ASA

Annie Searle & Associates LLC

Research Note

Delta Airline's Power Outage Risk Analysis

Sukhman Tiwana

July 2017

Keywords: Operational Risk; IT Risk; Reputational Risk; Airline Industry

Abstract: This paper discusses the power outage that sent shockwaves through Delta Airline's operations in August 2016 for multiple days, resulting in significant financial and reputational losses. The crisis revealed some underlying system and operational weaknesses. The author examines some of the potential steps Delta can take to reduce risks and improve future operations.

Introduction

A switchgear failure resulted in a crisis for Delta Airlines Corporation, causing multiple negative impacts to its business. On August 8th 2016, Delta lost access to Georgia Powers and its reserve generator, due to a power outage. This resulted in a "shutdown of Delta's data center, which controls bookings, flight operations and other critical systems."[1] Even when the power was restored, Delta's "critical systems and network equipment didn't switch over to backups. Other systems did."[2] Because of this power outage, Delta recognized vulnerabilities in its current systems. Due to this occurring in its Atlanta headquarters, it cancelled 2,300 flights over three days and its revenue for August 2016 declined approximately $100 million.[3] It faced operational risk failures in external vendors, dependencies on systems, and vendor risk that resulted in the risk of reputation damage, financial loses, and processes flaws. Delta could have prevented some of the revenue lost by better maintaining its systems, but the power outage was a black swan event. Delta is not the only airline company that has struggled with its Information Technology (IT) management; this has been a common issue across the airline industry. There are regulations in place that should assist these companies in their management, but even the auditors ignore or do not identify flaws.

Risk Environment

Delta's initial risk came from its high dependencies on an external vendor for power - Georgia Powers. The IT systems and networks cannot be supported without the external vendor

maintaining its operational and IT systems.[4] Delta needs to ensure that any vendor they use is updating and maintaining its technology systems and software. The vendor could have used a damaged switchgear or failed to replace the switchgear in a timely manner. Potentially, the power company also needs to improve its processes. However, the power outage may have been unpreventable, much like a natural disaster, because it did not have any warning signs. There is a chance that switchgear went out without any warning.

However, the power outage revealed Delta's systems risk. The risk came from Delta not merging its technology properly during new company additions. Perhaps Delta did not want system merges to affect its existing business processes and customers. Therefore, the company could have focused on finding the fastest way to merge its IT infrastructure without evaluating the impact and stability of the overall system. The *Wall Street Journal* reports that "the vulnerabilities in Delta's computer system … raises questions about whether a recent wave of four U.S. airline mergers that created four large carriers controlling 85% of domestic capacity has built companies too large and too reliant on IT systems that date from the 1990s. Delta merged with Northwest Airlines eight years ago."[5] Potentially, Delta may not have merged the IT systems of these four companies efficiently, resulting in Delta having issues with its computers not restoring to backup mode when the power did come back.[6] Regardless of the cause, the airline's systems were not able to handle the downtime and recover its state.

Because of these mergers, Delta's software systems may have been running on outdated technology, which goes back to 1990s, and if this is the case then its system runs the risk of breach and stolen data. When Delta merged with Northwest Airlines, it hired IT specialists from other companies to "upgrade their technology infrastructure to make it more durable, adding redundant power supplies to their computing centers and other facilities, [and] increasing the number of backup telecom providers."[7] It seems they added onto the existing IT infrastructure for both of these corporations, thought this approach did not solve the underlying technology problem. Adding technology is the quickest way to merge technology, but creating a new infrastructure is challenging and time consuming.

