2016

Up in the Cloud

Yulina Park

Yulina Park
Honors Program
Business 204
28 April 2016

Up in the Cloud

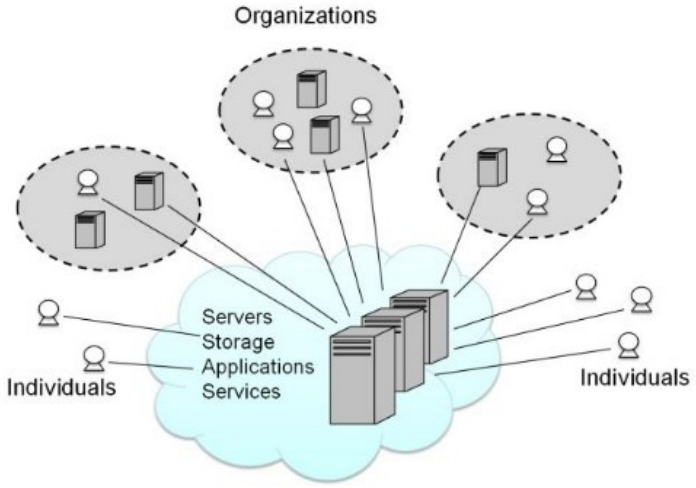
Electric cars. Smart watches. Nanoparticles. What do all of these have in common? They're all advancements in technology. Today, Americans couldn't even imagine living their everyday lives without the convenience and efficiency of technology; how would they commute without automobiles, how would businesses easily attract customers without the internet, and so on. In addition to the high demand for current technology, there are also high demands for new, better, and more efficient technology. Companies, like Apple, have to keep up with these demands in order to stay competitive and attract new and current customers. As a result, Apple introduced the new iCloud back in 2011 to hype up its customers and continually improved the iCloud to what it is today in 2016. Unfortunately, the iCloud and about 50% of small businesses (McCamy) has attracted the attention of new, better, and efficient hackers.

When Apple first announced the iCloud, it claimed it was different and better than all the other cloud computing technology since the iCloud stores the data to the end-users device, such as personal computer, smartphone, instead of storing the data from the end-user device to the Internet, like most cloud services (Ray). Furthermore, since Apple products were already popular, the iCloud will be an additional free service for current users (Ray). Apple also claimed the iCloud was perfect for businesses since the iCloud is able to synchronize all data, such as documents, emails, meetings, and make it accessible by all employees, even absent employees, to keep the business running smoothly (Ray).

Everyone was so excited about Apple's new iCloud that problems associated with the new iCloud was swept under the rug. In fact, in 2014, the unmentioned problems of the iCloud became a reality when several celebrities were hacked through their Apple iCloud and their private photos were leaked (Kovach). Although Apple denied that the whole iCloud system was not breached, it left the

question, “how did the hackers target only certain iCloud accounts,” unanswered (Kovach). It was made painfully obvious that the security of the iCloud was not as safe as some people thought and put users of the iCloud, including businesses, at risk.

Apple’s iCloud is part of a technology called cloud computing, but what exactly is cloud computing? Cloud computing is the latest technology in the field of computing where data and information are pooled into one place and can be accessed anywhere by anyone (Harding). This basic concept of cloud computing can be illustrated with this model (Harding):



A common network connects servers, hard drives, and applications to collect and save all data into one common place so that users, customers, remote users, and organizations can access any of the information stored in that common place through the Internet, Intranet, or private networks (Harding). One could say that the Cloud is very similar to a shared document on Google Docs, where anyone who has access to the document can modify it, regardless of their location, as long as they have Internet access, but, of course, the cloud is on a much larger scale.

So what makes the Cloud so great for businesses? There are several reasons for a business or organization to integrate the Cloud into their system, but the most important reasons are increased agility, performance, and cost efficiency (Harding). When we talk about increased agility for businesses, we mean the on-demand services cloud computing offers and the ability to quickly enter new markets

and adapt to changing demands in the current market (Harding). For example, businesses would be able to post new advertising ideas and everyone would have access to them in an instant and, likewise, old ideas can be taken down in an instant. Another reason for the increased agility is that the cloud keeps everything simple (Westervelt). It removes the complex IT infrastructure that only highly skilled and trained IT employees are able to navigate through (Westervelt). Furthermore, cloud computing services would provide their own IT specialists so businesses would not even have to worry much about having their own IT department (Westervelt).

