Learning Team B: Final Paper  
Bachmeier, Sciulli, Sims  
CMGT 445: Risk Management  
University of Phoenix  
August 11th, 2014

# McBride Risk Assessment

The senior leadership team of McBride Financial Services have determined that an assessment of risk to their organization is needed. They are concerned about several aspects of the business including but not limited to-- toxic chemicals and environmental concerns; public transportation; targeting by criminal activities and terrorism.

# Toxic Chemical and Environmental Risks

McBride Financial Services will be the preeminent provider of low-cost mortgage services using state-of-the-art technology in the five state areas of Idaho, Montana, Wyoming, North Dakota, and South Dakota. The customers will receive the most efficient and effective processing of mortgage applications from inception to closing. McBride Financial Service Company has a location in Sioux Falls, South Dakota market. However, McBride Financial Services has a potential risk at hand. A nearby printing press, Sisson Printing, which is approximately four blocks from the location, represents the risk of hazardous chemicals release.

According to the Environmental Protection Agency (EPA), "When hazardous wastes are released in the air, water, or on the land they can spread, contaminating even more of the environment and posing greater threats to our health. (Health Effects from Chemcial Exposure, 2014)" Public transportation facilities that might handle the carriage of dangerous or hazardous substances or which could be involved in major accidents holds a risk to people in the neighbor, people who own businesses, and the customers of those businesses. At public transportation facilities, there are always spilled spots of chemicals in the production and loading/unloading area. If those spills are not cleaned up, the chemicals will start to merge into the air that everyone breathes. All building in the world has a drain pipe somewhere. It is a risk that some of the hazardous chemicals can leak into a drain pipe o the main water source could be bad. While transporting chemicals, there is always the risk of leakage onto the road or in a drain pipe that leads to a lake or the ocean.

These situations will affect the employees and customers of McBride Financial Services. If the location is next to public transportation facility, the employees or customers of McBride can inhale those dangerous chemicals. If the chemicals get into the water system, it could affect the drinking water or shower water of employees and other people in the neighborhood. Other ways people can be affected by hazardous chemicals are from the soil, dust, or food. A lot of people does not think about the dangers of inhaling dust. Inhaling dust can affect the lungs and cause breathing problems.

According to the Environmental Protection Agency (EPA), "Chemicals affect our everyday lives. They are used to produce almost everything we use, from paper and plastics to medicines and food to gasoline, steel, and electronic equipment. More than 70,000 chemicals are regularly used around the world. (Hazardous Substances and Hazardous Waste, 2011)" More than half of those products are in use at McBride Financial Services. Paper is in use for supplies and signed documents. Plastic bottles are in the vending machines for the employees and bottle of water for the customers who sign with McBride. There is a large amount of electric equipment in use at the office. Some equipment in use is computers, printers, and copying machine.

According to the Missouri Department of Health and Senior Services, "Therefore, the state and federal governments have determined health-based comparison values for contaminants that when exceeded, exposure may result in excessive health risk. The chart below contains levels used by agencies to determine if doses of chemicals may be harmful to human health."

|  |  |  |  |
| --- | --- | --- | --- |
| **Government Agency Who Established the Level** | **Name** | **Type of Limit** | **Description** |
| EPA | Maximum Contaminant Levels ([**MCL**](http://www.epa.gov/safewater/mcl.html)s) | Legally Enforceable Limits | The highest level of a contaminant that is allowed in public drinking water. These are federally enforceable standards. |
| EPA | Maximum Contaminant Level Goals ([**MCLG**](http://www.epa.gov/safewater/mcl.html)s) | Advisory Levels | The level of a contaminant in drinking water below which there is no known or expected risk to health. MCLGs allow for a margin of safety and are non-enforceable public health goals. |
| EPA | National Ambient Air Quality Standards ([**NAAQS**](http://www.epa.gov/air/criteria.html)) | Legally Enforceable Limits | Standards for maximum levels of contaminants for ambient air. |
| ATSDR | Minimal Risk Levels ([**MRL**](http://www.atsdr.cdc.gov/mrls/index.html)s) | Advisory Levels | Used to evaluate short and long-term exposure to a variety of chemicals. |
| MDNR | Missouri Risk-Based Corrective Action Guidance ([**MRBCA**](http://www.dnr.mo.gov/env/hwp/mrbca/mrbca.htm)) DRAFT | DRAFT Legally Enforceable Limits | Health-based screening values for contaminants in soil and water. This document is being developed and is in draft form. |

# Handling Sensitive or Hazardous Materials

Not only is it important that McBride handle toxic chemicals in a method that will comply with governmental policy, it is also important that their employees are safe along the way. For example improper handling of hazardous materials can result in injury or death, which will impede the organization’s progress.

