

## **Worldwide IT and Business Impacts From Volcanoes**

*By Anyck Turgeon, Robert Riggan II and Jim Satterfield*

What lessons have we learned from the volcanic eruption of Eyjafjallajökull in Iceland?

Four major eruptions of the Iceland volcano have occurred in recorded history. They were in 920, 1612, 1821 to 1823, and now in 2010 respectively. Within only seven days, the immediate impacts of the latest eruption included a reported \$1.7 billion in losses for the airlines, over 102,000 flights cancelled, and more than 750,000 passengers affected. The total incurred expenses and losses will far exceed these preliminary numbers. Similar disasters, such as hurricane Katrina, reportedly incurred initial expenses in the millions and now, per the IMF, resulted in an excess of \$75 billion in total losses. It is apparent that we are far from having a complete financial estimate on the final cost of this volcanic eruption but, we can already anticipate that it will be monumental.

It is critical for us to evaluate our state of collective preparedness as well as assess the costs and risks associated with our global interdependencies. We may be able to overcome challenges in one remote area of the world, but how do we deal with the global implications and potential risks?

### **The Impact of an Eruption and Volcanic Ash**

The volcanic eruption of Eyjafjallajökull in Iceland is one of an increasing number of disasters that we deal with each year. According to the IMF, the number of disasters has grown from less than 100 in 1975 to more than 400 in 2005. The IMF estimates that approximately 2.6 billion people were affected by natural disasters over the past 10 years.

Some impacts of the previous eruption sequence in the 1820s of Eyjafjallajökull included an enormous loss of perishable goods, long-term climatic changes, substantial adjustments in trade balances, and extensive health challenges. Although our more civilized community infrastructures and modernized technologies have now empowered us to limit some of the damages, our level of global inter-dependency has also brought new issues into play such as domestic and international air traffic, regional environmental and technological compliance breaches, and disposal of hazardous and non-hazardous wastes. Most importantly, our current technologies failed to prepare us for this event. Disaster-related innovations in climatology, cleantech, recycling, high-tech, and other related fields are definitely required. A new wave of multi-disciplinary technologies is needed that encourages and facilitates collaboration, which is atypical, and that will require trust as well as ongoing changes.

Are our innovative minds of today properly enabled by executive management, the investment sector, and governmental oversight to bring us toward a more prepared tomorrow with lower natural disaster impacts, enhanced global collaboration, and advanced preparedness? How can we better anticipate the costs and challenges of natural disasters?

### **The Pros and Cons of Volcanic Eruptions**

One of the key issues and most visible manifestations of this disaster is volcanic ash. Its adverse affects have been obvious. Not so obvious, however, are some of its benefits. Contrary to common belief, when volcanic ash is mixed with water, the result can generate sulphur dioxide deposits with a Ph under 7. Agriculturally, this serves as a plant-ready nutritive sulfur source. It has highly-beneficial potential for use in the production of fertilizers, road construction materials, and pharmaceutical drugs . Could we not benefit globally from the capture, containment, and re-use of this natural source of sulfur? The challenge lies in determining and implementing the most efficient and cost effective methods for the capture and reutilization of it.

That said, the negative impacts of volcanic ash remain largely unmeasured and poorly remediated. It creates seemingly insurmountable challenges both during and following a major eruption. Though we have improved in our overall handling of the recovery phase of such events, we have not fully learned from past experiences. Below is a simplified glimpse into the issues involved and a summation of the challenges that we have encountered in relation to volcanic eruptions and ash distribution:

At the microscopic level, volcanic ash is a glassy material with sharp, jagged edges. One of its most obvious and immediate adverse affects is its impact upon air quality and health. It can cause respiratory distress or aggravate pre-existing medical conditions in humans and animals. Over time, extreme exposure can kill vegetation and lead to the death of animals and people. At the macro level, volcanic smoke and ash obstructs visibility, thus grievously affecting transportation in all forms. In our modern environments, volcanic ash also kills technologies. In fact, airborne dust particles are the arch enemy of technology, and there are some simple aeronautical examples depicting the tremendous challenges that volcanic ash can create.

In 1989, KLM flight 867 took a death defying plunge from 28,000 ft to 13,000 feet while flying over Alaska. A sudden burst of volcanic ash penetrated the engines, melted and coated the turbines – resulting in all four engines shutting down. In 1982, a British Airways plane experienced a significant scare as the flying crew was able to barely restart ash-coated engines during a 37,000 foot to 12,000 foot dive. Some claim this was a miracle. With an excess of 125 similar incidents being recorded since the 1980s, it is not surprising that the aviation authorities banned flights to avoid repeating such potentially fatal encounters.

Surprisingly, when it comes to human health concerns and vulnerabilities for high-tech facilities on the ground, there are little to no preventative measures and/or practices in place. Are the thousands of large data centers around the globe prepared to battle such microscopic, yet potentially damaging threats? Are we just too focused on wealth creation? Are we ready to face a volcanic explosion such as Laki or Katla that have the potential to be 10 times worse?