Business Impact

Delta's miscalculations of the IT systems influenced its business processes across the board. Any damage to its technology infrastructure could result in impacting "customer service ... business disruption and its adverse financial and reputational consequences."[8] They are aware of the potential damage from the systems being down for long periods; however, they did not treat or terminate this risk and instead, tolerated the risk, which resulted in increasing its overall risk. According to IT experts, "these systems — which run everything from flight dispatching to crew scheduling, passenger check-in, airport-departure information displays, ticket sales and frequent-flier programs — gradually have been updated but are still vulnerable."[9] Its systems failure disturbed its business processes and customer experience because the passengers were unable to fly to their destinations in a timely manner. In addition, their airport staff was unable to do their work efficiently because the company's systems were down. *The Washington Post* reports that some agents' "fallback seemed to be returning to pen and paper: Some airport agents started

writing out boarding passes by hand."[10] The agents did not have pre-printed forms that they could use to make this process efficient. They were writing the entire boarding pass by hand and trying their best to provide services to their customers. Many airports' staff worked around the clock because per the CEO of Delta, Ed Bastian, "there aren't a lot of crews to bring in to replace them. That's not how the system is designed."[11] Even though Delta mentioned in its 10-K Form from the fiscal year ending in December 2015 that it had "prevent disruptions and disaster recovery plans," its plan was not effective because it lacked a rotational employee program.[12] Their staff experienced fatigue and stress, which resulted in bad customer service and increased the risk of losing their customers.

The airline's business process increases its financial risk, because their customers and staff were unhappy with their process, by reimbursing its customers and paying its employees for overtime. Its current business process is paying its staff overtime, which results in financial damage for Delta. According to Delta Professionals, "Delta extended its offer of compensation to customers significantly affected by delays or cancellations to cover Tuesday. The airline also provided hotel vouchers to several thousand customers, including more than 2,000 on Monday night in Atlanta."[13] Delta struggled to arrange flights that met its customers' needs at no additional cost, which also affected their "passenger revenue per available seat mile (PRASM)" because now they were providing business to their competitors.[14] According to *Fortune*, Delta's PRASM "declined 9.5 percent in August from a year earlier" because the airline paid for overtime and reimbursed its customers.[15] Delta had no other choice but to absorb the financial loss because it was forced to choose between reputation and financial loss. It valued its customers and employees because it had spent years trying to gain trust and maintain a long-term relationship with most of them. Additionally, there was a higher financial risk in the coming months because it had to repair and improve its IT infrastructure, which took a toll on its budget.[16] The company may have been able avoided financial losses by having a crisis management plan or by troubleshooting its systems to check if they were outdated.

The Delta Airlines' reputation was at risk due to this power outage because it was not living up to its promises of flying a customer to their destination. In the *Harvard Business Review*, Robert G. Eccles, Scott C. Newquist, and Roland Schatz say that "Three things determine the extent to which a company is exposed to reputational risk." These are reputation reality gaps, changes in beliefs and expectations, and weak internal coordination.[17] Delta had a weak internal coordination because it did not have a strong method in place for crisis management. Its employees were unable to do their work for at least four days because that is how long it took to get a partially working system back up and running, which reveals that its internal coordination was not efficient.[18] According to its 10-K Form from fiscal year ending in December 2015, Delta mentioned how its business depends heavily on IT and that any downtime could result in reputational damage and poor customer service.[19] Delta's reputation was certainly damaged in August, because even after allowing changes to booking at no cost, customers continued to vent their frustration on social media platforms.[20] The *Wall Street Journal* reports that "on a typical day, there are about 3,600 social conversations involving Delta on Twitter, according to social

media analytics firm Networked Insights. On Monday morning, there were 43,000."[21] Even the people who were not physically experiencing the bad customer service were aware of the service through social media. Customers spent hours at the airport while Delta agents figured out flight status, booked hotels, and booked new flights. There were passengers who complained about wasting their time and being frustrated with the management process, even though the airline agents passed out blankets, water, pizza, and gave updates on the status of flights while their customers were waiting.[22]

Airline Industry IT Risks

Delta is not the only airline that has vulnerabilities and hazards in its systems, disaster recovery plans, and process management - there are others in the airline sector that face similar crisis due to its technology. Southwest Airlines cancelled 2,300 flights due to a router failure at their data center in July 2016.[23] It took Southwest 13 hours to reboot the carrier's computer systems, which is similar to Delta's experience where the system recovery was the major pain-point. *The New York Times* said:

> "In Southwest's case, a backup system was in place, but the airline said that system was not triggered as it should have been when the router failed. And Delta said on Monday that it was investigating why some of its own critical operations had not switched over to backup systems."[24]

