7bridges

Beyond The Black Swan

COVID-19 and the case for logistics resilience

The pandemic has affected everyone, everywhere. It is forcing changes in numerous areas of life, including the way we do business – and crucially, the way we manage our supply chains.

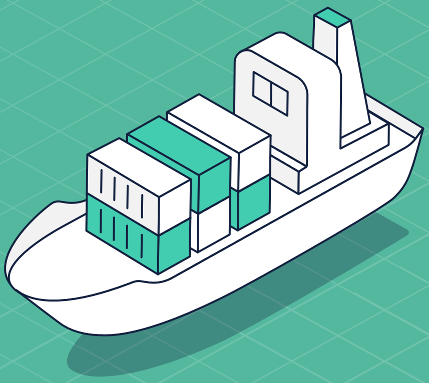
Supply chains that businesses have relied on until the beginning of 2020 have been tested and stressed as never before. Urgent new questions have been raised:

- how can sales volumes be maintained during lockdowns?
- how can spikes in online sales demand be fulfilled?
- how can margins be protected in the face of rising logistics costs?
- how can all this be achieved with uncertain staffing levels and overstretched capacity?

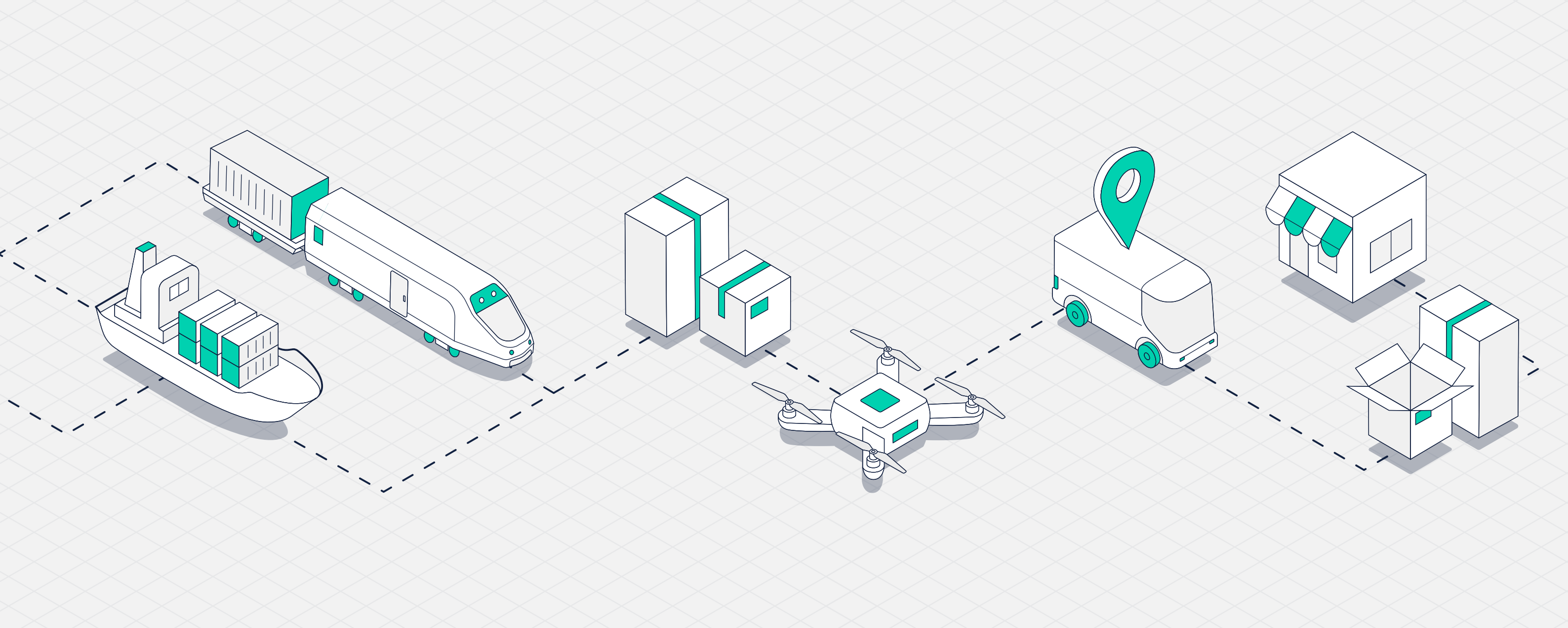
The challenge of the pandemic is extreme, and it brings into sharp focus the risks and vulnerabilities businesses are exposed to every day, from events that have been occurring every year, many with increasing frequency.

There are many other serious threats to profitability and even survival. And, because these threats are not pandemic, but cause disruptions only for a limited period, or only affect specific regions, or are even confined to individual companies, they have so far failed to bring about widespread re-evaluation. Nevertheless, for any organisation affected, these events are severe and can even be catastrophic.

In this whitepaper, we survey the major threats to business arising from logistics disruption during the current pandemic, and in other black swan events. We show the impact and damage sustained in some high-profile examples, and illustrate the more insidious dangers in less-visible threats. Some of these risks are accepted by businesses as unavoidable, but they need not be. In fact, every business should be taking steps now to ensure that it is resilient enough to survive any and all of these events.



In this white paper



Logistics disruption during the pandemic

Unprecedented in living memory, the global pandemic has presented an existential challenge to businesses, which have had to invent new ways of surviving in the face of disruption to sales, supply chains and margins.

Threat to sales

The obvious move for businesses when face-to-face commerce became difficult or impossible early in 2020, was to make it easier for customers to buy products online. But while it may be relatively easy to establish or give greater prominence to an online storefront, retailers have also had to address the sudden additional responsibility of B2C logistics at scale.

Even with online orders ticking over, revenue can't be generated without adding the new element of efficient B2C logistics. 'Efficient' is the critical word here, because while customers are prepared to accept that in the current circumstances deliveries might not be quite so rapid as they have been used to, any business selling online is competing against the logistics standard set by Amazon and other giant platforms. If a competing product is available on those platforms with a shorter delivery time or a lower charge, the sale may be lost.

!