For those interested in assessing risk and probability, it is important to clarify that Katla is a massive volcano buried under approximately 550 yards (500 meters) of ice that is located only 12 miles from Eyjafjallajökull. It has consistently erupted alongside Eyjafjallajökull during the last three eruption cycles: (i.e.: in 920, 1612 and 1821 to 1823). The probability of more chaos affecting Europe and the world is a factor that can

no longer be ignored – even if a secondary explosion may not be immediate. Yet, as press coverage of Eyjafjallajökull has passed, most of us have decided to treat Katla as a fairly low risk. Our attention therefore is now pulled to other directions without taking much time to review what lessons we could learn.

From large to small companies, governments to individuals, we must now begin thinking as the global community that we are – a community that modern transportation and the advent of the Internet has transformed into a giant, interconnected village with immeasurable interdependencies and influences. As electronic access is opening doors to global business transactions and exchanges, there are also direct and indirect impacts from natural disasters that we must all consider. For example, it is reported that the volcanic eruption in Iceland has created economic losses exceeding \$3.8 million per day in Kenya alone. It has also been affecting the economic strength of all European trading countries and corporate entities. Although more accurate financial loss estimates are not available as of yet, it is clear that we need to be concerned about its impact upon not only the local, but the state, regional, and global economies as well. Keep in mind that incidents such as the 1906 earthquake of San Francisco allegedly cost the equivalent of trillions of dollars over time. Hidden are the costs that continue to impact all of us as the final bill trickles its way down and is redistributed through elevated prices.

Air travel, tourism, and agriculture are three of the sectors that the press speaks of most, but what about IT and vital data centers? Although Iceland is not a renowned international hub for technology innovation, several European and American-based companies such as Oracle, Google, and Microsoft have considered at various points in time establishing data centers in that region. Supplementing Iceland's price-friendly real estate and fantastic land availability are geothermal energy benefits that result from the volcanic activity. Geothermal heated water and steam generated electricity are just a few enticements. Europe's data retention, privacy, and disclosure requirements have also contributed to the appeal of such a location.

As we ponder these overarching issues and look at our respective states of readiness, it is incumbent upon each of us to re-examine our continuity posture with a keen eye on our technological infrastructures. In so doing, consider the following:

### **Latest Top 10 Disaster Recovery and Business Continuity Recommendations**

Given the higher probability of an even more catastrophic challenge in Iceland and elsewhere, below are the latest top 10 disaster recovery and business continuity recommendations:

1. *BUSINESS CONTINUITY & EMERGENCY PREPAREDNESS FOR ALL*  
*As soon as you post content on a Web site, you automatically become a global entity in some respects. Purchasing transactions may not be performed internationally; however, access to your content is global. How can you ensure that your organization will survive and hopefully still thrive at all times – especially if one of your suppliers may not be capable of delivering services / products for an extended period of time?*

Aim for flexibility, adaptability, agility, and redundancy. Ensuring that you have alternative options provides flexibility. Cross training personnel in mission essential functions allows for adaptability. Regular rehearsal of event response protocols increases agility. Prearrangement of secondary and tertiary sources of supplies, services, and information storage and recovery capabilities is what redundancy is all about. With your governmental, corporate, and family/individual specific plans, it is critical that emergency readiness plans be reviewed, revised, and tested or exercised each year. In all cases, be prepared to engage with one or more third parties such as trusted business partners or family members to assist you in the event of a major natural disaster.

2. *DEALING WITH DISASTER AS A MEMBER OF THE GLOBAL COMMUNITY*  
*How can you ensure full business continuity if an entire continent is affected? What would happen to the rest of your business if North American air traffic was suspended for a prolonged period of time?*

For medium to large corporations, consider a multi-continental disaster recovery plan that includes a highly secure and tested cloud with enhanced service-level agreements and monitored access control policies.

3. *ALWAYS PLAN FOR THE WORST*  
*How can you continue delivering services and products to your customers if your offices are largely unreachable?*

As staff may become ill, or your region may experience severe climatic conditions, it is important to be prepared for full lights-out operations. Corporations, government services, and other key public infrastructure may have their operations suspended for a period of time – which is also referred to as static or hiatus mode. Operations may be halted – like airlines were banned from flying. Their business systems, however, were extensively stressed by trying to deal with unusual conditions such as rescheduling of flights, crews, passengers, etc. Subsequent to such circumstances the transition to recovery mode is also critical as every non-operational minute may have a substantial hidden set of costs. Having a simple, viable, well practiced business continuity plan in place prior to catastrophic events could mean the difference between business survival and failure.

4. *DEALING WITH GEOGRAPHICAL AND TECHNOLOGICAL DIVERSIFICATION*  
*How can you ensure business continuity if your corporate community can't reach their assigned work sites?*

Diversification is the key. As the likelihood that employees, partners, customers, etc. may become stranded for extended periods of time, it is important to consider alternative business and communication methods such as video teleconferencing, teleworking, and toll free messaging centers for all or most of your corporate community members. Keep in mind infrastructure bandwidth and alternate sources at the ISP level. Additional compliance requirements may be forthcoming for executives, board members, and IT practitioners. As their

information needs and corporate liabilities are increasing, diversification of business practices and communication methodologies may become a topic worth consideration.

