions.

Even though most companies are using a dedicated backup and disaster recovery system (either their own system or through a third-party service), the majority of companies surveyed say improving disaster recovery capabilities (61%), consistently practicing data backup (60%), increasing visibility into where specific data is stored (56%), and being in compliance with regulations and laws (52%) are top priorities around data storage and backup. Overall, these priorities are greatest among companies in Germany, France, and with 100 to 149 employees, and smallest among those in the Czech Republic and with 200 to 250 employees.

Figure 10: What are your company's priorities around data storage and backup? Please select all that apply.



Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)

Other Work-From-Home Issues

Respondents also indicated various other pain points related to work-from-home arrangements. For example, one-third said that employees have experienced hardware issues due to the pandemic (see Figure 9 above); this was especially true in the Netherlands (44%). Many new work-from-home employees quickly learned that their computing, peripheral, and network hardware weren't adequate for full-time home-based working (or even part-time working for that matter). They may have required new technology or maintenance or software updates to ensure they could work productively (and securely) at home. A greater percentage of respondents (49%) said that a lack of necessary employee hardware or software was an IT challenge associated with employees working from home (see Figure 3 above); respondents in the UK (56%), France (55%), the Netherlands (55%), and Germany (53%) as well as those in companies with 100 to 149 employees (56%) saw this as the biggest challenge.

49%

Of respondents cite lack of necessary employee hardware or software as an IT challenge associated with home-based working.



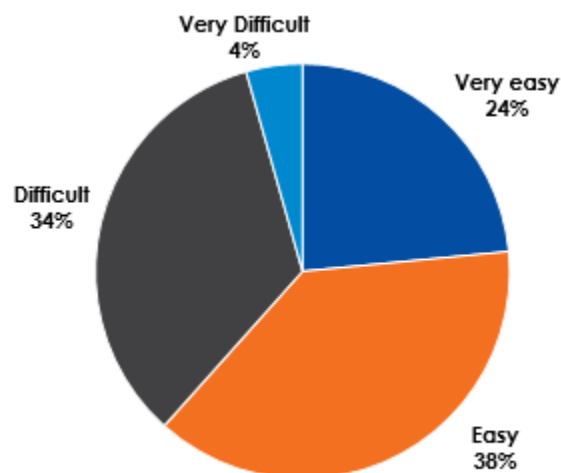
38%

Of IT decision makers view managing remote work as difficult or very difficult.

As for servicing/supporting IT hardware or software specifically, 44% of IT decision makers identified this as an IT challenge around employees working from home. Those in Germany (48%), the United States (48%), and France as well as in organizations with 100 to 149 employees (49%) saw this issue at a greater rate. Indeed, unless they work in IT themselves (or live with an IT expert), work-from-home employees do not have access to on-site IT staff to help troubleshoot and resolve technology problems. Remote servicing and support can certainly help in many instances, but it doesn't always provide the most efficient result.

Other challenges reside around onboarding and managing remote employees. As shown in Figure 8, 37% of respondents identify employee onboarding as a business operations challenge resulting from employees working remotely. And once the employee is up and running, many IT staff face difficulties managing remote workers and their environments. In fact, 38% of respondents say managing remote work is difficult or very difficult; this is particularly true in Germany (44%) and the largest of SMBs (48%)—possibly because there are more workers and environments to keep track of.

Figure 11: How challenging has managing remote work been for your organization's IT staff?



N = 550 IT decision makers across the Czech Republic, France, Germany, the Netherlands, the UK, and the US

Source: 2021 SMB IT and Business Operations Pain Points Study (Keypoint Intelligence/Konica Minolta)