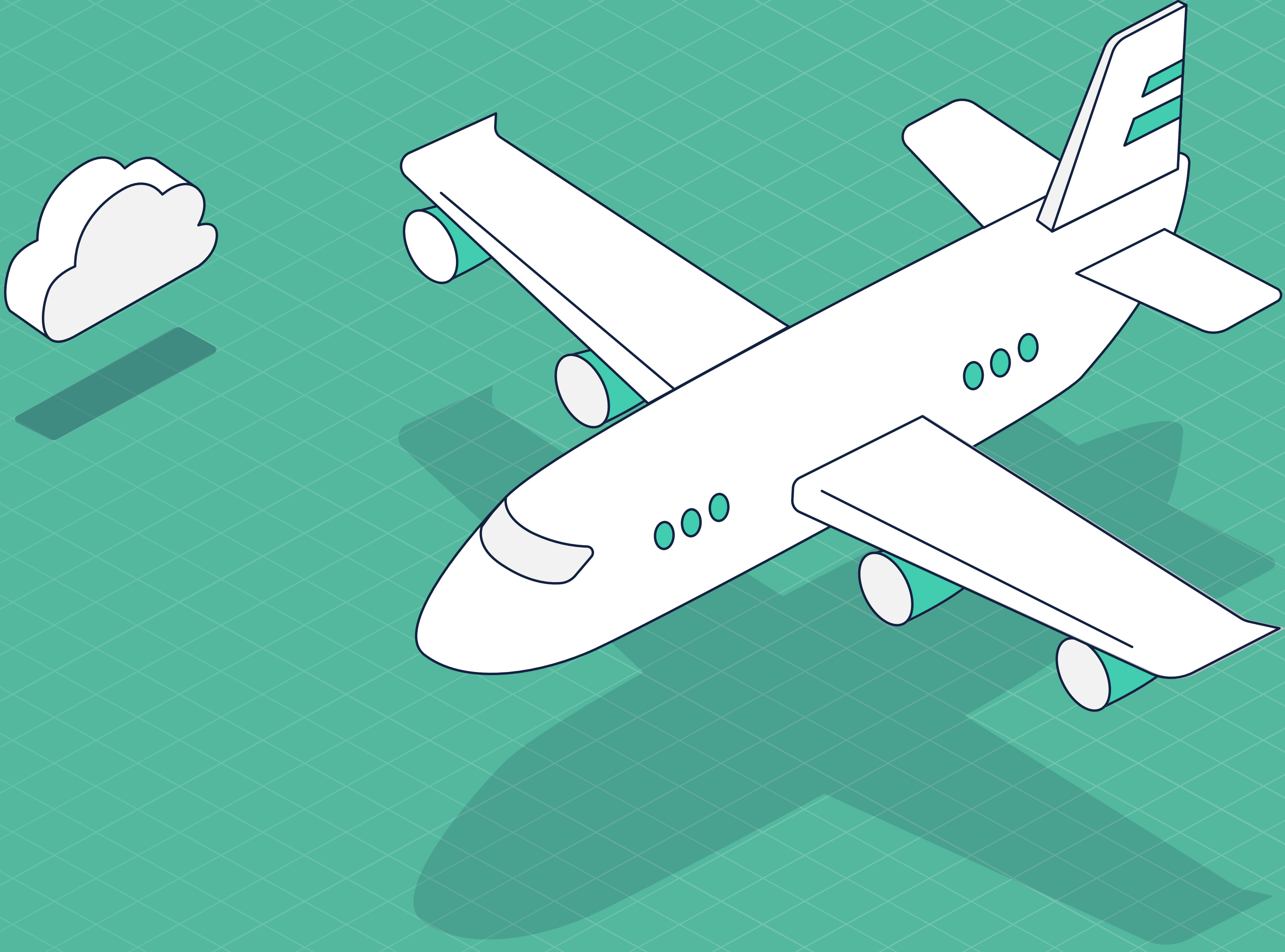
The hike in carriage costs experienced by businesses during the pandemic can be such that it wipes out the entire profit on a sale – an alarming situation when volumes are already depressed by adverse trading conditions

Threat to the supply chain

During the COVID-19 crisis logistics service providers have of course experienced the same challenges as other businesses, including:

- staff shortages due to illness
- the need to adapt to health regulations and social distancing rules
- closed borders
- local and national lockdowns.

Additionally, they've faced delayed freight shipping across land and sea, had access to limited capacity on commercial flights and seen a huge rise in airfreight charges.



Why did airfreight charges rise so dramatically?

The vast majority of commercial air traffic is passenger traffic. A significant proportion of airfreight is carried on those same passenger flights (often, around 50 percent). So when passenger flights came dramatically to a halt in the first few months of 2020, freight charges rose sharply. Suddenly, almost the only airfreight available was from 3PLs that operate their own planes, such as FedEx and UPS.

In the scramble that resulted from reduced airfreight capacity, freight forwarders, large corporates and express transporters were competing for space. This resulted in raised costs that were passed on to customers.

Threat To Margins

With the disruption suffered by carriers and the reduction in available airfreight capacity, carriage costs have risen sharply. These are passed on by the carrier to the business, and the hike in carriage costs can be such that it wipes out the entire profit on the sale – an alarming problem when volumes are depressed anyway.

In many cases the sudden negative impact on margins has combined with depressed volume of sales to create a serious cash crisis.

What happened to carrier surcharges in Spring 2020?

During the COVID-19 crisis logistics service providers have of course experienced the same challenges as other businesses. Additionally, they've faced delayed freight shipping across land and sea, and had access to limited capacity on commercial flights.

As a result, carriers have been passing on additional costs to their customers in the form of COVID surcharges, which has seen the price of moving stock and delivering items rise sharply for many businesses.

Businesses with a single or restricted list of logistics carriers have been paying significantly more for their shipping than organisations with a flexible and adaptive carrier selection process. The impact on an organisation's bottom line has been substantial, with those that were unable to switch shipping providers seeing their shipping costs soar by up to 30%.

Some businesses experienced a 30% increase in shipping costs during the first wave of the pandemic.

Compounding the threat to profitability, few enterprises will have been aware immediately of the impact of COVID surcharges on their logistics spend.

Why?

1. Logistics invoices offer confusing information at the best of times. There is no standardisation across providers, so data is challenging to interpret.

2. These additional COVID costs have been baked into freight charges and will have been invisible to the staff responsible for reviewing supplier invoices.

Even if a business has a contract for preferential rates with a logistics carrier, it is still exposed to these additional costs, and has little or no contractual control over when surcharges will occur. For example, in relation to COVID surcharges, UPS simply noted: 'Surcharges are subject to change without notice and peak periods may be extended or otherwise changed'.

Surcharges vary between carriers

Faced with this situation, it's vitally important for businesses to understand that in an event such as this, all logistics providers do not raise identical surcharges. In fact, 7bridges observed a variance of up to 100% in surcharges during April-June 2020 across the top logistics providers. This is mainly because carriers have differing degrees of exposure: some operate their own transport capacity; some have capacity in one country or region, but not in others; and some have no capacity at all.