5. *THE CASE OF MULTI-VENDOR REDUNDANCY & PREPAREDNESS*  
*What can be done to reduce dependency on a particular vendor?*

Consider multi-vendor negotiations. Having multiple suppliers on hand is critical to precluding a single point of failure. Many companies keep minimal inventories of administrative, technological, and other supplies as a matter of prudent fiscal accountability. To ensure continuity of operations, long-term planning of various supply options should be in place well in advance of any challenges. Reliance on only regional or single source suppliers no longer suffices. Negotiations should start now for multiple supply options from providers that meet your vendor assurance requirements. Do not forget service vendors as well. Having primary, secondary, and tertiary service agreements in place will not only enhance your continuity posture, but will also provide you leverage, via vendor competition for the top slots, in service contract negotiations.

6. *DISK VS. TAPE STORAGE*  
*What are the best long-term storage practices?*

Maintain a balanced and mixed use of tape and disk-based data storage. Many IT practitioners are migrating their entire storage infrastructure from tape to disk. This may not be a wise approach given disk's increased vulnerability to airborne contaminants – such as dust, metallic, and crystalline particulates. These can penetrate the filtered breathing vents of disk environments, clog the filters, and overheat the drives – causing more frequent head crashing and data loss. This creates a need to give more consideration to a balanced approach between disk and tape data storage.

7. *BACKUP AND RECOVERY BEST PRACTICES*  
*What can be done to minimize data loss and ensure data continuity?*

Adjusting the frequency of your backups is also important depending on the level of critical challenges in your environment. Many organizations are moving toward close-to-real-time replication and migration paths. This may need to be modified to meet new system architectural requirements. More importantly, performing ongoing recovery tests and removing as many causes for potential damages is critical. Several tools are available to measure and ensure the recovery of your business-critical data. Investigate your options.

8. *BEST PRACTICES IN DATA CENTERS*  
*How can I minimize the impact of volcano ash in my data centers?*

As the regional air quality may be affected by volcanic ash and other particulate matter, it is almost certainly a good idea to plan for more frequent filter changes

to your HVAC systems so that they remain clear, perform efficiently, and so that there is less potential for overheating of temperature sensitive equipment.

9. *FRAUD IN TIMES OF DISASTERS*

*How can I minimize data breaches and theft that arises due to a disaster situation?*

As has been the case in other catastrophes such as 9/11, new fraud opportunities are frequently capitalized upon by e-criminals and others. Be sure to implement proactive security polices, perform full analytical risk assessments, activate ongoing monitoring services, ensure the successful completion and integrity of live audits, and provide consistent security training. Remember, humans are the weakest link in a technological chain. Sound training diminishes the potential for this weakness to be exploited. Work closely with all business stake holders so that you can best manage new resources and staff acquisitions.

Additionally, ensure that you report unusual activities to your local law enforcement (or organizations such as [www.infragard.net/](http://www.infragard.net/) or [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)) and consider posting information covering data breaches on your Web site so that customers know what to do or what not to do.

A special toll-free line to address customer inquiries about security issues may also be appropriate, depending on your type of business. In Europe, usage of smart chips has apparently reduced the number and cost of breaches. We are, however, far from a fully-integrated and intelligent set of devices that would deter crime. As organized crime is now making more money from e-fraud than other traditional criminal activities, the addition of added deterrence will remain an ongoing area in need of improvement.

10. RE-EVALUTE THE RESILIENCY OF YOUR ENTIRE IT PRACTICES

*Is your data still located at the most secure location? What are you doing to ensure this?*

Re-evaluate the resiliency of your entire IT infrastructure. Placing a data center in the basement of a building may obviously not be the best idea in some regions. Ensure that your data is fully protected throughout all stages of its existence and implement data retention practices that can be easily followed by all communities that depend on stored data. Deletion and destruction policies are particularly challenging to implement correctly, as the proliferation of copies (especially in an over-virtualized environment) may be challenging to track. Storage guru David Hill has written an excellent book on the topic titled, "Data Protection: Governance, Risk Management, and Compliance."

The number of disasters has been rapidly increasing. At this time, we have no ability to stop them, but we are becoming more efficient at responding to their aftermath. In addition, we must learn how to become even more responsible global citizens and learn

how to use our current technologies in better ways, thus creating a more resilient environment.

*Special thanks to contributors: Jean Beauchemin, Jeff Briel, Curtis Breville, Megan Brownwell, Eddy Coenye, Eric Cowperwaite, Scott Draughon, Mark Gaydos, David Hahn, Leslie Harvey, David Hill, Don Hubbard, Kent Lamden, Doug Laney, Bob Leahy, Bill Leake, Mark Moore, Geoffrey Rutledge, Dorothy Segar, and Jon Toigo.*