Both companies were struggling with its backup systems in place. United Airlines also faced issues with its computer systems last year and American Airlines had a bug in its iPad software, which resulted in cancelations of flights.[25] Therefore, some of the airline sector does not have updated and powerful technology to manage its company's infrastructure during a crisis, event, or incident. They do not have IT systems and the plan in place to recover quickly without affecting their business, which results in influencing their financial revenue due to the cancellations of flights. *NPR* reports "experts say the airlines are struggling to merge and upgrade their IT infrastructure to keep pace with rapid growth."[26] The airline industry struggles to keep up with the rapid growth and change in technology, which were the reasons behind the lack of mitigating the risk of processes and systems. Therefore, since they did not have processes and systems in place that met their needs, they were unable to come up with sufficient disaster recovery plans. In order for the airline sector to lower their risk, they need to change their technology management style before they damage their reputation or finances to a degree where they cannot recover.

To mitigate risk in the airline industry, there are both U.S. governmental and international regulations in place. One of the regulations is called Sarbanes-Oxley (SOX) Compliance, which requires the signing officer to be responsible for checking the business's internal controls and only sign the paperwork if they meet the guidelines.[27] In addition, SOX Compliance requires that the company's "entire IT infrastructure—from server and network security to IT practices and operations—must be reinforced and configured to maintain and demonstrate compliance in the event of an audit."[28] Delta Airline did not have IT practices and operations in place that meet its

IT infrastructure needs. Therefore, the auditors should have caught this system flaw, which means they not only have vendor risk in terms of their power suppler, but also with their auditors. In addition, the auditor should have highlighted how Delta Airlines does not have a disaster recovery plan in place, which might have prevent the need for staff to create paper-based boarding passes, which increased their risk of fraud occurrence during those three days because anyone could have created them.[29] Therefore, during this crisis, Delta Airlines highlighted its weak internal controls, which means it is likely non-compliant with the SOX Compliance regulation. The auditors should have spotted the gaps in the disaster recovery plan or their proposed plan.

Recommendations

To improve its management system and avoid a black swan event leading to a greater crisis, Delta needs to change their business management style. Therefore, to reduce its vendor risk, it needs to meet with its vendors to ensure its internal control management meets its needs, since power supply is essential to IT systems and its business. It can take this opportunity to cross check its policies and guidelines with each vendor. It also needs to change its systems because of the new regulation, which is General Data Protection Regulation (GDPR) Compliance that goes in effect in 2018. The GDPR Compliance was enforced by the European Parliament & Council to manage European citizens' personal data. This law gives the citizens of Europe the right to control and regulate their personal data.[30] Therefore, when this law goes in effect, Delta Airlines IT infrastructure should be able to secure and manage data without any problem. Per their 10-K Form for ending fiscal year of December 2015, it "regularly review and update procedures and processes to prevent and protect against unauthorized access to our systems and information and inadvertent misuse of data."[31] However, even after regularly reviewing its systems, it was unable to get its system in backup mode, which might have been due to its merging scheme and lack of management of IT systems. It should create an effective plan for merging with other companies and its IT infrastructure. In addition, it should plan on how it is going to manage and update its IT systems regularly.

Another recommendation is to improve its disaster recovery plan and its overall IT systems. To do this, Delta should hire an auditor to conduct analysis and suggest changes to its system, which would reduce its system risk and improve its processes. Alongside this, Delta should create an improved disaster recovery plan that works alongside its IT, and it should train its employees on what they should do during an event, incident, or crisis. In order to come up with a stable plan, it should ask its employees of what they discovered as an issue during the power outage. The company does not have to agree with the suggestions, but this will help them understand what the crisis management was like, and what it needs to improve. The Delta Airlines could create forms that agents' fill out in replace of printing boarding passes when they are facing IT problems. In addition, it should have a printed copy of the schedule for the flights and should communicate with employees at the gate using a phone. Delta should have a disaster plan accommodating its IT systems when they are down. When Delta has established a process for disaster and technology recovery, it should check it with various scenarios. Because of this, it will