The following tables show some of the surcharges imposed by major carriers:

EUROPE to EUROPE surcharges (June 2020)

	Parcel (£ / kg)	Freight (£ / kg)
DHL	0.18 (no minimum charge)	0.18 (no minimum charge)
UPS	0.20	0.61
FedEx	0.18 (minimum £0.80 for shipment)	0.18 (minimum £40.15 for shipment)
DPD	0.3 - 2.25	n/a

Table 1: additional Surcharges by carrier (Europe)
Variances exist per service where day-definite services sometimes don't carry a charge. Some industry verticals are also exempt. Variances also exist per specific destination/origin country.

!

The huge variation across logistics providers presented an opportunity: businesses with the ability to change carriers at speed minimised their costs while rivals could not avoid the full impact of overnight price hikes

CHINA to EUROPE surcharges (June 2020)

	Parcel (£ / kg)	Freight (£ / kg)
DHL	1.60 (no minimum charge)	1.60 (no minimum charge)
UPS	0.61 - 1.42	2.03 - 3.24
FedEx	1.60 (minimum £0.80 for shipment)	1.60 (minimum £40.15 for shipment)

Table 2: additional Surcharges by carrier (China to Europe)
Variances exist per service where day-definite services sometimes don't carry a charge. Some industry verticals are also exempt.

Fuel charges vary too – and not just during COVID-19

You might think that fuel surcharges would be the same with every carrier, since the price of fuel rises or falls according to a standard price. But fuel surcharges also vary – again because some carriers are more exposed than others. Carriers may have hedged against future rises, or they may have large existing stocks and be able to delay passing the rise on to customers. Here are some variations in recent months:

UK DOMESTIC **fuel charge increases (by %)**

	April 2020	June 2020
DHL	9.75	7.25
UPS	11	9.75
FedEx	9	9
DPD	7	6

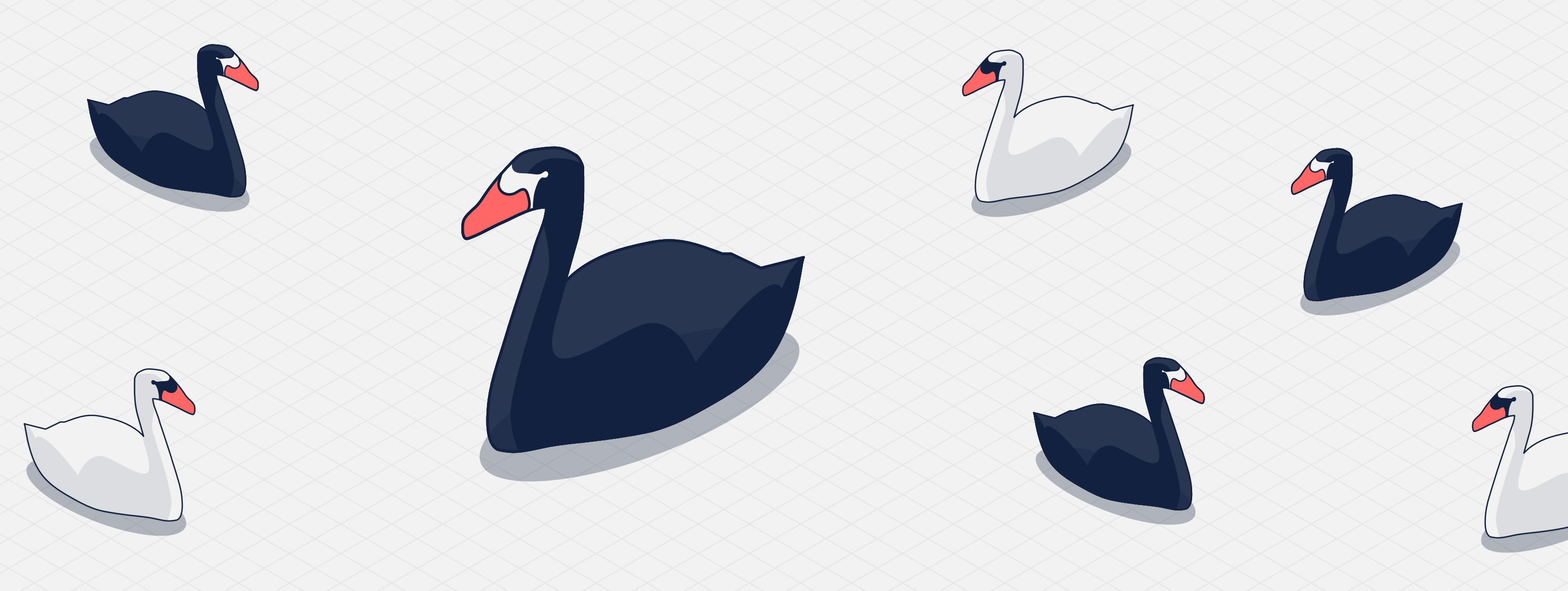
INTERNATIONAL **fuel charge increases (by %)**

	April 2020	June 2020
DHL	15	8
UPS	10.5	10
FedEx	9.5	10.5
DPD	17.75	15.5

Table 3: fuel surchages by carrier

What happens to surcharges in 'normal' times?

Although the variations shown here are during the period of disruption caused by COVID-19, fuel surcharge variations happen all the time, even in normal conditions (and unfortunately 'variations' almost always means 'increases', regardless of which way the oil markets are moving).



A pandemic is not the only hazard

For many businesses, COVID-19 has been the first real awakening to the need for resilience. However, lower-profile – but equally testing – challenges are faced by organisations around the world every week. Cyber-attacks, local or regional disasters, political conflicts; these are some of the more frequent events that can cause catastrophic disruption of supply chains and a severe threat to business survival.

The dire threat of cyber attack

As numerous high-profile cases demonstrate, carriers and logistics suppliers have not given enough priority to building resilient systems that can withstand DDoS, malware, ransomware and other forms of attack or failure.

- Companies have generally lacked the capacity and expertise to secure their systems
- Business leaders have not seen it as part of their core offering, and have not prioritised security

Yet the continued operation of logistics carriers and suppliers relies on the robust functioning of crucial computer hardware and software systems.

It is critically important for businesses that rely on logistics services from these providers to factor into their resilience strategy the risk posed by the supplier's vulnerability to systems outages caused by cyber attack.

Unfortunately, in many cases little has been done by the logistics provider to reduce this vulnerability, and it's also very difficult for a business to ascertain the degree of risk involved in a contract with a 3PL.

Of the high-profile events affecting logistics providers, perhaps the most dramatic and thought-provoking is the 2017 crisis at global container shipping company A.P. Moller-Maersk.