Better performance from managers and employees are also evident from businesses that switched to the cloud (Harding). As mentioned before, cloud computing enables users to access any data, including emails, meetings, documents, etc. that is stored in a collective place. Because of this feature, employees are able to better perform by increasing productivity since collaborating ideas and viewing work progress with other coworkers anywhere and anytime have become extremely easy (Harding). Efficiency can also be grouped with better performance. Cloud computing is a measured service, meaning, cloud computing services charge per-usage basis (Harding). This also means that cloud computing services must be able to measure how much is being used by measuring the amount of data stored, volume of network data transfers, IP addresses, and virtual servers (Harding). Having these measurements and numbers of usage information will allow managers to evaluate how well the IT sector is operating and to effectively and efficiently plan the distribution of resources (Harding).

Maybe one of the more obvious reasons for businesses to make the switch to the cloud is cost efficiency (Harding). In fact, some businesses claim to have cut their operating costs by 50%, even up to 75% (Dimensions). Cloud computing reduces costs by using usage-based pricing and reduced operational services and support (Dimensions). Cloud computing services bill their clients by the amount the clients use their services. Often times, businesses run into temporary work, like software testing and development, quality testing, seasonal websites, and large data analysis, which all require IT

services (Dimensions). IT workers will need time to gather the needed equipment, install it into the data center, and reconfigure the codes to fit the client's needs (Dimensions). This process could last from a few days to a few months (Dimensions) and IT workers are expected to be paid throughout that entire time frame and the businesses will also have to buy the hardware, power, and space for the temporary project. Businesses that use cloud computing, however, does not have to pay for the IT services, equipment, and space. Instead, these businesses only pay for the resources they used (Dimensions). For instance, a business may need ten servers to be able to test and develop their new product. Instead of buying IT services to do the job for them and bringing, installing, and configuring the ten servers that could take months, the business can buy ten cloud computing servers for, let's say two months, and simply pay for using the cloud servers rather than also paying for the installment and configuration of the cloud servers (Dimensions). Therefore, companies and businesses can save money by paying only for what they're going to use for the exact amount of time and not need to pay for IT operations services and support for the hardware.

Unfortunately, technology is not perfect. There are concerns and problems associated with cloud computing, which have drawn the attention of hackers and users. The main concern with cloud computing is cyber security and privacy, which is often an issue with many technology. Almost all cloud computing services have the option of automatically syncing data, which is very convenient and means all of your data will be automatically backed up. However, this allows hackers to break into cloud accounts, even without a password (Kraynak). This type of cyberattack is called Man-in-the-Cloud (Kraynak). Man-in-the-Cloud, or MITC, is just like identity fraud, except the hacker doesn't need any of your credentials, instead, the hackers needs security tokens, which are small files on a user's device that contains authentication codes (Kraynak). Usually, the user would have to input their authentication, like a username and password, however, automatic data sync allows authentication input to also be automatic when the device is turned on, which means the user does not need to type in the username

or password (Kraynak). The authentication code is stored and encrypted into a security token, but because it's automatic, hackers can steal these security tokens with ease and insert them into their own devices, giving them access to the original user's cloud account and all the data stored in their cloud (Kraynak). Once a user's security token has been stolen, there is no notification or alarm that detects the removal and unfortunately, the removable of a token makes the account unrecoverable (Kraynak). This means a new account must be made and all the data that was stored on the original account will be lost (Kraynak).

Another feature of cloud computing that backfired for many businesses is that *all* their data, from a client's bank account information to last week's meeting presentation, is stored in one convenient place (Palmer). It's convenient for businesses and it's convenient for hackers. When hackers do their job and complete a cyberattack, they must do so as quickly as possible before somebody notices, so hackers look for a target that will give them the most for their resources and time (Palmer). It's like a robber choosing to rob a bank that has $500,000 versus a bank that has only $500. Therefore, when a hacker sees an opportunity to infiltrate a business's cloud, it's very much like winning the lottery with almost no luck needed.

Hackers also target the cloud because more and more companies have made the switch to cloud computing (Palmer), meaning there are more "lotteries" to be won. However, because all cloud computing services are generally the same, the installation, security, and infrastructure of all clouds are also generally the same (Palmer). This makes it even easier for hackers to get into the cloud because the holes in security and application of the cloud is standardized across all cloud computing services (Palmer). Essentially, a security flaw in Verizon's cloud will be similar to a security flaw in Microsoft's OneDrive.