reduce its financial risk through an employee rotational plan incorporated into the recovery plan resulting in employees not working around the clock. This way, employees could provide services to customers with energy, which would reduce the company's reputational risk. In order to ensure that its reputation is not at risk, Delta should create a "strategic alignment, cultural alignment, quality commitment, operational focus, and organizational resiliency."[32] These five frameworks of managing reputational risk will ensure that the board is overseeing the company, the company's values are followed, its customers are satisfied, and it has a controlled environment.[33] Ultimately these management frameworks will improve Delta Airlines' customer and employee interactions and the organization will have a unified understanding of guidelines and principles. Because of these changes in its overall business, it could be the ideal airline for its IT systems, processes, and disaster recovery mechanisms.

---

[1] Carey, Susan. "Delta Equipment Malfunction Triggered Loss of Power." *The Wall Street Journal*. 09 Aug. 2016. Accessed Dec. 2016 <www.wsj.com>.
[2] "Delta Operations Update for Tuesday, August 9." Delta Air Lines. 9 Aug. 2016. Accessed Dec. 2016 <www.pro.delta.com>.
[3] "Here's How Much Delta Lost On Its Massive Flight Outage." *Fortune*. 2 Sept. 2016. Accessed Dec. 2016 <www.fortune.com>.
[4] Carey
[5] Ibid.
[6] "Delta Operations Update for Tuesday, August 9."
[7] Carey
[8] *Delta Air Lines Form 10-K For the Fiscal Year Ended December 31, 2015*. U.S. Securities and Exchange Commission. *Form 10-K For the Fiscal Year Ended December 31, 2015*. Accessed Dec. 2016 <www.sec.gov>.
[9] Carey
[10] Peterson, Andrea. "Delta's Massive Computer Outage Is Part of a Much Bigger Problem." *The Washington Post*. 8 Aug. 2016. Accessed Dec. 2016 <www.washingtonpost.com>.
[11] Isidore, Chris, Jethro Mullen, and Joe Sutton. "Delta Flights Resume but Cancellations and Delays Continue." *CNNMoney*. 8 Aug. 2016. Accessed Dec. 2016 <www.money.cnn.com>.
[12] *Delta Air Lines Form 10-K.*
[13] "Delta Operations Update for Tuesday, August 9."
[14] Here's How Much Delta Lost On Its Massive Flight Outage."
[15] Ibid.
[16] Carey
[17] Eccles, Robert G., Scott C. Newquist, and Roland Schatz. "Reputation and Its Risks." *Harvard Business Review*. Feb. 2007. Accessed Dec. 2016 <www.hbr.org>.
[18] Carey
[19] *Delta Air Lines Form 10-K For the Fiscal Year Ended December 31, 2015.*
[20] Carey
[21] Carey
[22] Isidore
[23] Kurtz, Annalyn. "Delta Malfunction on Land Keeps a Fleet of Planes From the Sky." *The New York Times*. The New York Times, 8 Aug. 2016. Web. 05 Dec. 2016.
[24] Kurtz
[25] Kurtz

[26] Booker, Brakkton. "Delta Air Lines Cancels Nearly 700 Additional Flights." *NPR*. 9 Aug. 2016. Accessed Dec. 2016 <www.npr.org>.
[27] "Sarbanes-Oxley Act Section 302. Sarbanes Oxley 302 Made Easier." SOX Law. N.D. Accessed Dec. 2016. <www.soxlaw.com>.
[28] "Sarbanes-Oxley (SOX) Compliance: Comprehensive, Cost-effective and Risk-based." *Tripwire*. N.D. Accessed Dec. 2016. <www.tripwire.com>.
[29] Peterson
[30] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016." *Official Journal of the European Union*, EUR-Lex. 27 Apr. 2016. Accessed Dec. 2016 <www.eur-lex.europa.eu>.
[31] *Delta Air Lines Form 10-K For the Fiscal Year Ended December 31, 2015.*
[32] "Board Oversight of Reputation Risk." *Board Perspectives: Risk Oversight 83 (2016): 1-4.* Protiviti, Sept. 2016. Accessed Dec. 2016 <www.protiviti.com>.
[33] "Board Oversight of Reputation Risk."