Maersk:
a near-fatal episode

Imagine a company where a ship with 10-20,000 containers enter a port every 15 minutes, and for ten days, you have no IT… We were basically average when it came to cybersecurity, like many companies.

Jim Hagemann Snabe,
Chairman, Møller-Maersk

Maersk's IT and control systems were disabled in an attack during the non-Petya campaign, which was based on a software exploit leaked from the US National Security Agency (NSA) targeting Microsoft Windows systems. With its origins in a cyberwar effort in the struggle between Russia and Ukraine, and initially seeming to be a ransomware attack, non-Petya had a serious impact on thousands of organisations around the world, including the UK's National Health Service, FedEX, pharmaceutical giant Merck, and many other large corporations.

The attack 'bricked' all of Maersk's computers, forcing staff to operate the company manually for ten days.

It was only saved from complete collapse by pure chance: just one of the company's servers – in Ghana – remained uninfected, and only because a power outage caused it to be disconnected just before non-Petya spread through the rest of the network. From this server's hard drive, Maersk was able to rebuild the all others over ten days and restore its operations to normality, defeating the attack and ensuring the company's survival.

> In all, Maersk had to rebuild 4,000 servers, 45,000 PCs, and re-install 2,500 applications; the reported cost of the damage was $300m.

Total damages from non-Petya were estimated at $10b by the US government. Other high-profile corporate losses from non-Petya include:

$870m
loss Merck

$384m
loss Saint-Gobain

$188m
loss Mondelēz/ Nabisco/ Cadbury

Carrier outage: TNT/FedEX

Also in 2017, FedEx suffered severe disruption to its TNT subsidiary as a result of the Wannacry malware. TNT's intercontinental operations were interrupted, with pick-ups, delivery operations and access to tracking systems affected.

The malware made infected computers impossible to use and did not appear to be designed to extract a ransom but simply to cause disruption. TNT's computers were vulnerable to infection because – as is so often the case – they had not been kept up to date with the vital security patches. These were not applied because it would have meant interrupting the operation of computers that were in use 24/7, and possibly breaking key applications.

During the outage, trading in FedEx shares was briefly suspended, and the company later estimated its losses at around $300m. In a statement released later in the year, FedEx said that TNT Express volume, revenue and profit still remained below previous levels.

2016 Regional outage: DDoS on East Coast of USA

Another form of cyber-attack causes more widespread disruption by degrading or disabling internet services across a region or regions. The DDoS attacks on internet infrastructure provider Dyn in 2016 prevented users in Europe and North America from accessing hundreds of major internet platforms and services including Amazon, CNN, PayPal and Twitter.

DDoS attacks are a constant presence and the scale has continued to rise over recent years, by 2016 exceeding a terabit per second. Advanced and persistent forms of these attacks can last for weeks, with the longest so far documented being sustained for 38 days. Attackers may attempt to evade countermeasures by switching between several targets while still concentrating the main attack on a single victim. If the victim chosen is a key part of the internet's infrastructure such as Dyn, then the negative effect can be difficult for any internet user to avoid.

In-house cyber-security

A supply chain is only as resilient as its weakest link, so a business should take all necessary steps to protect its own in-house operational systems against attack and failure. Regarding external systems and suppliers, it is crucial to have the ability to rapidly switch volumes between providers to reduce your risk.

Cyber-attacks at a relatively small scale are more common than is generally known, since businesses avoid publicity whenever possible.

Ransom attackers know that smaller targets are unlikely to have the resources to fight off the assault and ransomware attacks have been aimed even at individual manufacturing plants or warehouse operators, and often the least damaging recourse is to get the operation going again quickly by paying the ransom.

Extreme weather and natural events

Some of the disruptive natural events that cause difficulties are part of an established climatic pattern; others such as severe flooding are indicative of more frequent instability caused by climate change; and still others such as volcanic eruptions and earthquakes can be considered as freak events. But irrespective of their predictability or lack of it, they can all pose serious obstacles to normal commerce.

Volcanoes, hurricanes and commerce

The 2010 eruption in Iceland of a volcano that projected a huge ash cloud into the atmosphere produced weeks of disruption to air traffic over Europe. Civil aviation authorities from Ireland to Bulgaria were forced to shut down or severely restrict air space to avoid damage to aircraft, hindering global airfreight and causing a shift in European cargo from planes to ground-based transport. UPS, FedEx and TNT were among those affected. There were delays in a wide range of goods, from foodstuffs to medical supplies and precious gems.

Rather more predictable, the yearly cycle of hurricanes that affects the Eastern Seaboard of the American continent causes widespread, if transient, interruption to regional transport. Comparable patterns of seasonal weather occur globally.

Hurricane Harvey, which hit Texas in August 2017 was registered as the most damaging ($125 billion) since Katrina in 2005. This was closely followed by Hurricane Irma in Florida less than a month later. In this exceptionally stormy year, there was widespread disruption to air, sea and land transport.

Hurricane Irma was the culmination of an exception year, causing disruption to air, sea and land transport:

- Irma alone disabled 16% of the refining capacity in the USA
- Amazon was forced to abandon its flagship two-day delivery pledge
- Port closures caused delays and re-routing, extra drayage and storage charges
- Extra demand on road transport caused a 66% spike in the cost of rig rentals in the week ending 2nd September.

The effects of the hurricane on the supply chain continued to be felt through the elevated fuel prices arising from damage to regional refineries and fuel stores.

Extreme events such as these tend also to affect logistics in neighbouring regions not directly touched by the disaster itself. Transport capacity in areas close to the disaster zone tend to be diverted to supply emergency materials for recovery and re-stocking, aid and medical supplies. When there's some warning of an impending event, this diversion of capacity can be felt even in the run-up, as pre-storm preparation shippings of food, water, plywood, particleboard all place extra demand on capacity.

After the disaster, delivery of reconstruction materials, food and water, medical supplies continue to soak up capacity from adjacent areas. Across the USA as a whole, the week ending 2nd September saw a 6.7% rise in trucking costs as a result of the pressures of Harvey and Irma.

Man-made events: political and financial collapse

International or global operations cross numerous cultural and political boundaries. Businesses seek to insure themselves as far as possible against fluctuations caused by changes in political regimes and alignments, hostile legislative environments, and instability in trading agreements.

Beirut explosion: August 2020

The August 2020 explosion in the port of Beirut is another example of an event producing a major impact on regional logistics. Without the capacity to adapt quickly, events like these can cause severe stress on business operations.

