Legal considerations when advising on business continuity

Received (in revised form): 16th July, 2023

Erika Andresen
Founder, EaaS Consulting, USA

Erika Andresen

Erika Andresen *is a recovering lawyer, who has spent nearly two decades in both the corporate finance world and the military. Erika became a subject matter expert on national security and disaster preparedness/response while advising different commands and during high-risk situations in Afghanistan. Her work with actual disasters led her to attain a Master of Public Affairs (MPA). Erika left active duty in 2020 and has since started EaaS Consulting, LLC, with the goal of keeping businesses in business. To that end, she authored* How to Not Kill Your Business: Grow Your Business in Any Environment, Navigate Volatility, and Successfully Recover When Things Go Wrong*. Erika is also a professor of emergency management for the MPA programme at the University of Texas at El Paso.*

Abstract

With the rise of climatic concerns and cybersecurity incidents comes the expectation that investments are made in business continuity measures. This expectation has legal teeth from the perspective of shareholders as well as regulatory bodies, contracting attorneys, vendors and supply chain entities. This paper explores the use of US legal system as a tool for enforcing liability and action from decision makers like the board of directors and C-suite officers, as well as between the parties of contracts. Shareholder derivative lawsuits, which occur predominately in the USA but have, as recently as 2020, started to include foreign-owned businesses, and breach of contract claims are two of the more prominent issues with business continuity tie-ins. This paper intends to arm the business continuity professional with a knowledge base about legal liability for failure to have a business continuity plan, an understanding of how disasters and disruptions will excuse the full performance of a contract and an ability to determine proper courses of action with respect to supply allocation after an incident.

Keywords: business continuity, shareholder derivative, force majeure, fiduciary duty, breach of contract, board of directors, cyber security, preparedness, supply allocation

E-mail: info@eaasc.com

Journal of Business Continuity & Emergency Planning
Vol. 17, No. 2, pp. 130–139

1749–9216

INTRODUCTION

When it comes to the practice of business continuity, two of the biggest areas of legal impact to a company are shareholder derivative actions and force majeure clauses for disasters and disruptions. While legal counsel advises on both areas, not all legal advice is followed. A business continuity professional does not need to be a lawyer or legally trained, although being informed about these two concerns will put a client in a much better position when advising them.

UNDERSTANDING BUSINESS LIABILITY

Successful business continuity programming requires two prerequisites: leadership buy-in and money. These two are also the two hardest won. Decisions about spending on mitigation and preparedness

measures are open to scrutiny and litigation from shareholders. Behaviour is often manipulated by enforcing accountability. The best sticks to that carrot are lawsuits and regulations.

Fiduciary duty looms large in a company setting. To be a fiduciary, there needs to be a beneficiary. Corporate directors and officers are fiduciaries to the company and its shareholders — the beneficiaries. This duty is one of honesty and loyalty. Boards of directors are the decision makers and creators of company policy. Officers carry out the policies and make the day-to-day decisions for the company. While there is a difference between the two, it is not strong enough to keep them shielded from liability, eg delegating authorities or following procedures can still flow backwards to the originator or attach to the actor in the latter case if either is done without proper care.

Each of the actors has a power, a duty and liability. As stated already, the board has the power over all major decisions and the officers have powers delegated by the board. The board members all have a fiduciary duty, which includes staying informed and making informed decisions, and a duty of loyalty, which is to put the interests of the company before personal interests. Officers have a duty of good faith, fidelity, honesty, fair dealing plus a duty of care. The duty of care is that of an ordinary or prudent person in similar circumstances acting in the best interests of the corporation. The duty of care is violated when there is a responsibility to act but a failure to do so.

Liability for the board can be found in two places: violating a statutory standard of conduct, which looks like federal Securities and Exchange Commission (SEC) regulations, for example, and violating the fiduciary duty. Officers must comply with standards. Liability can look different in publicly held or privately held companies as well as nonprofit organisations. For public and private companies, minority shareholders or members can sue, although the difficulty in bringing a lawsuit changes from state to state.