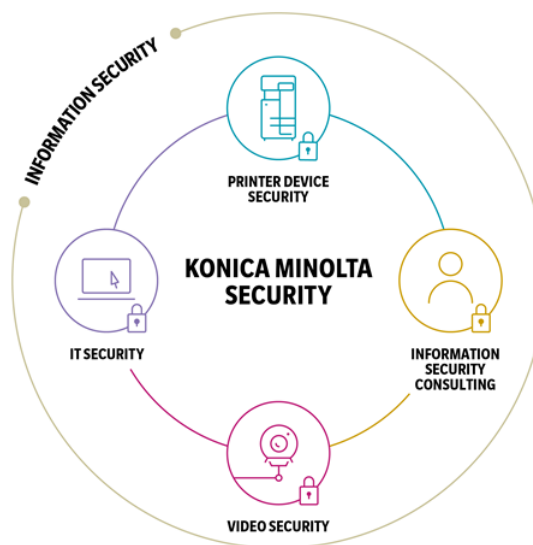
Opportunities to Address Pain Points

It's evident from Keypoint Intelligence and Konica Minolta's 2021 *SMB IT and Business Operations Pain Points* study that SMBs in Europe and the United States are facing a range of IT challenges, particularly when it comes to security, adopting new technologies, and equipping employees with the right tools to do their jobs. But there's no need for IT departments to despair. Fortunately, a breadth of solutions is available to help overcome these challenges, including technology and services for security, digitalisation, and employee productivity. Konica Minolta is one vendor providing offerings in each of these categories; several example of these products and capabilities are discussed in the paragraphs below.

Security Solutions

Protecting an organization's assets—including its information, systems, employees, and clients— isn't as simple as using an anti-virus software for computing devices. To best safeguard corporate assets, companies must adopt a comprehensive approach to security that considers the many aspects of cybersecurity as well as areas like printer device security, security compliance legislation, and even video/building security.

Figure 12: Konica Minolta 360-View of Security is an Example of a Comprehensive Security Approach



Source: Konica Minolta



IT Security/Cybersecurity

Cybersecurity is the state of being protected against the illegal or unauthorized use of electronic data, or the actions taken to accomplish this. When implemented in a thorough manner, it addresses the various ways digital information can be compromised—including through network vulnerabilities, Internet-connected devices that store electronic data, and software tools filled with business intelligence.

Cybersecurity tools exist to ensure that the network is properly segmented, the firewall is adequately configured, and devices and solutions are appropriately set up for maximum protection—all in line with security policies that have been implemented. In the event there is any kind of breach or breach attempt, these tools are ready to detect the issue and respond to it automatically—through methods like health check, malware hunting, threat hunting, digital forensics, and incident response. This includes threats that are both outside and inside the organization. In addition, regular scans and evaluations can be set to provide continuous updates on the state of IT security.

Organizations can acquire the technology to conduct these configurations, scans, and remediations themselves; they can outsource these tasks to a third-party security expert; or they can engage in a mix of security technology acquisition and third-party support. Partnering with a managed security provider on some level may be particularly valuable to SMBs that don't necessarily have extensive security expertise in house.

Printer Device Security

One area of security that is often neglected is printer device security. For various reasons, organizations don't consider their printers and multifunction printers (MFPs) to be vulnerable to security breaches. But as these machines have become more and more sophisticated, connecting to the corporate network, cloud-based enterprise software, and now home wireless networks, there are numerous ways in which they can be infiltrated by hackers. Plus, exposure of hardcopy documents to unauthorized individuals (e.g., through a document left unattended on the output tray) remains a problem.

To remove these security risks, new print technology is equipped with many standard and optional features to protect access to the device and its functions; secure the data and documents that are transmitted to and from the device (as well as stored on the device's hard drive); and immediately detect and remediate any security threat attempts. These capabilities include virus scan, fax line security, GDPR readiness, ISO 15408 certification HCD-PP, secured ports and protocols, S/MIME encryption, SMTP authentication, and user authentication methods.



Information Security Consulting

Just when a company thinks it has a handle on all the necessary information security best practices and regulations to abide by (e.g., the EU General Data Protection Regulations and international standards like ISO 27001 ff), the components of the regulations shift, more regulations are added, or new technologies demand new solutions. To stay on top of all the relevant information, security laws, and requirements, organizations may be wise to work with an information security consultant whose focus is to stay abreast of the regulation and technology landscape and make accompanying recommendations to address these changes. The cost of hiring an information security consultant can be well worth it, given the potential financial losses involved with inadequate data protection and governmental compliance.