## Risk of Sensitive Materials

Employees will periodically come in contact with sensitive materials, such as customer credit card numbers or other personally identifiable information (PII). When they do it is important for them to have had the proper training to ensure they do disclose this information either intentionally or accidentally.

A scenario where the employee may accidentally disclose the information is by having it on a personal laptop, which is then lost. This was the case at a Boston based hospital, which resulted in $1.5 million in fines for violating the HIPPA act (Security Magazine, 2012).

This incident could have been mitigated through proper security training of the employees. For example if the files had been on an encrypted drive the data would have been safe. If the files had remained on a corporate controlled server and only remotely accessed, it would have been even safer. The organization could have deployed Digital Rights Management (DRM), to further protect the information after it left their network.

## Risk of Hazardous Materials

In most corporate offices the employee’s exposure to hazardous chemicals is fairly minimal. They may still be present in printing chemicals or in cleaning products found in janitor’s closets. No matter where they originate it is critical that they do not contaminate the workplace. For example due to oversight water filled with bleach might be left out which later results in chemical burns.

To mitigate these risks it is useful to always have chemicals stored in dedicated containers that clearly specify what is the risks of contact are. Unfortunately not all accidents can be prevented, which is why the organization also needs a poison control response plan. The response plan needs to identify who should be contacted and how the incident should be handled. For example the local poison control or medical center contact information should be clearly displayed. The plan should also specify steps to clean up the area after the problem has been discovered. Depending on the substance the building may need to be evacuated.

## Proper Disposable of Materials

If the substance is sensitive in nature or hazardous to one’s health, then it is also important to consider the disposable procedure of the material. Different materials will need different disposal procedures.

In the case of the sensitive document it may be sufficient to run it through paper shredder. While an electronic document may need the hard drive to be wiped with random data for multiple passes before being sent for demagnetization (Whitney, 2009).

Hazardous material cannot be thrown in the dumpster or poured down the drain, instead it must be recycled through a licensed facility. Identifying these facilities during the procurement stage will reduce risk and stream line the process of removing the material.

# Target of Criminal Activity

McBride Financial is a mortgage company that provides mortgage at a fixed rate of $1500 dollars to all approved applicants, they are seeking our professionals and retirees who are purchasing primary and secondary properties or families and individuals that are purchasing recreational properties, but in order to be able to offer these services, it is necessary to calculate the organization risks and develop a plan to mitigate the risks. McBride Financial Services is a mortgage lender that provides loans for home purchasing and refinancing. McBride Financial Services' vision is to be the leading provider of low cost mortgage services.

Marketing plays a very important role in the success of any business. Any successful business goals are to reach out and win new customers. They must also be able to keep customers happy and satisfied with superior service for their hard-earned dollar. In order to achieve this goal McBride Financial must have good sound methods for reaching out and gaining new customers. Their marketing must be able to attract qualified customers through different venues. McBride Financial must first determine who their target market is and how to reach them. According to their website these are your target market Professionals, purchasing a primary or secondary residence, Retirees purchasing a primary or secondary residence, and family or individuals purchasing recreational properties

When applying and receiving a loan from a loan provider with any financial company is often a difficult and complex process. There many documents to complete and the authorization process can be time consuming and stressful. With the increase in Internet activity, to alleviate this situation McBride Financial Services has implemented a loan application process that can complete online. This process will save the client time by allowing him/her to complete a loan application without having to visit the financial company. Resources and money can also be saved by adjusting the structure of how loans are finalized. The drawback to the online process of loan application is security issues. The objective of this paper is to discuss the present loan process of McBride Financial and to recommend method to improve their current structure. There were two ways McBride Financial offered the potential buyers of applying for loans; in-person and online. The online process was quicker since clients did not have to appear at the financial company to complete paperwork.

However one disadvantage to online applications process is that if an applicant has questions, it can only be answered when the loan application has been received by a loan officer or when they contacted by one of McBride’s offices staff or representative. Protection of sensitive information is a main concern for all companies. When accessing sensitive information can easily become a target risk, application fraud occurs when a thief can get access to this information. Identity thief can happen to anyone, information such as social numbers, date of birth, bank account numbers, bank account number and routing number can be obtained by criminals. Security risks will arise for any company that uses Internet to conduct business as is the case with McBride Financial.