While this paper focuses on for-profit companies, other entities should be briefly addressed. Nonprofit organisations also have duties to and liabilities for their members and the communities they serve. As the board members of nonprofits are for the most part a volunteer force and are not compensated, their duty of loyalty is to avoid personal gain — financial or otherwise — from conflicts of interest with outside business ventures.

LAWSUITS AND FINES

A shareholder derivative lawsuit requires the following elements: (1) duty, (2) breach of that duty, (3) damages and (4) causation. If any of the four elements are missing, there is no standing for a lawsuit. Each element will be examined before moving on to the next. If any element is missing, the lawsuit fails. To that point, there may be a duty and a breach of that duty, but if that duty does not result in actual damages, there is no liability. Recall for there to be a fiduciary relationship, there needs to be a beneficiary. Once established, the analysis goes on to see if any action *or inaction* qualifies as a breach of the duty.

A breach can occur in two distinct ways: nonfeasance (failure to act; not informed) or malfeasance (a wrongful or illegal act, either major or minor). Not acting decisively falls under nonfeasance, for example. Violating the duty of care requires an act of gross negligence — which is reckless or purposeful indifference. A careless business decision that causes the company to lose profits is not a breach of fiduciary duty. Breaching fiduciary duty looks more like putting personal profit ahead of the company's. It can also be assuming a lot of

risk capriciously or intending to do actual harm. An easy and common example of a breach would be for a board to make a dividend declaration (how board members get paid) that is larger due to money not being spent on those matters that keep the business operational. If a higher dividend leaves the company at risk and then the risk occurs, this would lead to damages for lawsuit purposes.

The element of damages can be economic or non-economic. Continuity professionals recognise reputation as an asset; so would a court. What is vital to the inquiry, however, is that the damages were caused directly by the breach or should have at least been a foreseeable consequence of the breach. If there was an intervening cause for the damages, there is no liability to the board. A simple example of an intervening cause is throwing a rock in one direction, the rock hitting a car and then bouncing in another direction and hitting something else. While the rock caused the damage, it was the car that overtook the chain of events and caused the specific outcome. The car is an intervening cause. There is an issue worth noting that works against the shareholders, however, and that is the Business Judgment Rule.

The Business Judgment Rule is the doctrine followed by the courts in adjudicating the lawsuit. Judges will not put themselves in the place of or second-guess the decisions of board members or officers provided that they acted in compliance with their duties. That means if each was reasonably informed, exercised good faith and had no conflict of interest, there would be no breach and no liability. A good example of this is the familiar case study of Nokia and Ericsson. Even though Nokia wound up taking market share from Ericsson by being proactive in addressing a fire in an Albuquerque chip manufacturing plant, Nokia failed to maintain that space when it made decisions that were not aligned with what the consumer base wanted or where the market was headed. Business continuity had nothing to do with that failure and the decisions made by Nokia were wrong rather than wrongfully intended.

Who can get sued for a breach of duty? Board members and officers.

Who can initiate a lawsuit? Shareholders or members can sue board members or officers. Officers can also sue the board members that lead them. Board members can sue other board members. The State Attorney General (especially in the case of nonprofit organisations) can sue the board or officers.

What kind of fines will the company be subject to? State and federal regulatory bodies will levy the fines for non-compliance. Where the fines go depends on which entity is doing the fining. SEC fines, for example, go to three different places, one of which is to harmed investors. The Attorney General fines go to specific programmes or a general fund for the state.

A special note on volunteer board members of nonprofits and government entities: these board members are given federal protection from personal liability through the Volunteer Protection Act 1997. Like the Business Judgment Rule, members are given immunity from personal liability if there was no wilful, reckless or flagrant indifference to the rights or safety of those harmed. If, however, the harm involved a sexual offence or a violation of civil rights, the protection is lost and they will be held personally liable.