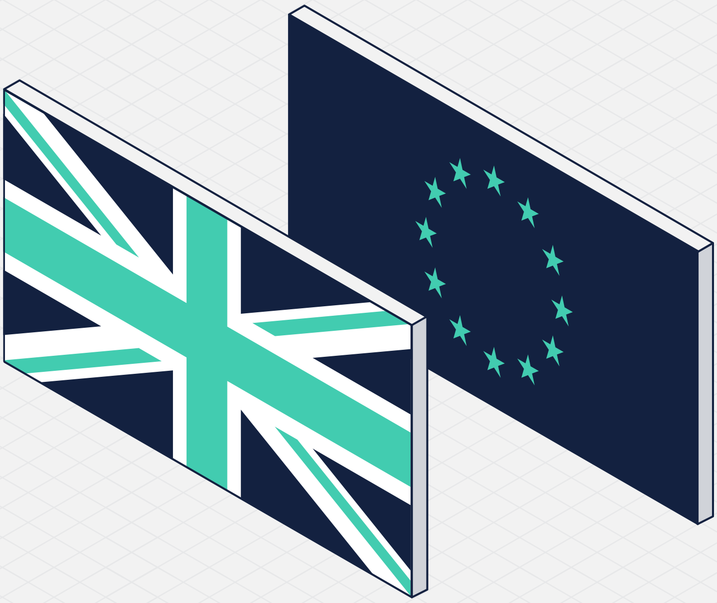
The end of the Brexit transition: January 2021

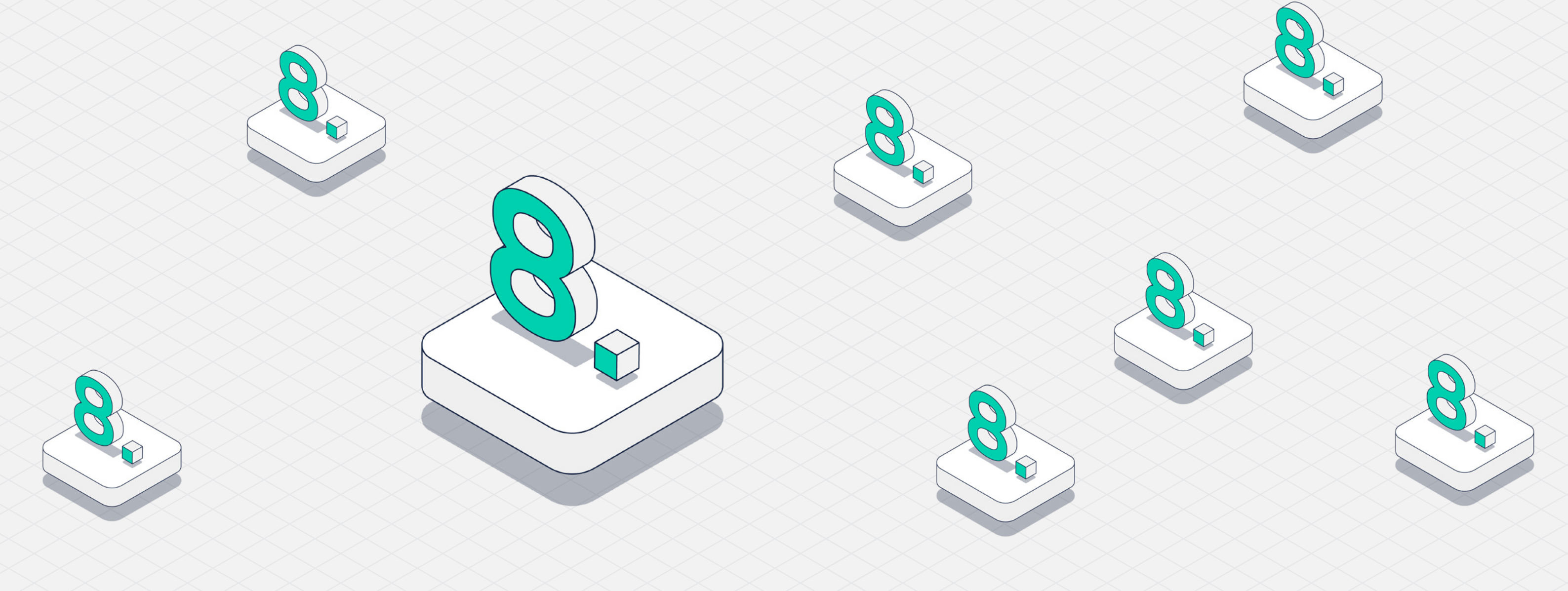
The disruptive potential of a new customs procedure can be considerable if a business fails to update its own processes and workflow accordingly.

A re-alignment on the scale of the UK's exit from the European Community presents a daunting challenge to both exporters and importers, with a greatly increased administrative burden.

This type of challenge should be bracketed together with pandemics, cyber-attacks, terrorism and extreme weather in the category of 'operational threats', and addressed as part of an overall plan for resilience.

Brexit presents similar operational threats to businesses as pandemics, cyber-attacks, terrorism and extreme weather.





8 Steps toward true resilience

As cases like that of Maersk show, a lack of resilience can bring even a large, well-established business close to a sudden, complete failure. To protect against disaster, there are several tiers of resilience that can be developed, in distribution, technology and strategy.

8 Steps to logistics resilience

Logistics Strategy	Technology Strategy	Business Strategy
Multi-Carrier Approach Instant, no-penalty switching between carriers for best value	Distributed Ops Systems Software and hardware redundancy across multiple sites	Business Model Agility Adapt and rapidly implement new ways of doing business
Multi-Site Distribution Distribute stock intelligently, and ship from any site	Distributed Server / Cloud Failover between redundant sites in separate regions	Marketplace Agility Quickly switch focus and traffic between regional markets
Multi-Fulfillment Method Dropshipping vs. regular distribution		Proactive Resilience Analyse trends, anticipate changes and prepare contingencies

Part one: A resilient logistics strategy

These are the measures a business can take to ensure that its logistics operations are sufficiently agile to avoid being badly degraded, becoming too costly, or even brought to a complete halt, by severely disruptive events.

Carrier switching

The first and most obviously beneficial tier is to introduce the ability to switch carriers instantly, automatically, and without any kind of penalty. When a business can do this, it is no longer vulnerable to these hazards:

- Poor performance from the carrier
- Uncompetitive charges by the carrier
- DDoS, ransomware and other cyber-attacks on the carrier or its systems
- Carrier infrastructure outages or bottlenecks (in severely disruptive events)
- Sudden financial collapse of the carrier

The business is also much less vulnerable to:

- Non-negotiable fuel and 'special circumstances' carrier surcharges
- Extreme weather events
- National or Regional political disturbances
- Pandemics

As we've shown elsewhere in this paper, these factors do not affect every carrier to an equal degree: at any given moment and in any set of circumstances, some carriers will offer better performance and value than others. But a few days, weeks or months later, best value and performance could be offered by quite a different carrier or group of carriers.

