
FIDI
FOCUS
Digitalisation for moving and relocation businesses
Guidelines for getting started
November
2023

Introduction

While almost all companies have digitalised some of their processes – most of us use email and desktop computers at the very least – there are many movers who have yet to develop a coherent approach to rolling out this increasingly central part of modern business.

Digitalisation is now an important part of **FAIM Certification**, with FIDI members already required to demonstrate 'digital readiness'. That means having a paperless office and remote digital access to warehousing for auditing purposes – or, as a minimum, having a detailed plan for developing this before their next third-party compliance procedure.

It has been included in the FAIM standard as an important indicator of quality, because of its role in enhancing everything in a moving business from risk management, transparency and efficiency, to convenience, communications, and the all-round customer experience.

Mandatory requirements will become more extensive when the next version of the FAIM standard is released in 2026, and Affiliates will need to ensure their audits can be carried out fully remotely, at the same level of quality as the current on-site audits that take place every three years.

FIDI Focus has put together these guidelines for movers who are in the early stages of their digitalisation journey, to help them identify priority areas and quick wins, and map out a straightforward plan and concrete actions for the benefit of customers and their bottom line.

The guidelines are divided into two parts: the first section on 'getting started' looks at the simple digital changes that movers can implement to drive cost savings and efficiencies in their companies from the beginning. The second section deals with risk management and examines the business-critical issue of cyber security, highlighting the steps firms can take to protect themselves, their staff, and their customers as they become more digitally connected.

Digitalisation: a definition

FIDI's definition of digitalisation is 'the process of transforming moving and relocation from analogue to digital businesses, improving efficiency and generating new opportunities in the process.'

Getting started

1. Define your plan

Most industry technology experts and movers agree that firms should begin their transformation journey by defining a simple plan. This means developing a strategy linked to the company's overall mission and based on a firm's key goals, which identifies priority areas and the actions needed to digitalise processes to drive efficiencies and cost savings.

As a priority, the plan should ensure that the changes being put in place will boost, rather than compromise, the experience of your customers.

Your transformation plan should have clear and measurable goals, indicating what digital change is needed in each part of the company, and specifying a timeline and budget, if needed. These should be reviewed regularly, in the light of analysis – of data and qualitative feedback from customers, employees, and other stakeholders – and the ongoing growth in capability brought about by new technologies.

It should show where automating repetitive tasks and processes can bring efficiencies, and where investment is needed to bring this about, defining any changes in employees' roles and responsibilities, and outlining what training will be necessary to ensure staff are fully prepared to work with – and alongside – new digital tools.

Action: Set up a tech taskforce to govern your digital transition and report to management. This should represent every department within the company, across a variety of different job roles.

The tech taskforce should outline your digitalisation plan, highlighting priority areas for attention and a timeline for implementation. See boxed article below 'Defining your digitalisation plan' for more information.

Defining your digitalisation plan

Here are some of the questions your company needs to ask itself when outlining its strategy for digital transformation.

1. What is the business case for digitalisation? List your objectives and goals – a focus on developing efficiencies and cost savings and improving your customers' experience should be a key part.

2. Where are we now? Assess your current digital capabilities, including the software, hardware, and technological infrastructure your company already has – and where it might be lacking.

3. What budget and resources do we need? This includes defining available budget, investment in technology and availability of staff, and other resources. It is a question worth asking at the beginning of and during the process of defining what you want to achieve with digital transformation.

4. Who are our stakeholders? Define who will be involved with the process of digitalising the business and who it will impact. Include customers, suppliers and others outside the company.

5. What technologies do we have – and what do we need? Choose the relevant applications and other technology you need to deliver your plan. Review this regularly.

6. What are the compliance and regulatory requirements? New technologies demand you conform to new rules, particularly on data security. Ensure you research these.

7. How do we manage the change? This includes planning for changes in day-to-day business practices, developing staff training and setting a timetable for transformation. Ensure you consider business continuity so you can keep operating smoothly when processes change.

8. How do we measure and improve? Set clear KPIs, reporting windows and metrics for improvement.

2. Ask your staff

Involve a range of your workforce in the process of digital change, particularly younger employees who are often the most tech-savvy and agile-thinking people in a company, with a positive attitude to change.

A business has a lot to gain from incorporating this bottom-up approach. A top-down strategy can work, but often requires stricter change management practices.

Asking for input from staff members at every level can bring a wider range of effective new ideas to the digitalisation process. Engaging your workforce in this way also helps with the development and retention of good people.

Action: Develop a questionnaire and send it to staff asking for their help. Here are some suggested questions:

- What are the digital tools or processes you currently use most and why?
- Which tasks or processes can our business automate digitally to make us more efficient?
- What would be the challenges in making these changes?
- How can technology improve our services for customers? What problems can technology help us solve for customers?
- What digital skills or training would be particularly useful to you in your role?