Many hackers will hack into a device, steal the valuable data, and leave, but there has been an increasing number of cases where hackers will steal the data, encrypt it, and ask for a ransom, or

money, in return for the data (Shanhani). This is what happened about 500,000 other businesses and also to Eric Young, who works for a small business in Tennessee (Shanhani). Young stated that the hack came in a form of a hyperlink that looked like PayPal and stated, "Somebody paid you money." When the link was clicked, the webpage turned into a threat that stated to pay the unknown hacker or else all the files in the company's network will be locked up so tightly that no one can ever open it again (Shanhani). The hacker gave Young's company 72 hours to pay the ransom while the hacker started to infiltrate every computer connected to the company's server; the company was about to lose everything they have built for the last 14 years (Shanhani). These types of situations are called ransomwares which uses an anonymous online network so all communication between the hacker and its victim is hidden (Shanhani). Unfortunately, ransomware has advanced while the solution to ransomware has not. When a hacker gets ahold of your data and encrypts, there is no way to recover the data, except by giving in to the hacker (Shanhani). Young's business decided not to pay the ransom because they did not trust the hacker to return the stolen data and concluded that no one could solve the problem (Shanhani). The business lost the majority of their files but did have a number of files backed-up, which were not stored in the cloud (Shanhani).

The hacker that infiltrated Apple's iCloud accounts made his big reveal of exactly how he did it (Kumar). He used a botnet which was named iDict to bypass the iCloud's security system and the authentication security that was supposed to prevent "brute force attacks," like iDict (Kumar). The hackers says the botnet is "100% effective" and frighteningly simple (Kumar). iDict contains a file of 500-word-long lists of passwords, therefore, if an iCloud user has an easy or simple password, their account is at high risk of being hacked (Kumar). However, the hacker stated that his intentions were not to humiliate the celebrities by leaking their photos in their iCloud accounts but to make it obvious to Apple that something must be done to fix major problems with iCloud security (Kumar). Therefore, the damages done to Apple and its customers were not significant.

Fortunately, there are laws concerning hackers, cyberattacks, and cyber securities. Hacking falls under the broad category of cybercrimes, which are any crimes done through the computer and over the Internet community (Miller). Of course, since it's a type of crime, there must be laws to punish those who commit these crimes. Congress came up with the Counterfeit Access Device and Computer Fraud and Abuse Act, or CFAA, to address these crimes (Miller). The CFAA basically states that any person who accesses a computer with the intention of obtaining classified, restricted, or protected data is liable for criminal prosecution (Miller). Types of data could include, financial records, medical records, legal documents, and government files (Miller). The cybercrime is treated as though the criminal physically committed theft and can be convicted as a felony, if the stolen data was valued over $5,000 and be sentenced up to 20 years of imprisonment (Miller).

However, unlike thefts that are done physically, it may not always be obvious who the criminal is in a cybercrime (Schneier). When someone robs a bank, the criminal can be physically seen and even by described as short, tall, male, female, etc. When someone steals data over the Internet, the criminal cannot be physically seen or described; their whole identity is hidden. That brings the question of "how are we supposed to enforce the laws and punishments if we don't even know who committed the crimes?" There are ways to trace the crime back to the hacker or criminal, however, this requires intensive knowledge of technology and computers and many hackers have advanced their techniques enough to make it nearly impossible to uncover their digital tracks (Schneier). Otherwise, finding the one responsible for the cybercrime is a tedious process and takes a lot of time, especially since hackers are able to reroute their tracks through third parties (Schneier).

Another issue comes up when the criminal behind the crime is unknown because there are no boundaries over the Internet. When a business or person becomes a victim to a cyberattack, they don't know if the attacker is a bored genius living in Nebraska or a group of hackers in Germany. Anyone in the world who has access to the Internet could be the culprit (Schneier). Which means, the identified

hacker, or cybercriminal, could thousands of miles away in another continent. How is the crime approached then? Would the state government take care of the convictions or the U.S government? What if the attack came from a group of cyberterrorist? Would the U.S military have to be involved then or the FBI (Schneier). A clear line cannot be drawn when it comes to convicting cybercrimes as they can for physical theft and other physical crimes. Of course, gathering evidence may lead to who did the crime and clear a few things up on who should do the convicting (Schneier). But as mentioned before, finding the culprit requires a lot of time and work.