Video Security

Protecting information is crucial but so is protecting people and physical spaces. Organizations can complement their information, network, and device security efforts with video security systems that enhance security in and outside the workplace. The latest generation of video security cameras can be linked directly to the company network, which means the existing network can be used and the cameras controlled remotely. While companies can set up a video security system themselves, partnering with a provider with strong IT security and video security expertise can guarantee that this system is designed, operated, and implemented in a reliable and comprehensive manner that satisfies companies and clients alike.

Digitalisation Solutions

Most organizations acknowledge that further digitalisation of business processes and systems is a step forward in boosting workplace productivity and gratifying employees and clients. Yet many don't know where to invest next, fearing the potential cost of a new technology, as well as the seemingly unproven nature of its compatibility with existing systems, privacy protection capabilities, and other characteristics. Fortunately, there are some easy and demonstrated ways to move a bit further along the digitalisation curve, including solutions for document capture and management (paired with enterprise search), digital contract management, electronic approval, and digital mailroom.

Document Capture and Management Paired with Enterprise Search

A key step toward digitalisation is converting hardcopy documents to digital files. There are many manual (and thus, time-consuming) ways to achieve this task. A better approach is using a dedicated document capture and/or document management solution that automates the electronic capture of hardcopy documents, extraction of data elements and application of mega data, and routing of this information to a



document management system (new or already existing) for storage and eventual search and retrieval. Some additional characteristics of these solutions may include:

- ♦ Barcode recognition
- ♦ Stamp annotation
- ♦ Image enhancement
- ♦ Document workflow initiation from a mobile device
- ♦ Routing to email and cloud-based services

While document management systems incorporate search and retrieval mechanisms, dedicated enterprise search solutions let workers locate and retrieve data in practically any format using a wide range of connected data repositories. A related offering creates insights and reports from all the indexed data, helping companies find all documents containing a certain type of data (e.g., personal identifiable information). These kinds of solutions offer strong security protections and options to help ensure information is kept confidential, as well as compatibility with existing hardware (including MFPs) and business applications. For an extra level of protection and integration, a third-party IT company can provide installation services and/or managed document services.

Digital Contract Management

One of the most commonly printed documents in today's companies are contracts, whether they are with customers, suppliers, partners, or employees. To save time and effort in creating and managing these contracts, digitising these processes is a great option. Digital contract management solutions now exist to draw up contracts digitally (e.g., using templates and automation to fill them with the correct data pulled from various tools) or at least digitise hardcopy contracts and move them into a digital workflow. Regardless of the contract's source, the information contained within is automatically indexed; staff members, parties, and signatories can be automatically notified when the contract has reached different steps in the contract creation, approval, and archival process.

With this solution, all the contracts can reside in one, central electronic database—providing full visibility to authorized users of the contracts that are—and have been—in place. Managing contracts in this way can result in less human error, better version control, and faster approvals and information retrieval. In addition, staff can perform analysis on groups of contracts, looking at (for example) past contract conditions, values, and limitations.



Digital Mailroom

Physical mail is still very much in use across the business world, providing a challenge for companies that wish to track, secure, and store all the mail they receive (physical and e-mail) in a unified manner. Companies can address this obstacle through a digital mail room solution that manages both kinds of mail. These solutions incorporate a document capture element that brings physical mail (including letters and faxes) into a document management system alongside e-mails. This results in the full range of mail—including invoices, contracts, orders, complaints, and questions—being quickly and accurately moved into a secure repository.

These solutions often do not require a large investment, as they can be created by bringing together a mix of already existing technologies—including MFPs and intelligent software that extracts pertinent information and organizes the documents. Another capability of digital mail is forwarding a digitised piece of mail to the employee it is addressed to, reaching them regardless of their location (and they receive a notification when there is new mail in their personal digital post box).

Operational Employee Solutions

Employees should have the tools they need to do their jobs productively and securely. In addition to the security and digital solutions mentioned above, technologies and services are available to help them communicate and collaborate, ensure access to the business systems they need, and work from a mix of locations.

Communication and Collaboration Tools

Most employees do not perform their work in a silo, having to communicate and collaborate with multiple colleagues on projects—often from a distance due to work-from-home arrangements and co-workers spread across offices. Being able to work with these colleagues remotely includes having an easy, cloud-based, and device-agnostic way to communicate with them (e.g., through video chat), access files and data, and use business applications (e.g., Microsoft Teams) and social networks needed for team projects.