3. Look for low-cost, quick wins

Low-hanging fruit can include anything from digitalising documents (see part 4) to adding an automated online pricing calculation tool to provide rapid estimates for clients.

Most companies already have access to a wide range of software tools that are under-utilised and can be used to do more. Staff training or demonstrations by the owner software firms can help build knowledge and capabilities of what is possible with existing resources.

There are also many free tools available online, giving businesses access to facilities such as automatic emails, project management, online team collaboration, and so on.

Action: Define these quick wins in your digitalisation plan – where are they? How fast can they be implemented? You can add more when new technology becomes available, and evolve your plan.

4. Go paperless

Switching from paper to digital documents is a natural place to start digital transition across your company.

Having digital documents brings immediate benefits, including boosting efficiency and transparency to your staff, customers and suppliers. It facilitates remote and flexible working, ensures continuity when staff are ill or unavailable, and generally increases the speed and quality of services to your clients.

Make sure digital documents are easily accessible to everyone who requires them – this must include mobile devices, too – and ensure everything needed to work with

them, such as the digital signing of PDFs, is functioning too.

It is important to note that moving your and your customers' documents online exposes them to the risk of data theft or other fraudulent activity. However, these risks can be mitigated by taking straightforward steps – as set out in the 'Managing the risk' section on page 7.

Action: List all the categories of company documents (contracts, inventories, shipping, and so on), who needs access, and from where they need access.

5. Embrace virtual surveys

The pandemic turbo-charged the acceptance of virtual surveys, and they have become a permanent part of moving businesses' service offer.

In addition to speeding up and enhancing traceability of the survey process, virtual surveys help upgrade parts of your business from the customer experience and sales, to operations and the move itself. Investing in a digital survey platform is a good early step for movers who want to see quick benefits of digital transformation.

Action: Read up on the different survey apps available and arrange a trial for your business. Learn from the experiences of your industry peers, too.

6. Mitigate new risks

As your business becomes increasingly digital and connected, it will be exposed to the threat of online crime such as fraud and data theft.

Having important data and functionality available in the cloud opens your business up to accompanying risks affecting systems and processes. These can range from having incompatible technologies and errors, to risk relating to cybersecurity (see section 2) or lack of staff skills. It can lead to accidental or deliberate exposure of private or otherwise sensitive data, leading to leaks.

Automating and digitalising can cause issues of continuity and compatibility in the business processes they involve; they can also create new weaknesses to address, such as larger potential impact of disruptions such as server outages.

Staff training is also essential to ensure employees are fully aware of the potential risks and what they need to do to minimise these for the benefit of themselves and the company.

Action: Make a list of all parts of your company exposed to digital threats – alongside the measures you will take to mitigate the risks to your business.

7. A marketing makeover

While FAIM's digitalisation mandate is focused on relocation operations and activities themselves, digital technology also allows movers to target prospective customers much more precisely and reach lucrative new audiences, too.

Budgets for digital market activity – funding wide-reaching pay-per-click campaigns, for example – can be huge, but you can be strategic without spending big money. Some of the most effective steps only require minimal investment,

including precise customer demographics for digital marketing efforts; or simply producing a landing page for each part of the business that prospective customers will look for to create direct hits on Google searches.

With almost 90 per cent of customers now sourcing moving services with the help of online reviews on platforms such as Google – well before they visit your website – managing reviews is another simple yet powerful way that marketing digitally can benefit your business. This includes promoting positive and responding to any negative reviews; and implementing best practices such as taking fake customer complaints offline, thanking people for leaving a review; apologising and telling people what you are going to do to rectify mistakes; and sharing information when necessary on external factors such as shipping delays.

Action: Audit your marketing activity, asking how you can reach more of the right people. How can digital tools help refine your target group and market to them better? Define an advertising and marketing budget, if needed. Allocate a staff member or team to oversee activities including managing customer reviews and incoming leads from digital marketing.

8. Measure and review

Revisit your digital transformation plan at regular intervals, collecting data and analysing it to measure the success of what you're doing.

This should be an ongoing process, with everything from systems, outcomes, software, digital marketing and risks evaluated regularly to assess and improve.

Include qualitative evaluation, too. Invite management and staff to feed back on the success of the changes you have implemented.

Action: Add a review section – including what you will measure and when – to your company's overall digitalisation plan.

9. Start somewhere

While a business who fails to embrace digital technology may survive in the short term, it will quickly lose ground to those businesses that ensure they are interacting with customers and their supply chain online, and are taking advantage of the efficiencies and benefits that digital technology has to offer. Make sure you're one of the latter.

Action: Remember to stay pragmatic and take digitalisation one step at a time. Focus on the priority areas you have identified – and look for solutions that will serve you for the long term.