The main ways of finding the source of the cyberattack is through circumstantial evidence and digital fingerprinting (Greenemeier). Often times, the culprit of the cybercrime can be narrowed down by examining the malware and botnets used, the techniques used, and what type of data was stolen (Greenemeier). Cyber forensic investigators can learn a lot from examining and analyzing the computer that was hacked into and what type of malware was used as the "weapon," such as the code that was used, how the code was written, and how it was communicated back to the hacker (Greenemeier). A unique malware code means the culprit is most likely a very skilled programmer with advanced equipment while a common malware code can be traced to several programmers (Greenemeier). Also, the type of data stolen is a big clue. For instance, if a small business's data was stolen and held for ransom, the cybercriminal is probably a young hacker trying to make some money whereas if government files were stolen, the hacker was probably part of an anti-government group. Forensic investigators also use digital fingerprinting, which is a marker for a certain format style for a program, such as how the program distributes data memory and how it avoids security detection, (Greenemeier). Although these methods usually don't lead to exactly who was behind the attack, it gives investigators significant clues, In fact, over the years, they have found that a more unique, complex, and efficient code for stealing data can be easily traced to the programs (Greenemeier).

When a business gets hacked and its data is stolen, the hacker is not the only one held responsible for the cyberattack (Vijayan). A federal court in New Jersey ruled that businesses that were hacked can also be held responsible because they have failed to take the steps to increase security (Vijayan), which is a great reason a business should take the extra steps to increase security of their cloud. Wyndham Worldwide Corporation experienced a cyberattack where thousands upon thousands of client's debit and credit card information were revealed (Vijayan). The data breach resulted in about $10.6 million in theft and fraud losses (Vijayan). Wyndham was accused that it had "deceived" its customers into thinking that their card information was protected, however, the corporation denied such accusations and stated that the Federal Trade Commission did not have the authority to blame the company for data breaches and regulate data security (Vijayan). Wyndham Worldwide Corp lost the lawsuit and was liable for the losses (Vijayan).

Businesses that are hacked sometimes try to defend themselves by blaming others, which may or may not work; it all depends on the situation (Narisi). For example, Choice Escrow and Land Title, a company in Missouri, experienced a data breach where the hacker stole the clients' bank ID's and passwords (Narisi). The company sued BancorpSouth, a bank where the clients' accounts were held, and stated that the bank should have offered more security (Narisi). The court, however, did not find the bank responsible because it found that the bank did have enough protection and even offered additional security if the client wanted to do so (Narisi). On the other hand, a different bank was held responsible for a cyberattack, which resulted in the theft of its clients' money, because the bank did not offer a sufficient amount of security protection, such as multi-factor authentication (Narisi).

To make matters worse, not only the court, but your own clients could sue your business in a cyberattack, especially if the damages were significant (TechInsurance). There are two main ways a business can be sued in a cyberattack or data breach; first-party liability and third-party liability (TechInsurance). A first-party liability is when a business or company stores private data or clients'

information directly into their network, therefore, in a cyberattack, the business is responsible for taking necessary steps to offer sufficient security protection (TechInsurance). In a third-party liability, the private data is stored on the client's computer or device but a business offers the service and IT management, such as cloud computing or mobile apps (TechInsurance). If a client's cloud gets hacked, they can sue the business providing the cloud computing service because there was a security flaw in the business's software (TechInsurance). When the damages are significant and cause suffering to the victims, the clients suing will most likely win the case (Narisi). However, the court's judge will take the definition of "suffering" to the dictionary. For example, a group of Aetna employees tried to sue their company because Aetna was hacked and revealed their Social Security numbers, phone numbers, home addresses, and work history (Narisi). The case was denied because the judge ruled that the employees did not actual "suffer" but only became more prone to identity theft (Narisi). If the Aetna employees proved that they actually experienced financial losses, it would be a different story, as many customers did in the Hannaford Bros. case (Narisi). Hannaford Bros. is a grocery chain and lost over 4 million customers' credit card information when a hacker infiltrated their network (Narisi). Its customers suffered from many financial losses, even though some of them paid for increased security protection, such as credit monitory services or identity theft insurance (Narisi).