Having all these capabilities in a single platform can help guarantee that communication and collaboration are simple, and that time won't be lost trying to find the right piece of data or remembering the right password for an individual application. When also layered with easy setup, automatic updates, top-notch security, customization, and extensive search capabilities, this kind of tool can prove invaluable to today's hybrid and knowledge workers. Similar tools can also be leveraged for client communication and collaboration (or working with other key stakeholders), extending quick, easy, and secure interactions and teamwork to more environments.



A related solution is digital document collaboration/file sharing solutions that are both modern and secure. These offerings enable fast, unlimited information exchange with the possibility of document collaboration. They can be linked to existing IT infrastructures and/or public clouds so that all files are available through a single interface. For flexibility and security purposes, users can decide whether certain data will be shared to a cloud service (and if so, which one) or stay within the organization's own on-premises cloud.

Connectivity/Business Continuity Solutions

Reliable network and/or Internet connectivity are vital for most knowledge workers, giving them a means for accessing the kinds of platforms mentioned above, and in turn their colleagues, key data and information, and necessary applications and cloud services. For SMBs with limited network expertise and resources, partnering with an IT services company to ensure network optimization is likely worth their while. This partner can continuously monitor the network, as well as analyse it for any deficiencies or improvement opportunities. As network needs shift (for example, as the number of connected systems increases), this provider can make the proper adjustments for hassle-free network performance.

This IT services provider can also provide data backup services or recommend solutions for this task. Having a comprehensive data backup plan and implementation provides the peace of mind that crucial and sensitive information will not be lost or compromised. In the event of a crisis, the system and/or service in place will enable the organization to restore every bit of information—keeping them in compliance with privacy laws and allowing employees to continue working productively.

Remote Work Solutions

With remote and hybrid work increasingly common and accepted, it is vital that these workers are equipped for working from home and/or multiple locations. An IT partner can help a company assess its remote and hybrid work landscape to determine what technology investments and adjustments are needed. This likely includes the proper computing and peripheral hardware, the right software solutions (including cloud-based software access), secured VPN access, and access to IT support in the event of a technology issue. Giving remote workers a single point of contact for their IT support needs can simplify working outside of the traditional office, enabling them to receive comprehensive advice and help versus support for a specific product only.

Investing in hybrid edge computing is another way for companies to support remote and hybrid work. A hybrid edge IT platform allows organizations to choose which data is stored and processed on site, and which data is saved and processed externally, depending on factors like security and regulatory concerns, as well as limited Internet connection speeds. For workers handling large amounts of data in remote and branch locations, it may make



sense to bring computation and data storage close to the devices where data is being gathered—at least in certain instances. A reputable IT services partner can help companies ascertain how to configure its their hybrid edge IT platform based on the needs of workers at different sites as well as security and regulatory considerations.



opinion

Opinion

There is a reason that SMBs are very much concerned with IT security, investments in new and digital technologies, and keeping their employees up and working productively. These things are crucial to the successful operation of a company, from a financial, compliance, competitive, employee satisfaction, and even physical safety perspective. COVID-19 exacerbated many of these concerns, but fortunately there are many possible solutions to each of these challenges. From comprehensive security offerings that address network security, printer security, and video security, to software solutions that efficiently transmit paper-based information to user-friendly, searchable document management systems, to platforms for employee collaboration and communication, data backup, and remote working; now more than ever companies have their choice of beneficial technology to solve key IT problems. To ensure the best implementation and support for these solutions, SMBs are encouraged to partner with an experienced IT services company—whose chief job is to stay abreast of and on top of these kinds of issues.



authors

**Christine Dunne**

Consulting Editor
+ 1 973-440-5681



Christine Dunne is a Consulting Editor for Keypoint Intelligence. Her responsibilities include responding to client inquiries, conducting market research and analysis, and providing coverage of industry events.

[Comments or Questions?](#)



Download our mobile app to access to our complete service repository through your mobile devices.



This material is prepared specifically for clients of Keypoint Intelligence. The opinions expressed represent our interpretation and analysis of information generally available to the public or released by responsible individuals in the subject companies. We believe that the sources of information on which our material is based are reliable and we have applied our best professional judgment to the data obtained.