The key to both resilience and profitability is in being able to switch instantly as soon as a current carrier does not offer the best value and performance, before your service and costs are impacted. For this to happen, a business must have the means to continually identify best value/performance, and adapt immediately: clearly, if it takes a business weeks to identify and adapt, it will already have incurred uncompetitive costs and service degradation. In addition, the business may never benefit from switching carriers, because the best value/performance may already be offered by yet a different carrier.

Continuously adaptive automated carrier-switching ensures the best carrier value and performance: logistics costs are typically reduced by 30% or more in normal conditions, and the effect of pandemic surcharges can be mitigated

Why don't businesses use automated carrier switching?

The advantages are so obvious, but as anyone involved in logistics operations knows, most companies work with two or three carriers – or even a single carrier – because operationally, it's the easy option.

To companies with conventional systems and operating methods, it would be impossible to be continually aware of which carriers offer the best value/performance even on a single route, let alone for the multiple routes used by an international or global business. It would also be impossible to switch instantly from one carrier to another without new contract negotiations; new process rules and staff training, systems development, and more.

Carrier-switching is the single most effective resilience measure to introduce, but for businesses with a conventional, legacy logistics operation, it's simply not practicable.
To understand how to approach carrier-switching, download the guide:

> How to reduce your logistics costs by shifting your fulfilment to a multi-carrier strategy

Multi-site stock and fulfilment points

For businesses fulfilling orders either in bricks and mortar stores or online, stock held in a central warehouse is a vulnerability. The stock and the facility is vulnerable to physical disaster, outage caused by political action, cyber-attack, or inoperability caused by pandemic.

To protect itself, a business can create redundancy by building a distributed stock holding in several warehouses suitably sited to spread risk across regions and continents. Then, if any one or more stock holding points is out of action, another can continue to fulfil orders in the interim.

Retailers can continue to keep bricks-and-mortar outlets profitably occupied in black swan scenarios such as the COVID-19 pandemic by repurposing them as stock-holding and order fulfilment points.

Retailers can continue to keep bricks-and-mortar outlets profitably occupied in extreme scenarios such as COVID-19 by repurposing them as a network of distributed stock holding and order-fulfilment nodes

- A business with a chain of stores across a continent can ensure that its stock will never be inaccessible because of a local lockdown or staff sickness at a central warehouse.
- With each store operating as its own micro-warehouse and fulfilment point, orders can also be fulfilled in the most cost-effective way over the best selection of routes and carriers from the nearest point to the customer.
- The availability of so many distribution points means stock can be quickly re-allocated between them in anticipation of unfolding events.

Why don’t businesses use a distributed stock model?

Apart from the extra resource cost of multiple warehouses, a multi-node distribution network requires some serious computational power in order to deliver its potential benefits.

Stock has to be intelligently allocated between nodes in a way that most economically places the stock that’s needed close to the people who need it, and keeps stock levels linked to varying demand as the situation unfolds. The costs of deliveries and returns from this multi-node network have to be carefully managed to achieve best value. And customer expectations of delivery date and service quality have to be met.

All this is difficult enough for most businesses with only one or two distribution hubs. When the extra dimensions of a multi-node network are factored into the logistics calculations, the administrative challenge increases dramatically. Again, with conventional systems and methods, most companies would not be able to make a multi-node distribution model work well.

For those with integrated logistics systems that already encompass the manufacturing site during the normal logistics operation, the switchover to drop-shipping can be made almost instantly

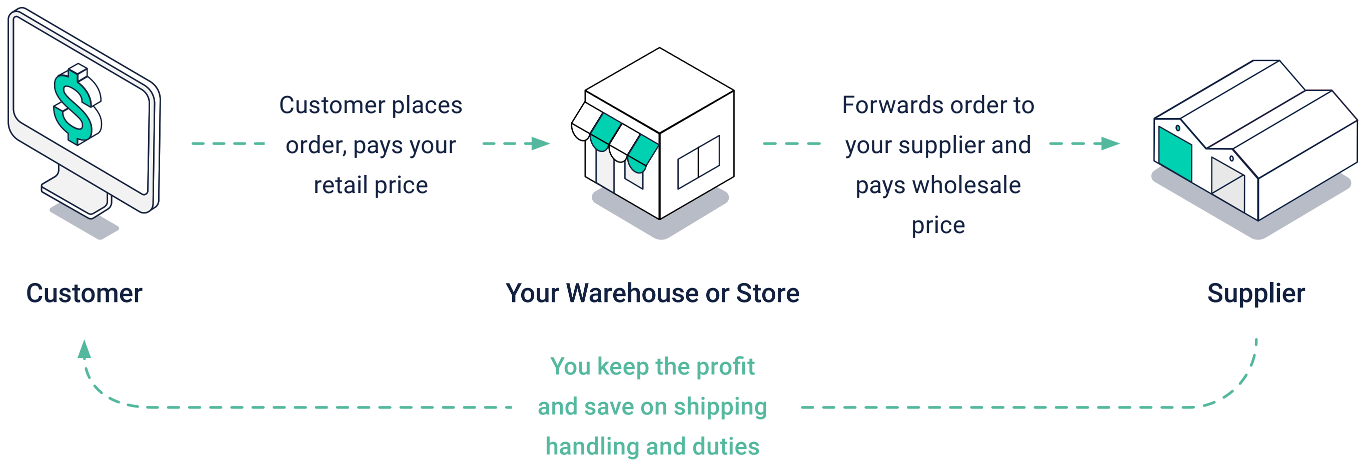
Multi-channel fulfilment: the ‘drop-ship’ option

For yet another tier of redundancy, a business could enable shipping direct from a manufacturing site to the customer. This option is a solution to the question: what happens if my usual distribution network is working, but the business suffers some critical damage to its normal channel?

As an example: a European company sells product manufactured in Asia; the product is normally shipped to a warehouse in Germany, and orders are fulfilled from there. If the German warehouse is knocked out of action, orders could still be fulfilled by shipping straight from the Asian site to the customer.

If the business is equipped to ship from the manufacturing site, it can not only supply customers direct, but it also retains other options, such as direct injection (whereby bulk shipments are made from the manufacturing site to target countries, and distribution to the customer is completed from there), or even supplying the product to other distributors.