BUSINESS CONTINUITY AND PREPAREDNESS

The journey from business continuity to shareholder derivate lawsuit is not a long one to make. Business continuity and

preparedness cost money. Spending decisions are made by the board and officers. There the inquiry starts as to what level of service is achieved: Is it enough for compliance, just enough to stop a major incident, or all the bells and whistles? If it is the deluxe version, there may be an issue of waste and spending too much. Officer and board members' compensation is based on earnings statements and stock prices. Is it better for the personal bank account if company profits are spent on the band-aid and not the system overhaul? There will also be decisions evaluating the cost of cyber versus paying high premiums for insurance. Finally, shareholders want their dividends, too. Shareholders might not want to pay for IT upgrades or cyber security.

Not investing in cyber security is going to lead to a lot of shareholder lawsuits if a cyber event happens. This is an easy warning flag given that cyber events are an expectation at this point. One particularly interesting series of shareholder derivative lawsuits came out of inappropriate responses to the COVID-19 pandemic. Both Tyson Foods (Tyson) and Norwegian Cruise Lines (NCL) were sued by shareholders based on their delayed response or lack of initial response to protect the workforce (for Tyson) and customers (for NCL). The lack of response from Tyson led to factory shutdown and prolonged the inability to carry on business, which then led to lost profits.[1,2]

What are companies spending their money on if not business continuity and general preparedness? Stock buy-backs, for one. Stock buy-backs were illegal in the USA until the 1980s. They are used to drive up the price of stock, which in turn drives up dividend payout. Companies are also paying fines for the standards and regulations they are violating. Sometimes that stick is not big enough for the carrot to deliver compliance. This truly depends on the size of the company. For larger companies, fines have become a cost of doing business. For some really large corporations, fines are a drop in the ocean. Experian's fines for privacy breaches in 2022 were US$16m, but its annual revenue was in the billions.[3,4]

CYBER SECURITY AND THE SECURITIES AND EXCHANGE COMMISSION

On 26th July, 2023, the SEC announced new rules and amendments to close problems of inconsistent disclosures previously required under 2011 and 2018 rules. The 2011 rules required the disclosure of risks and incidents in publicly traded companies. The 2018 amendments required the disclosure of cyber security policies and procedures. The new guidelines concern reporting *material* incidents within four days of determining such an incident has happened rather than when the incident was discovered.[5] There is one exception: where immediate disclosure would risk national security or public safety and the SEC is notified in writing of this reason for delayed compliance.[6]

The new rules, in practice, may present difficulty in achieving compliance. Materiality is hard to determine as many businesses lack any form of process to perform such an analysis. The determination, according to the SEC, must include the nature, scope, timing and impact — real or reasonably likely — of the material incident.[7] A decision needs to be made regarding who sets these parameters internally and when they have been met. There is also an issue of whether materiality changes once looking in the aggregate at incidents that were previously determined non-material. This would create a need for constant vigilance and evaluation of current and previous events.

The SEC also wants updates provided on previously reported incidents, annual

policy updates about cyber security within business strategy, and information about the board's and management's expertise, which must be proven with credentials.[8] The intent is for investors to be able to evaluate and manage risk exposure. While the SEC has control over public companies, it shows an interest at the highest level of government for cyber security to be a priority.

CASE STUDY: SOUTHWEST AIRLINES

During Christmas week 2022, Southwest Airlines (SWA) had to cancel over 15,000 flights due to a cold-weather event. SWA uses older software to navigate its point-to-point system of flying as opposed to the hub-and-spoke system used by other airlines. This cheaper software has created a technical debt, which is the difference between where it is versus where it needs to be. The way the software code was written made it difficult to fix and expand, and thus less resilient. It is normal for other airlines to track and re-route staff with automation and a website. SWA, on the other hand, requires staff to phone in and re-routing done manually. Such is the lack of agility in this solution that a flight crew was available to crew a plane at Baltimore/Washington Thurgood Marshall International Airport (BWI) while sitting in the boarding area of BWI, however, the manual system was not able to make that easy connection happen, resulting in a cancelled flight and available crews timing out. The system created cascading cancellations for days.

