Computer Security: Discussion On Security Issues And Security Countermeasures

Background

Computer security is the protection of computer and information systems from theft, unauthorized use, or damage to the hardware, software and information. How to keeping a computer secured has become commonplace for todays. The computers may contain many private data such as personal data, or company data that need to keep secure from any possible threats that may lead to security-related problems that may affect individuals or company daily activities.

One of the areas that make computer security is being threatened is natural disasters. A natural disaster can become a tricky and serious problem for computer security since the natural disaster is cannot be predicted or foreseen. A natural disaster normally can be defined as an event or phenomenon that happen when there are some geology issues happen in the particular area that cause the natural phenomenon that interrupt the normal daily life of human and computer system.

A natural disaster can come in many forms, there are tsunami, hurricanes, volcano eruption, earthquakes and more geologic processes. The natural disaster will affect the normal life function like working processes and will have an interruption in daily activities, also may have life endanger issues that depend on the level and severity of the natural disaster. The natural disaster phenomenon existed since the Earth was formed and happened when the geologic issues such as the Earth crust crushing or more that may cause the butterfly effect which lead to the natural disaster phenomenon. Natural disaster normally happen for example the floods. Floods are hydrological disasters that happen when there is an overflow of water that will cover up the land area for a temporary or a particular time. Other than that, there are tornadoes, which are a meteorological disaster that are caused by extreme weather, which is destructive and sudden to the environment. A tornado, or as known as a cyclone or a twister is a violet natural phenomenon that rotates the column of air that connect both earth surface with a cumulonimbus cloud that have has a high wind speed and will travel a few miles before it disappears. The tornado has different categories, and each category will cause different degrees of damage.

There are many natural disasters that may occur which may be a possible threat to the computer security, but according to a phrase, which is “prevention measures” that can be defined as prevention is always better than from foreseen. The natural disaster is a security issue that can be prevented from or reduced that damage caused by natural disaster when there is protection are being implemented or applied for.

Discussion on Security Issues

Natural disasters can be defined as any calamitous events caused by nature or natural processes on the Earth. Each natural disaster is measured by the lives lost, economic loss and the rebuild population ability. The calamitous events are not considered as a natural disaster

when it occurs in unpopulated area are not considered as a natural disaster. For example, an earthquake occurs in an uninhabited island will not considered as a natural disaster because it would not cause any live lost or damage. On the other hand, when the earthquake occurs in a populated area, it will be considered as a natural disaster. All the natural disasters will cause losses in some ways such as live lost or damage to data in the computer systems. The natural disaster can be divided to a few of major categories, which are geological disaster, hydrological disaster and meteorological disaster

Geological disaster occurs when the natural geological processes are affected people's daily activities. Earthquake, landslides and avalanches are the common one in the geological disaster. The earthquake is known to be caused the rock's relative motion within the earth's crust or due to the collisions of tectonic plate. The waves spread out when the earthquake is happened, and when the waves are arrived at the surface of the earth, it will shake violently near the earthquake's source but softly at a distant point. There is no any forewarning when the earthquake strikes and cause huge damage to the building, roads and bridges, and may take hundreds or thousands of lives. Besides that, the landslide can be defined as a down-slope movement of rocks, debris or soil. A landslide is a form of mass-wasting, which means the down-slope movement of rocks or soil is occurred under the trigger or direct influence of gravity. The impact of landslide can be extensive, it can be included lives lost, damage to the land or road, destruction of infrastructure, and loss of natural resources such as forest. The landslide can increase the risk of flood because it may block the rivers when the landslide materials flow into the rivers. Other than that, the avalanche is similar to landslides in the down-slope movement. The down-slope movement of a mass of snow that are slide down rapidly is called as an avalanche. The avalanche can be triggered by some nature forces such as rapid temperature changes and precipitation, or due to human activities for example, the avalanche may occur when a sudden addition of human weight on a weak area of snow and cause the weak area become fractured. Most of the avalanches are occurred in the backcountry, for example it may occur outside the developed ski areas. The avalanche also has an impact on the human and environment such as it can block the path and restricting the traffic movement.