However, a business should not wait until they have been hacked and leave it up to the computer forensic investigators and laws to figure out the mess. Business can take steps and precautions by using security and monitoring software to greatly reduce the risk of getting their cloud hacked (Kraynak). For example, Cloud Access Security Broker, or CASB, is a service used to monitor the cloud service and alert the business if there is any unusual activities within the cloud (Kraynak). Businesses should also use Database Activity Monitoring and File Activity Monitoring, or DAM and FAM, to monitor activities happening outside the cloud and alert them is someone is trying to forcefully

access their data (Kranyak). Knowing when something is wrong right away will enable you to fix and prevent the problem before it gets out of hand.

Another way to increase the security of your cloud is by encrypting the data that is stored in the cloud (Windows). This way, if a hacker does get ahold of your business's data and documents, he or she will not be able to read and place value on the data to threaten the business for ransom. Cloudfogger is a free service by Windows that provides another layer of protection for your cloud files by automatically encrypting online and offline data when it's uploaded and saved in the cloud (Windows).

We are always excited about new technology and advances in technology. However, this also brings in new and advanced risks. Cloud computing is a new technology that has become a huge hit for businesses because of its many advantages, including increased productivity and cost efficiency, but it has also become a huge target for hackers and cyberattacks. There are laws and punishments to deter cybercrimes but they are not always effective. Therefore, the first line of defense is the business and taking these few extra security steps can greatly reduce the risks of becoming a victim to cloud hacking.

Works Cited

Dimensions Data. "Cost." *Reducing Infrastructure S with Cloud Computing*. Dimensions Data, 2016. Web. 24 Apr. 2016.

Greenemeier, Larry. "Cyber-Attack Scene Investigation." *Scientific American*. Nature American, Inc., Jan. 2016. Web. 24 Apr. 2016.

Harding, Chris. "Cloud Computing for Business." *Cloud Computing for Business : What Is Cloud?* The Open Group, Aug. 2011. Web. 24 Apr. 2016.

Kovach, Steve. "We Still Don't Have Assurance From Apple That ICloud Is Safe." *Business Insider*. Business Insider, Inc, 02 Sept. 2014. Web. 24 Apr. 2016.

Kraynak, Mark. "A New Cloud Threat for 2015: The Man in the Cloud Attack." *Imperva Skyfence*. Imperva, Inc., 20 Aug. 2015. Web. 24 Apr. 2016.

Kumar, Mohit. "Hacker Released 'iDict' Tool That Can Hack Your ICloud Account." *The Hacker News*. The Hacker News, Jan. 2015. Web. 24 Apr. 2016.

Miller, Roger LeRoy., and Frank B. Cross. *The Legal Environment Today*. Australia: Cengage Learning, 2009. Print.

Narisi, Sam. "When Can Data Breaches Get Companies Sued?" *IT Manager Daily*. Catalyst Media Network, 03 Apr. 2013. Web. 26 Apr. 2016.

Palmer, Danny. "Why Are Hackers Increasingly Targeting Cloud?". Incisive Business Media, 14 Oct. 2015. Web. 24 Apr. 2016.

Ray, Ramon. "ICloud: A Special Cloud for Apple Devices." *Business Insider*. Business Insider, Inc, 05 Oct. 2011. Web. 24 Apr. 2016.

Schneier, Bruce. "Hacker or Spy? In Today's Cyberattacks, Finding the Culprit Is a Troubling Puzzle." *The Christian Science Monitor*. The Christian Science Monitor, 04 Mar. 2015. Web. 24 Apr. 2016.

Shahani, Aarti. "Ransomware: When Hackers Lock Your Files, To Pay Or Not To Pay?" *NPR*. NPR, Dec. 2014. Web. 24 Apr. 2016.

TechInsurance. "Insurance and Technology: Protect Your Business from Security Lawsuits." *Techinsurance*. BIN Insurance Holdings, Jan. 2014. Web. 26 Apr. 2016.

Vijayan, Jaikumar. "FTC Can Sue Companies Hit with Data Breache." *Computerworld*. Computerworld Inc., 10 Apr. 2014. Web. 26 Apr. 2016.

Westervelt, Robert. "10 Ways Cloud Services Improve Security, Reduce Complexity." *CRN*. The Channel Company, Oct. 2014. Web. 24 Apr. 2016.

Windows. "Cloudfogger Review: Security for Your Cloud Storage Accounts." *The Windows Club*. The Windows Club, 10 Apr. 2013. Web. 24 Apr. 2016.