The dropship model



Customer places order, pays your retail price

Forwards order to your supplier and pays wholesale price

Customer

Your Warehouse or Store

Supplier

You keep the profit and save on shipping handling and duties

Why don't businesses deploy a drop-ship strategy?

Manufacturing sites are normally geared to shipping in bulk to the customer's warehouse, from where the business handles the packaging and delivery to the consumer. It takes time and planning to prepare a manufacturing site to step into the role of B2C logistics.

Obstacles that all need to be surmounted before the business can feel confident that the manufacturer is ready to supply the consumer direct (while maintaining expected brand standards of service) include:

- Cultural differences
- Lack of trained staff
- The requirement for compatible systems
- A supply of customer-ready packaging

Unless the business has already taken steps to enable the manufacturer to ship direct to the end customer, sales and revenue will suffer a period of disruption while these measures are put in place.

But for many businesses, it may not seem worth the effort of overcoming these obstacles to enable this option, especially if some of the more fundamental resilience measures have not yet been implemented. However, if those fundamental measures are implemented correctly with suitable technology, drop-shipping becomes very much easier to achieve. For those with end-to-end integrated logistics systems that already encompass the manufacturing site during the normal logistics operation, the switchover to drop-shipping can be made almost instantly.

Part two: A resilient technology strategy

These are measures a business can take to minimise its vulnerability to technological failures that could hinder or paralyse its operations. These vulnerabilities arise not just in the company's in-house systems, but also in those of the logistics partners and others on which the company relies.

Distributed operational systems

As numerous high-profile cases demonstrate, carriers and logistics suppliers have not given enough priority to building resilient systems that can withstand DDoS, malware, ransomware and other forms of attack or failure. These companies have either lacked the capacity and expertise to do so, or have not understood the need to devote time and resources to the task. Many have not seen the need to offer resilient service to their customers as a crucial part of their core offering. Yet their continued operation relies on the robust functioning of crucial computer hardware and software systems.

Any business that relies on logistic services from these carriers is itself at risk from potential failures arising from the the supplier's vulnerability to systems outages caused by cyber attack.

There is the additional risk for most businesses that its own systems could become the target of an attack from a variety of sources, ranging from computer viruses to ransomware and other forms of cybercrime. Such attacks are more common than is generally known, since businesses avoid publicity whenever possible, and ransomware attacks are often made at relatively small scale. Attacks have even been aimed at individual manufacturing plants or warehouse operators, and often the least damaging recourse for them is to get the operation going again quickly by paying the ransom.

Cyber-security measures should include a rigorous software maintenance schedule, hardware redundancy, and safe 'silos' to provide a last-resort resource against infection.

But while a business can take reasonable steps to protect its own systems from attack or sudden catastrophic failure, it's impossible for any business to reliably assess how well-protected its logistics providers are against similar attacks. To mitigate the consequent risk, it's essential for a business to be able to switch carriers instantly and seamlessly in the event of a problem.

Redundancy and failover in cloud-based systems

Where a business relies on cloud-based software and systems for the advantages of resilience, it remains vulnerable to outages at the facility hosting the service. As the DDoS episodes referred to above demonstrate, the scale of disruption caused by an outage can have a serious impact on an organisation's ability to operate. Even the temporary loss of email (as in Microsoft) can cause significant interruptions.

To achieve an advanced level of resilience, a business should try to ensure that the cloud-based systems it relies on can failover to an alternative facility in the event of DDoS or other event that disables the primary provider.

Part three: A resilient business strategy

Strategic resilience is achieved by developing the ability to adapt rapidly to change and circumstance, and creating a culture which looks for opportunities as well as threats when planning for disruptive events.

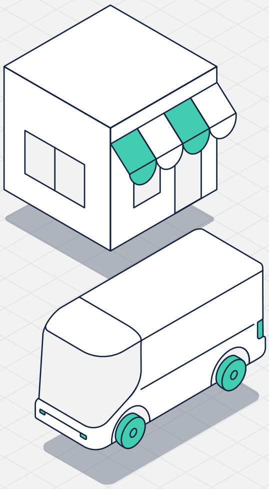
Business model agility

In the uncertain conditions brought about by a pandemic or other serious disruption, the businesses that perform well are the ones that can adapt rapidly. Inflexible procedures and systems limit the ability of a business to respond to the pressure of events. This can mean that:

- A business is suddenly unable to generate revenue in the normal way
- Margins are wiped out
- Organisations are unable to reposition themselves to take advantage of any new opportunity created by a fluid, evolving situation

COVID-19: the retail response

In the early months of the pandemic, online sales soared in most retail sectors, creating pressure on businesses to rapidly transfer resources away from bricks and mortar.



It was not easy for many to provide a high-quality response to this sudden increase in demand, especially when logistics carriers were themselves struggling to provide a good service with lockdowns and reduced capacity. The inertia and rigidity inherent in systems and supply chains left many businesses unable to compete with the dominant players, and they are losing sales as a result.

By contrast businesses with a highly adaptable supply chain and logistics systems were able to anticipate unfolding events, model ways of adapting, and rapidly implement new configurations for generating and meeting demand. Decentralised stock distribution, ship-from-store, and drop-shipping are some examples of this kind of agile adaptation.

The pandemic has also spurred major brands to address the threat to their traditional bricks and mortar channel by supplementing B2B sales with a new B2C implementation. To suddenly start shipping directly to consumers is a serious challenge for organisations of any scale without the most advanced logistics capability.

Marketplace agility

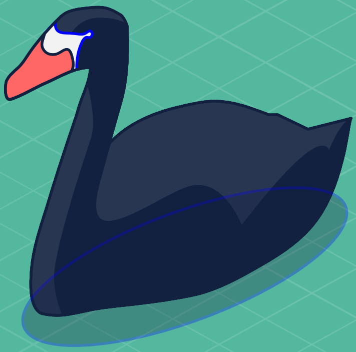
Any resilience planning should also provide for an agile response to regional opportunities and variations in demand. Marketplace evolutions brought about by extreme weather events or climate change, political re-alignments and altered trading conditions, all test an organisation's capacity to adapt and stay competitive against the best practitioners. Logistics systems and processes that limit the ability of a business to implement swift regional re-configurations are a serious disadvantage.

Proactive resilience

The most successful brands operating today have pointed the way toward 'anti-fragility': the ability to benefit from disruptive events by stepping in to soak up demand that others are unable to meet.

WalMart for example, rushes large supplies of bottled water to areas about to suffer flooding or other extreme weather; when less agile retailers run out of stock, WalMart continues to meet demand. Any serious event that disrupts established patterns of living, trading and consumption can offer opportunities, and the most advanced businesses operating today are equipped to take them.