The second category of disaster is hydrological disaster. Hydrological disaster can be defined as a destructive change which are violet and sudden due to the quality of the water in Earth, or the distribution and movement of water on the land below the surface. The first example of hydrological disaster is floods. Flood is occurred when an overflow of water invades a dry place or populated areas because the flow rate of water exceeds the capability of the natural watercourses. The impacts of the flood are including lives lost, damage to property and loss of livestock. Besides that, the disruption to the infrastructure may cause long-term effects such as disruptions to communication, transport and electricity. The disruption to the business and company can make people feel continuing stress. One of the examples is 2011 Queensland floods. In 2011, Queensland floods showed that more than 50% of organizations experienced a modest, significant or critical impact on their business viability. Many organizations in Queensland have found that their server rooms have been affected by flooding, so they are unable to operate normally, even externally. Another example is on Christmas day 2015, severe flooding in Leeds, UK, temporarily knocked out Vodafone's data center. While the data loss was negligible, the outage temporarily disrupted mobile phone service. Vodafone, of course, has a history of flooding, including one of the most notorious data center disasters in 2009 when its data center in Istanbul was destroyed by flooding. The second example of a hydrological disaster is tsunami. A tsunami is a series of water waves caused by the displacement of huge amount of water in an ocean or large lake. It can be hundreds of kilometers long and it start

suddenly. The tsunami not only makes lives lost, and also has a catastrophic impact to animals, plants, insects and natural resources. The tsunami can cause environmental impact such as change the landscape. It destroys the animal habitats and also uproot the trees and plants.

The third category of disaster is a meteorological disaster. Meteorological disaster is the disaster caused by the extreme weather such as extreme hot and cold, rain, and wind. It does the violet, sudden destructive to the environment and affect the atmosphere. Hurricane is one types of meteorological disaster. Hurricanes also known as cyclones or typhoons, they are same phenomenon although the names are different. A hurricane is a large rotating storm with high speed and formed in tropical areas over the warm water. The sustained wind of hurricane has at least 74miles per hour and the low air pressure area at the center is called the eye. For the hurricane forms, it needs warm ocean water and humid air in that area. At a low-pressure zone, the moist air is flowing upward over warm ocean water, the storm clouds are created as the water is released from the air. The hurricane can bring a lot of rains, and it may rain continuously. This will cause flood and brings another destructive impact. The first example is Hurricane Sandy. In 2012, Hurricane Sandy caused widespread damage in New York: several data centers in lower Manhattan were knocked out, basements and power generators flooded, and switchboards were restored to normal after being damaged. Causing nearly $70 billion (2012 dollars) in damage, it was the second-costliest hurricane on record in the United States until it was overtaken by hurricanes Harvey and Maria in 2017. In 2016, the river Aire in Leeds, England, burst its Banks and flooded a Vodafone facility, paralyzing it for several days. Another example is Hurricane Harvey. For instance, the news of “Houston data centers withstand Hurricane Harvey”. Edward Henigin, Austin data foundry's chief technology officer, said their north Houston data center was 'built specifically to withstand the winds of a category 5 hurricane.' Just before the hurricane Harvey, the company beefed up its staff to maintain data centers throughout the emergency and provided food, showers, beds, books and video games for five-day employees. Major data center providers in Houston reported no outages during the emergency. That's impressive. Hurricane Harvey destroyed 203,000 homes and cost at least $125 billion in damages. Besides that, another disaster example is tornado. A tornado is a violently rotating column of air that connecting and touching between the cloud and the surface of Earth. Tornado comes with many shapes and sizes, but usually in the form of funnel. The tornado affects the environment by destroying the building and forest. It also affects the food chain due to kill the animals. Besides that, the tornado caused the food shortage at the surrounding area due to destroying the farms. For example, in 2011, a devastating tornado hit several hospitals in Joplin, Missouri, including a data center. While none of the missing data is mission-critical, this is only because most of the information stored there was migrated to a new offline data center a few weeks ago. Hospital officials point out that if the tornado had come a month earlier, the loss of data would have been catastrophic and the hospital would have been completely disabled.

Among the potential security threats and issues, computers become more and more a part of everyday life, more and more important data is stored in home and office databases and file systems. In the past, computers were mainly used to store personal data and documents. Now more and more computers are used to store sensitive data, such as patient information, financial records and transaction history. To secure the data, companies take various steps, including copying and backing up, to ensure that their data is secure. They will also spend time ensuring that data is protected from malicious users and attackers by assigning permissions, installing and updating antivirus software, and installing firewalls. But despite all these precautions, what happens when data is lost? Catastrophic data loss is relatively rare, mainly