The point-to-point system generally works very well for SWA. In this instance, however, the external influence of the weather impacted negatively on the company due to spending decisions made on the inside. That a severe storm would create such problems, however, was no surprise: not only had the pilot association warned SWA how a severe storm would create technological problems, back in 2014,[9] but a similar incident had already occurred just a few months prior. The system and its manual process have now become of such a concern to SWA's pilots and crew that in their most recent labour negotiations they put demands for a system upgrade ahead of pay increases.[10]

So, what will the fallout be this time? Lawsuits from angry customers and a drop in customer numbers? If SWA pays for a system upgrade, will that cost force the company out of the low-cost (not to be mistaken with budget) airline designation — a unique selling point on which it prides itself? Was this a bad business decision or an utter lack of preparedness and assumption of risk? This is something for a court to decide and to apply the Business Judgment Rule when doing so. Certainly, the financial fallout has already been significant — SWA's expected loss is upwards of US$825m — and it is only going to get worse.[11]

Following on the media's reporting on the pilot association's assessment from 2014, on 12th January, 2023, shareholders filed a lawsuit against SWA in Dallas, Texas.[12] The key point of the lawsuit is SWA's 2020 annual report, which downplayed the technical issues that left it vulnerable to system-wide failure in December 2022. The report touted the benefits of the point-to-point structure over the hub-and-spoke, never mentioning any concerns. Further, Secretary of Transportation Pete Buttigieg is looking for accountability from SWA for the US$7bn it was given as part of COVID-19 relief, as the money was not spent on software but rather route expansion and then, after another injection, payroll.[13] Also, SWA is under investigation by the Transportation Department for potentially scheduling more flights than it could handle, thereby deceiving customers.[14]

On 30th March, 2023, SWA released its action plan based on the December 2022 disruption to services.[15] The SWA 'action plan' has a root-cause analysis, action plan and initiatives listed for each of three critical areas: winter operations, operational investments and cross-team collaboration.[16] These are all forward-facing steps to make its business operations resilient, but they do not change the course of the lawsuits already filed as the harm has already been done.

A WORD ON LEGAL ADVICE

Getting a legal opinion is an accepted practice in the business world. At times it can be a matter of compliance for compliance's sake, but the final decision regarding whether or not to follow their lawyer's advice is always the client's to make. There is an assumption of risk in that course of action, however. At times, a lawyer may be too conservative and going against advice is helpful. At other times, going against legal advice is reckless and prompted by hubris. At all times, however, that assumption of risk is only investigated and litigated if something goes wrong — and if no prudent person with the same information available would have made the same decision (Business Judgment Rule).

FORCE MAJEURE

Force majeure is a clause in a contract that is colloquially known as the 'get out of jail free card' among legal professionals. Most parties to a contract are unaware of its existence, first, and what it means, second. Force majeure is not defined in English law, which is the common law that much of the world uses. The intent of the clause is to suspend an obligation to perform the terms of a contract, with the ability to completely terminate the contract, for events that are beyond the reasonable control of the performer of the contract. The fundamental principle behind the clause is that it would be inherently unfair for a vendor company to be held to a contract and fined for non-performance if they were victim of a disaster. Hence, force majeure denies or minimises the threat of legal action against a party that is in breach of contractual terms due to no fault of its own. To a point …

Force majeure suspends performance of a contract *during* the force majeure event. Termination rights arise if the impact of the event is continuous over a long period of time. What constitutes a force majeure event? Originally force majeure meant an act of God, which is a severe, naturally occurring event with no human responsibility. The definition has grown through the years to include man-made disasters or evolving disasters. Sometimes the actual clause in the contract is defined; other times it is not. When defined, it is possible to add items to the definition that were not originally contemplated because they did not exist — hacking being one such example. Most force majeure clauses in 2020 did not include 'pandemic'; now they do. Not defining the events means the clause is not limited at all except by the bounds of reasonableness, which will ultimately be litigated in court.