The most foresighted business will include as part of its resilience planning a capability to analyse and model hypothetical events and opportunities. This capability should allow a business to transform itself from one that merely responds to circumstances into a proactive, opportunity-seeking enterprise with strategies for benefiting from disruptive events.



Conclusion:

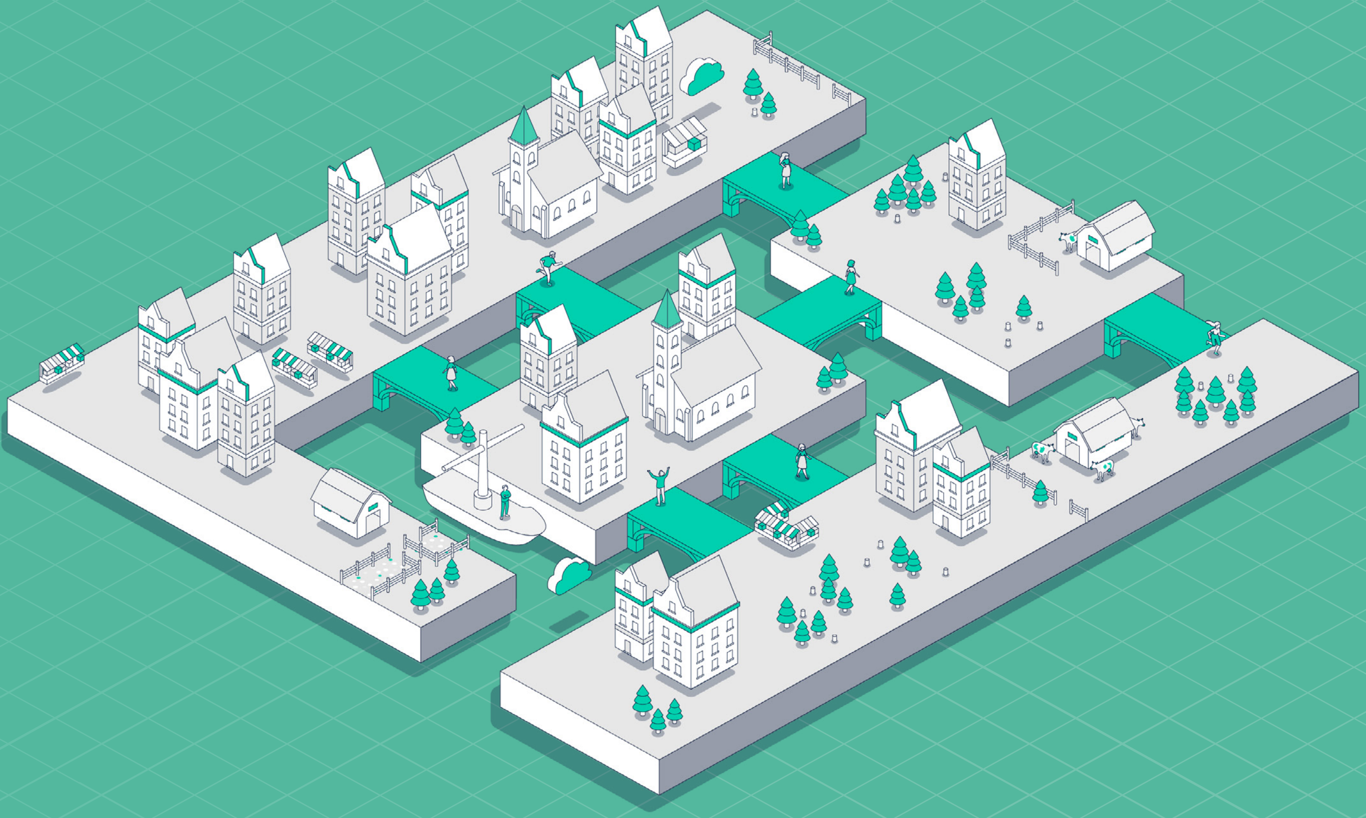
Thinking beyond the black swan

It could be argued that the term ‘black swan event’ hinders clear thinking about and planning for resilience. A ‘black swan event’ is usually thought of as a damaging event so rare and unpredictable that even the possibility that it might occur cannot be known. A meteor strike that wipes out a continent would be an example of that kind of event.

At or near the top of the lists of threats published by many bodies (including the UK Government) in the years leading up to 2020 are ‘pandemic’ and ‘cyber attack’. Foreseen and regarded as likely, a pandemic is therefore far from a ‘black swan event’; it is, instead, a fact of our modern existence. So ‘black swan’ is an inappropriate and unhelpful concept for business planners if it leads to the idea these are events for which no preparation can be made in advance. And if a pandemic is not a black swan event, then the other hazards that disrupt business continuity – and especially business logistics – should be considered even less exceptional. They are part of the ordinary landscape of risk, in the same way that fire is an ordinary risk. No business would operate a warehouse without fire insurance, and no business should operate without ‘insuring’ themselves against cyber-attack, fuel surcharges or postal strikes by systematically building resilience across their organisation.

At the heart of the black swan fallacy is a calculation of probability against the cost and difficulty of minimising the risk from the event. In terms of business logistics, that calculation has changed fundamentally over the past couple of years, as advanced logistics technology has made it much easier for businesses to implement resilience measures that were close to impossible or prohibitively expensive with legacy systems and procedures.

To find out how to make your logistics operation and supply chain resilient within weeks, visit the7bridges.com



About 7bridges

7bridges is a smart logistics platform, used by retailers and other high-growth businesses to offer exceptional delivery experiences at the lowest costs.

Smart logistics technology for year-round resilience

The platform connects businesses to an open ecosystem of transportation carriers and logistics suppliers, and uses real-time AI technology to dynamically select the best route, carrier and packaging for every shipment. This ensures the best outcome for every order that's sent, and can reduce logistics costs by up to 50%.

At a strategic level, the technology offers businesses a significant advantage over their competitors. The platform is inherently flexible and adaptable, and instantly responds to shock changes in supply or demand, such as the COVID-19 crisis.

Company history

The company's name is a reference to the classical maths problem 'the seven bridges of Königsberg', from which network analysis originated: this is the foundation upon which the 7bridges platform is built.

7bridges was **founded by Phil Ashton and Matei Beremski**, and was recently selected as one of Europe's hottest AI startups in 2020 by **Business Insider**.

Request more info

2 weeks to integrate

50% savings on direct costs

4 weeks to reach ROI