Cyber-security: Managing the risks

At the highest level, cybersecurity is recognised as one of the greatest emerging risks to businesses, including those in global mobility.

As more elements of the moving and relocation process have been digitalised, they have been exposed to new threats. Personally Identifiable Information (PII) and other private information is requested for shipping and other documents, for example, many of which are now digital. Meanwhile, cyber-attacks that use malware or ransomware to try to extort money by destroying, blocking, or gaining access to this data, have become increasingly common.

Accordingly, data security, compliance, and standardisation have become a growing focus for movers, who must ensure they have adequate protection against the theft, loss, or damage of business-critical data. Failure to do this puts their customers at risk of identity theft, fraud, and other types of criminal activity – and ultimately threatens their reputation and long-term business prospects and can even have legal consequences.

Confronting the mounting risks involved is an entirely necessary task but it can be costly. However, by taking a few straightforward steps, moving and relocation companies can mitigate a great deal of risks involved without necessarily spending large sums of money. Here are some of them:

1. Plan ahead

Cyber security should be a key focus for your tech taskforce, which should evaluate potential threats to your company's business-critical networks, systems, and information.

It can be easy to think about these threats as coming purely from outside of your organisation, but it's vital that businesses consider what's happening inside it, too, and examine their own role in minimising their exposure to technological risk. This includes analysing systems and processes, educating employees about their responsibility to keep data safe, and putting straightforward security procedures in place.

Every company should create an action plan of measures to boost its protection as an integral part of the business digitalisation plan described in part one. It should include a list of connected devices, software, the data that could be compromised, and what needs to be done to make each more secure. It should cover where data is stored and who has access to it and identify how unauthorised people could obtain it, alongside the protective measures needed.

Employees should be given specific responsibilities, including the precautions they need to take themselves, and what needs to be done in the event of a cyber security breach. If some or all or your firm's data is stored in the cloud, you should ask the supplier to get involved with defining your plan.

Technological change happens fast, and risks evolve, so remember to review this plan regularly – and whenever there are significant changes in how your company stores and uses its data.

Action: Create a dedicated cybersecurity section to your overall digitalisation plan outlined in section 1. Schedule a review of this at least once a year. Appoint someone in charge of keeping track and regularly updating your company's cybersecurity plan.

The following points will help you specify the contents of your plan further.

2. Update, upgrade

To reduce the risk of compromising business-critical data, your computer software needs to be kept up to date with the latest versions. This

is especially important for antivirus software, but also for the apps, web browsers, and operating systems your company is using.

Most software has a setting that can be activated to update it automatically whenever a new version becomes available.

Action: Make a list of the software in your business, with the most important ones at the top and noting the data each one uses. Schedule any manual updates needed, as well as a full software audit at least once a year.

3. Precautionary tales

There are numerous precautions firms can take to secure their networks and files from the possibility of a cyber attack. These include insisting on strong passwords, such as those with letters, numbers, and special characters; or using multi-factor authentication – where someone requesting access must enter a password but also other elements, such as a code sent in a text to their phone.

Consider the security measures you need for every item on your list of connected company devices – and implement them.

Company servers, for example, should be protected with an up-to-date firewall and software, and routers protected with secure passwords and software. Encryption such as WPA2 (Wireless Protected Access 2, a security protocol that protects internet traffic) should be in place to secure networks or mobile devices.

Servers and other essential company data should be backed up regularly to minimise the damage caused in the event of data loss. Meanwhile, introduce formal procedures for deleting electronic files and decommissioning old devices; and ensure you limit access to company data: always ask 'does this person really need to have this access?'.

Action: Working with a third party can help you identify more risks and ultimately give you more thorough protection. While there are many straightforward measures your company can recognise and implement on its own, if you don't have a dedicated IT person or department, consider outsourcing this part of your plan.

4. Patch work

Patch management is the process of updating software, firmware, and

drivers, on systems from laptops and PCs to other hardware, on an ongoing basis, to keep them protected against potential leaks or other breaches. In addition, by keeping systems safe from cyber attacks and running smoothly, it can increase productivity, lower the cost of device life-cycle management and repairs, and help a company meet compliance requirements and standards such as GDPR.

Ongoing monitoring is essential to good patch management, too, as it will help your business identify gaps in its systems and deploy the right solutions.

Your company should patch different parts of the business in cycles, scheduling regular checks to make the process predictable, allowing people to prepare. Responsibilities for patch management should be clear, usually falling to one of the software/system providers, IT managers or, in smaller companies, individual users.

Action: Allocate responsibilities for patch management across your company. Work with an external IT provider and use patch management software to coordinate this process if you need help.

5. Staff training

Keeping staff informed about cybersecurity hazards and empowered to tackle them is one of the most important parts of any company's approach to this side of digitalisation.