Everything in a contract can be negotiated unless it falls under the terms of service (ToS) of a party with massive bargaining power. The most common ToS are related to web-based services, which most users click through and check the box that declares they have read *and* accepted the terms of the agreement. Below is an actual force majeure clause in the ToS for a social media platform (emphasis added):

> 'Additionally, ___ shall *not be liable* to you for *failure or delay* in performing any obligations hereunder even if such failure or delay is due to *circumstances*

> *within* ___*'s control* and/or beyond its reasonable control'.

In this paragraph, the provider says that they will be excused from any liability due to 'circumstances within [their] control'. This segment goes against the spirit and intent of a force majeure clause: circumstances beyond reasonable control. It is easy to read this as saying cyber security is not a priority or their cyber posture is weak at best. The next paragraph from the same ToS displays a more traditional force majeure clause interpretation, but it should be examined piece by piece for what it is really conveying:

> '_____ shall not be responsible for any failure to perform due to *unforeseen circumstances or to causes beyond* _____*'s reasonable control*, including but not limited to *acts of God*, *war*, *riot*, *embargoes*, *acts of civil or military authority*, *fire*, *floods*, *accidents*, *strikes*, *acts or omissions of carriers*, *transmitters*, *providers*, or *acts of vandals*, *or hackers*'.

The clause starts out traditionally with 'acts of God'. Next there is 'war', which is not defined (the USA has not declared war since the Second World War; everything after 1945 has been an 'armed conflict', which has different connotations than 'war'). '[A]cts of civil authority' refers to eminent domain or emergency declaration powers. When the influx of migrants to the US border with Mexico hit El Paso, Texas, in December 2022, the city declared it a disaster and under its powers, took over a convention centre for shelter and processing.[17] If the convention centre had any contracts for meetings, those were (rightfully) cancelled without penalty to the centre. While it may seem confusing that 'fire' and 'floods' are spelled out, they contemplate those started by humans as acts of God happen without human responsibility. Supply chain and vendors are considered with 'strikes; acts or omissions of carriers, transmitters, providers'. This section is dangerous as it embeds the force majeure events of third and fourth parties and would, if upheld by a court, allow a company not experiencing a force majeure event itself to stop performance based on one of its vendors.

The final two items are newer additions based on recent events. '[A]cts of vandals' would now include the recent events from Moore County, NC and Eastern Washington State, where local power stations were maliciously damaged, denying service to the community.[18] '[H]ackers' also deserves special attention: US courts have held that Russian-launched malware attacks could not be 'foreseen' because they were state-sponsored and beyond reasonable control.[19,20] State-sponsored is not the same thing as state-sanctioned, however, so a question remains. Fortunately, courts will evaluate a force majeure clause before applying it.

What is written ultimately does not matter, and the strength of the clause relies on what was done beforehand. European courts tend to protect the consumer and have displayed resistance to broad force majeure clauses. US courts will do their inquiry into whether a force majeure clause excuses performance based on three steps: (1) was the event beyond reasonable control; (2) did the event prevent, hinder or impede performance; and (3) were reasonable steps taken to avoid or mitigate the event or the event's consequences? It comes down to two items that a business continuity professional or lawyer needs to advise on: was it reasonably anticipated and was the business reasonably prepared. This means for any coastal business, hurricane preparedness is non-negotiable. With cyber security, on the other hand, 'reasonably prepared' becomes more difficult to

define and comes back to spending decisions by board members and officers.

OTHER CONTRACT ISSUES

Companies and businesses continuity professionals should also consider the impact of doctrines. *The Restatement (2d) of Contracts* is a legal treatise for judges and lawyers based in common law. The doctrines of impossibility (§261) and frustration of purpose (§265) rely on an unforeseeable event that makes a performance impractical or impossible by no fault of that party. The circumstances are strikingly similar to that of a force majeure clause, and it becomes a fail-safe of sorts, especially when advising companies that are part of the supply chain.