because data replication is relatively cheap. Because multi-terabyte hard drives cost less than a business lunch, most companies keep backups of important data on at least two or three computers. As a result, catastrophic data losses are often caused by natural disasters such as earthquakes, hurricanes, floods, and fires. Hurricanes cause catastrophic data losses through the physical damage caused by power surges, high winds, and flooding. For example, about 10% of data or application outages are directly caused by natural disasters such as fire or flood, and another 40% are caused by power losses. So, in Australia, we can estimate that about $5 billion a year is lost as a direct result of natural disasters. According to the industry data, IT outages can cost an enterprise $5,000 to $10,000 per minute in lost revenue and/or lost productivity. Losses can run into the millions of dollars in highly sensitive industries such as high-frequency trading, online retail/e-commerce. While this is a financial cost, it can also impose non-financial costs on the business, such as loss of customer reputation, loss of employee productivity and loss of morale. Power surges can damage fragile computer hardware and cause hard drive electronics to stop working. If a building collapses or a branch falls off the roof of your data center, and flooding is bad news for any electronic device, the hard drive could suffer physical damage. Earthquakes can also cause severe physical damage to hard drives, resulting in severe data loss. Not only can a fire cause heat damage to the hard drive, it can also cause dust and smoke particles to flow between the disk reader and the disk. The space between the read and write head and the disk is so small that almost anything can get into the disk and begin to damage the disk surface.

Discussion on Security Countermeasures

The threat of natural disasters lingers in the minds of data center providers around the world. Managing the power, cooling, and security needs of data centers is difficult enough even before considering threats like hurricanes, earthquakes, or floods. Maintaining data access in the event of a disaster can mean success or failure for the company. Therefore, every data center must have a comprehensive plan to protect data in the event of a natural disaster. While every effort should be made to maintain uptime for servers, data centers must consider the possibility that, in the event of a disaster, they fail to deliver on their promises. After all, even the most robust SLA doesn't make much sense if the power fails and no one has physical access to the data center to get critical systems running again. The first step in any data center's response to a disaster is a comprehensive risk assessment. This review will determine the likelihood and expected consequences of potential disasters. Once these risks have been identified, the provider needs to create a step-by-step list detailing what actions to take in the event of each particular disaster. All concerned should be familiar with these plans and conduct regular exercises to ensure that everyone knows what to do in a disaster situation. In addition to saving customer data, keeping the network up and running is an important consideration. Every moment of downtime comes with a real financial cost. Any good data center should already include a lot of network redundancy in its computing infrastructure, but these backup plans need to be more reliable in the event of a disaster. Regular testing is critical to ensuring that customer data and critical operations remain online and secure in the event of power outages and system failures. In addition, all relevant personnel must be trained in what to do if redundant systems do not work as designed. This usually involves critical manual interventions, where personnel must be trained in a 'manual' environment to gain experience and understand the process and system response to manual transfers.

Data centers also need to consider how disasters will affect the infrastructure around them.

When hurricane Sandy hit New York City, for example, many backup generators failed because they ran out of fuel and couldn't refuel because the city streets were flooded. Since physical access to a data center may be limited and remote access may be impossible, it is critical to install automated backup systems in place to ensure that mission-critical data and services for customers are not lost or interrupted in the event of power outages. If you want to back up data in another data center, that facility should be far from the center affected by a natural disaster. Datacenter providers across a wide geographic area can better ensure that large natural disasters do not overwhelm all their services. As natural disasters like hurricanes and wildfires become more frequent, data centers must take aggressive steps to protect their facilities, and thus their customers. While cloud services make it easier to back up basic assets, and modern build techniques can better protect devices from physical hazards, data centers still rely on factors beyond their control to keep them up and running. Only by being prepared to deal with disruptions in their daily operations can they be truly prepared for any disaster that nature throws at them. For companies physically located on the fault line, architects and contractors build earthquake-proof structures into the structure. Commercial sites in these areas, especially those used as data centers, are ideally located on bedrock, with seismic isolation systems and adequate wall structures. Data centers must have adequate cooling water and fuel reserves in case of a major earthquake. While bedrock stabilizes during earthquakes, it is of little use during fires or floods. In cases where evacuation may be required, your disaster plan should include options for data security transmission. This can't just be a copy of the data sent to the hard drive. At the very least, there must be a way to transfer basic data on a hard disk. It is also important to decide in advance where a company will operate during and after a disaster. Your company must have procedures in place to deal with power dips and blackouts. Power outages can occur due to storms, heatwaves, rodents and a variety of accidents, which is a serious data security issue and a threat to equipment. In 2017, there were 3,526 power outages in all 50 states, with an average outage of 81 minutes, affecting more than 26 million people. Uninterruptible power systems (UPS), power-regulating software, and generators can help maintain a continuous power supply. Review past power outages and coordinate with power companies to avoid or minimize future impacts.

In my opinion, to reduce the natural disaster from damaging the computer security is used high-quality equipment of computer’s hardware. Most of the computer’s hardware are fragile and not waterproof, but with nowadays the technology many computer’s hardware are waterproof and not easily broken. So, use high-quality equipment might be a good selection for user. Next, I will always store the important data into another hard disk for backup. I also will check the weather forecast to know the recent situation. If there will be natural disaster coming, I will bring my hard disk with me to take refuge.