However, it can be a complex area and companies should use straightforward language in communications on this subject, so every employee understands the risks involved – to the business in which they work and them personally - and the precautions they need to take to lessen these.

Rather than take a 'one then it's done' approach to training, run regular interactive employee education sessions, so you keep them informed about both current and emerging risks. Once again, consider outsourcing this part of your plan, to ensure you have the most up-to-date information – but be sure to balance this with internal checks of your own.

Employees should understand that they can themselves fall victim to social engineering attacks, where they are deceived into releasing confidential company data or personal data that can be used in fraudulent activity. This includes 'phishing', where attackers pretend to be a bank or other organisation to steal information such as log-in details or credit card details.

Phishing attacks have become more sophisticated. Where generally low quality, grammatically incorrect and poorly put together messages used to be the norm, today's much more well-targeted and well-presented emails and other messages can be much more difficult to spot. 'Spear-phishing' attacks, where criminals cleverly use their targets' names and other personal data to extract money or information, and 'whale-phishing', which focuses on high-level employees such as CFOs and CEOs, are both on the rise.

Action: Work with employees to define their own cybersecurity responsibilities and create a clear plan stating the action needed in the event of a data breach.

6. Response ready

Even with the correct planning, things can go wrong, so prepare an incident response plan. This will help your organisation move quickly and efficiently to minimise the damage caused by a breach of security.

A good plan will identify the different categories of data breach, alongside a list of everyone who needs to do what, who should be informed, and how to maintain business continuity quickly after a breach.

Action: Draft an incident-response plan, including clear steps for action, and who should take them.

7. Plan for PR

The incident response plan should also outline what external communications are needed to help manage and limit the possible reputational damage of a breach.

An incident plan should also include international and external communications, to manage the reputation of your business. You must also make it clear what can and can't be communicated outside of the company about the breach and that staff understand how your company is going to respond.

Transparency is a must in this process. Ignoring or hiding a data breach only sets a business up for future damage. So, a carefully considered communications plan is a must.

Action: Add your PR draft to your incident-response plan and circulate it to staff

8. Balancing act

While the more complex aspects of cyber security will usually require some kind of expert third-party assistance, moving and relocation companies should balance this with their own in-house know-how and checks. External providers can cover 'behind-the-scenes' technical elements, but in-house staff will understand how the business works and, crucially, the implications of the failure of the systems within it.

Businesses should also take a balanced view of risk and understand that while the tightest of security

measures can dramatically reduce the possibility of a cyber-security incident, they can never eliminate it entirely. Staff training and awareness plays an important part in this understanding.

9. Do something

Cyber security has been described as one of the top two issues facing movers in the next decade. With a significant amount of most moving jobs now carried out online, it is essential to protect the transactions and data involved.

As new protective measures are developed and implemented, criminals are fast finding sophisticated ways to overcome them. Mobility businesses need to move fast, too and, remembering that protecting against these risks isn't always expensive, must continually monitor themselves for security gaps and identify business-critical areas to prioritise for protection.

FIDI has advised those businesses that haven't yet acted on this issue to do so as a matter of urgency. The worst thing any company can do is nothing.

10. A final word

As Thijs Deweerdt, Senior Manager and auditor at EY Consulting, pointed out in a recent edition of *FIDI Focus*, with more than 20 billion devices connected to the internet already, and this number growing fast, the need for companies to ensure they are protected is only getting stronger.

'When everything was on paper, you didn't need that much protection, just a good lock and key,' he said, adding that those who are not mindful of their data security will go out of business. 'If not for financial reasons, then operationally because you can't work properly; or it will be due to reputation, if your clients or other organisations in your supply chain know you're not data-protection savvy.'

Meanwhile, FIDI is continuing to monitor developments in this area, including emerging legislation and case studies. With digital auditing capability mandatory for FAIM from 2026, but around four out of 10 FIDI Affiliates still yet to go fully paperless or digitalise their processes, there is plenty of work to do in the next two years.

Action: Get started as soon as you can – and talk to your industry peers who have already started their digitalisation journey.

● **If you are a FIDI member, you have free access to the tailor-made digital proficiency and cybersecurity training module developed by the FIDI Academy. Read *FIDI Focus* for latest developments and advice on digitalisation and cyber security.**

For more information or questions about this report or other FIDI publications, please contact

Magali Horbert
magali.horbert@fidi.org
www.fidi.org

FIDI Global Alliance
Fountain Plaza Building 501
1st Floor, Belgicastraat 1
1930 Zaventem, Belgium
fidi@fidi.org
www.fidi.org

Published on behalf of FIDI Global Alliance by CPL One
For details on future reports and opportunities, please contact:

Dominic Weaver
+44 1223 378000
dominic.weaver@cplone.co.uk
www.cplone.co.uk