There is an obligation to allocate supply. If an event comes about that is explicitly force majeure or qualifies for protection under the frustration of purpose or impossibility doctrines, there can be an ancillary conflict with customers seeking to get the largest share of a limited supply. Customers can sue a company when it fails to provide at least some supply. The basis of such a claim is that the company decided to allocate its supply in a specific way, not because of the force majeure event. Business continuity professionals should be advising on allocation to avoid litigation and finding acceptable like-kind supply.

WHAT CAN A BUSINESS CONTINUITY PROFESSIONAL DO?

Business continuity professionals are not in possession of top-secret information: lawsuits are part of public record from the moment they are filed. The first suggestion is to include shareholder-derivative lawsuits in the risk analysis portion of the business continuity plan. This will no doubt become useful when reviewing the strategy for allocating budget between those operations and measures that are most vital to maintaining continuity and those that are most likely to leave the company open to litigation if they are absent or weak.

The second suggestion is to coordinate with in-house or outside legal counsel, depending on which one the company has. When it comes to shareholder-derivative lawsuits and avoiding them, while having a seat at the boardroom table or occupying a C-suite office may not be options, leadership buy-in is. Having a united front from allies within can be well received. Align with the lawyers to speak to the nuts and bolts of the programmatic solutions to the legal concerns. It is better for leaders to understand if the legal theory is joined with specific options offered by subject matter experts.

The third suggestion is to read each contract for the force majeure clause and translate what each part means. This becomes another layer of evaluating the provider a company is contracting with. If the clause is too broad, alert leadership to the possible weaknesses associated with the provider's own business continuity plan or their posture on further contracting with entities that do not have a business continuity plan. When it comes to negotiating the company's own force majeure clause, work again in conjunction with the lawyers with an honest assessment of the posture of the company and make sure those disasters and disruptions are accounted for to excuse the company from performing without penalty.

Finally, take a moment with leadership and legal and discuss contracting for specific allocation of supplies. It is entirely possible that an incident could expose the company to a breach of contract lawsuit if things are not planned for in advance. It is not difficult to add a clause in a contract that looks like the following:

> 'In the event of a Force Majeure incident, Frustration of Purpose, or Impossibility, the actual number of products provided will be reduced to a percentage that allocates the supply to active contracts due during the incident commensurate with order volume' (or something to that effect).

Further, aside from thinking about alternative suppliers to use as part of a business continuity plan, considering alternatives for the purpose of avoiding a lawsuit may present opportunities for having extra alternatives. Tactics like these will protect the company, please all stakeholders and make the business continuity professional an even more vital part of the team.

CONCLUSION

Disaster and disruptions are not the only incidents that can bring a business to its knees. Spending decisions, contract negotiations and supply allocation fall plainly within the risks a business will face. While they have the spectre of legality looming over them, business continuity planning can assist and save the day. Reasonable and informed decisions are always in alignment with duties owed by the highest levels of a company.

Who owns the decisions for when a disaster or disruption (or even a 'material' cyber security event) has taken place? Is it the business continuity practitioner? The chief information security officer? The lawyer? Having a discussion is not necessarily having administrative bloat. Each is a subject matter expert in their respective area: much like G. W. F. Hegel posited with his theory about dialectics, two equally strong parts are even stronger when combined. Business continuity professionals should be emboldened to assist with making those decisions alongside and in partnership with the legal team if they have a general working knowledge about the legal aspects of business continuity planning.

References

(1) Martin, C., Reitema, P. and Suskin, H. (2020) 'Early lessons from the first COVID-19 securities class action lawsuits to hit cruise line and pharmaceutical company', American Bar Association, available at: https://www.americanbar.org/groups/litigation/committees/securities/practice/2020/norwegian-cruise-lines-covid-19/ (accessed 9th July, 2023).

(2) Hussein, F. (2021) 'Tyson officials didn't protect company from pandemic, suit says', Bloomberg, available at: https://news.bloomberglaw.com/safety/tyson-officials-didnt-protect-company-from-pandemic-suit-says (accessed 9th July, 2023).

(3) Pennsylvania Attorney General (2022) 'Attorney General Josh Shapiro announces $16 million settlement with Experian and T-Mobile over data breaches', available at: https://www.attorneygeneral.gov/taking-action/attorney-general-josh-shapiro-announces-16-million-settlement-with-experian-and-t-mobile-over-data-breaches/ (accessed 9th July, 2023).

(4) Experian (2022) 'Annual report financial review', available at: https://www.experianplc.com/media/annualreports/2022/reports/028-financial-review-1074-T01.html (accessed 20th June, 2023).

(5) US Securities and Exchange Commission (2023) 'SEC adopts rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies', available at: https://www.sec.gov/news/press-release/2023-139 (accessed 31st July, 2023).

(6) *Ibid.*

(7) *Ibid.*

(8) *Ibid.*

(9) Southwest Airlines Pilots Association

(2022) 'Leadership update', available at: https://www.swapa.org/news/2022/two-legacies/ (accessed 9th July, 2023).
(10) Union of Southwest Airlines Flight Attendants (2022) 'President remarks', available at: https://makeitrightswa.org/wp-content/uploads/2022/05/President-Remarks-March-2022-RH-ed.pdf (accessed 9th July, 2023).
(11) Koening, D. and Associated Press (June 2023) 'Buttigieg's Transportation Department says it's investigating Southwest Airlines "holiday debacle that stranded millions"', *Fortune*, available at: https://fortune.com/2023/01/26/southwest-airlines-investigation-dept-transportation-pete-buttigieg-holiday-flights-cancelled-debacle-stranded/ (accessed 9th July, 2023).
(12) Stempel, J. (2023) 'Shareholders sue Southwest Airlines over flight meltdown', Reuters, available at: https://www.reuters.com/business/aerospace-defense/southwest-airlines-sued-by-shareholders-over-flight-meltdown-2023-01-12/ (accessed 20th June, 2023).
(13) Rucinski, T. and Shivdas, S. (January 2021) 'American Airlines, Southwest post record losses and signal need for more aid', Reuters, available at: https://www.reuters.com/business/american-airlines-southwest-post-record-losses-signal-need-more-aid-2021-01-28/ (accessed 20th June, 2023).
(14) Koening, ref. 11 above
(15) Southwest Airlines (2023) 'Final summary and action plan re: December operational disruption', available at: https://swamedia.com/releases/release-0e5c5e4d7e00de7004a990a48818295a-final-summary-and-action-plan-re-december-operational-disruption (accessed 20th June, 2023).
(16) Southwest Airlines (2023) 'Travel disruption action plan', Southwest Airlines, available at: https://www.southwest.com/travel-disruption-action-plan/ (accessed 20th June, 2023).
(17) Fischer, F. and Mancini, N. (2022) 'El Paso Convention Center, 2 vacant schools will be used as migrant shelters, city says', KFOX14, available at: https://kfoxtv.com/news/local/el-paso-convention-center-2-vacant-schools-will-be-used-as-migrant-shelters-city-says-bassett-middle-school-morehead-middle-school-immigration-december-20-2022-title-42 (accessed 20th June, 2023).
(18) Planas, A. and Romero, D. (December 2022) 'Four substations attacked in Washington State, leaving thousands without power', NBC News, available at: https://www.nbcnews.com/news/us-news/three-substations-attacked-washington-state-rcna63214 (accessed 20th June 2023).
(19) *Princeton Cmty. Hosp. Ass'n, Inc. v. Nuance Commc'ns, Inc.* Westlaw: S.D.W.Va; 2020. p. *5.
(20) *Heritage Valley Health Sys., Inc. v. Nuance Commc'ns, Inc.* F Supp 3d: W.D. Pa.; 2020. p. 184, n4.