Because McBride Financial does not have any type of monitoring equipment; Hackers and their complex plug-ins can finds ways into all sorts of sensitive material and potential customers are an easy target for identity theft. White collar crimes are usually carried out by organized criminals. Examples of white collar crimes that are likely to occur to McBride Financial Services Company are: tax fraud and false accounting; corruption and bribery; phishing; insurance fraud; embezzlement; credit card and checks fraud; and corporate identity fraud. As Bolan (2008) assert, money laundering is increasing among businesses. The proceeds of white collar crimes are usually laundered by financial institutions such as McBride. According to Ross and Sherman (2009), criminals use mortgages more often as a way for money laundering. For example, a criminal can obtain the spurious documentation that is used to prop up mortgage applications on a forged or fraudulent basis.

When awarding contracts as Bolan (2008) puts it, businesses such as McBride can be susceptible to money laundering, that is, when they advertise various assignments together with jobs for tender, those contracts will automatically underbid by bogus companies. Considering last year alone, 10 percent of businesses were victims of corporate identity theft, whereby, the target criminal uses web services and counterfeit products posing as official to steal a business brand or name. For instance, if a company moves its offices, the buildings are usually left behind with a build-up of financial material. This information can be used by a fraudster who will portray him/herself as legal business, which he/she uses to carry out money laundering or nefarious activities. Also if a fraudster accesses the documentation of the company, he/she can forge checks and/or bank drafts which he/she then uses to settle his own bills (Sherman, 2009).

Most organizations have been victim of phishing, that is, a fraudster attempts to acquire clients and/or customers personal detail through e-mail. For example, criminals use fishing to convince customers to disclose their clandestine information, like PIN numbers, credit card numbers, and account numbers. The gang then tries transferring money out of the account of the customer to offshore destinations (Ross, 2009).

According to International Narcotic Control Strategy Report (2009), suspicions of terrorist backing as well as revenue commissioners ought to be reported by those businesses that are regulated. For example, all white collar crimes ought to be reported by company auditors. That is, a corporate ought to report if he/she suspects that a customer or client is either amassing funds for a terrorist act or a terrorist group, or else, the corporate could be found culpable of the offence. As McBride (2007) puts it, business individuals are being arrested in circumstances where they deem themselves within the jurisdiction of the criminal law.

McBride Financial Services will report those transactions that look suspicious and that are associated to terrorist activity to Financial Crimes Enforcement Network, which will assist to ease the instantly transmittal of the information to law-enforcement. Also McBride may contact government offices, like the local FBI field office with regard to terrorist-associated transactions, which require an instantaneous attention of law enforcement (Sherman and Ross, 2009). Terrorist activity to a business is politically sensitive. For example, if a corporate accuses the software company sells software, which encourages credit-card fraud, it can be taken to court so as to seek legal action. Terrorist activity in financing can be group-based; activity based or country based (McBride, 2007).

# Target of Terrorist Activities

In addition to being the target of traditional criminal activities, organizations now need to be on the lookout for terrorism. When one thinks of a terrorist, they may think of Middle Eastern people of Muslim decent. However this narrow view does not encompass the full range of terrorist that may want to disrupt the normal business activities. The list must also include “governmental or military, protestors and activists, and even people that do it for the lulz (Olson, 2013, p. 23).”

## Risks of Physical Attack

Terrorist may try to physically compromise the building or a dependent secondary infrastructure. A secondary structure could include cell tower, power station, or water intake; to name a few. For example if an electric transformer was blown up it could cause a denial of service for many businesses and last for several days.

To mitigate these risks to the secondary infrastructure it is important to have backup and redundancy programs. For example if the transformer was blown up, the company could switch to diesel generators until the problem is resolved. Another solution might be to route the workload to other sites which have not been impacted (Marchewka, 2012). These alternative sites may be owned directly by McBride or leased on demand through a third party.

While secondary infrastructure is mitigated through fail over and redundancy, attacks to the primary infrastructure can be mitigated through on premise security (Hernandez, 2012). For example a terrorist might walk into the building and begin arbitrarily shooting employees.

To mitigate these risks checkpoints need to be in place to vet each person as they enter the premise. One solution might be to deploy armed security guards to monitor the entrances (Stallings & Brown, 2008). In addition the gates should require some form of identification, such a smart card or employee badge.

Having proactive solutions in place handles the first half of the problem, the second is handling the reactive state. Through proper training, the employees need to be taught how to act in a crisis, such as hiding below a desk or barricading a conference room, during the shooting.

## Attacks on the Network

The crazed gunman is a real scenario that needs to be thought of, though the more common terrorist attack will be through the network connection (Microsoft, 2013). Compromising a financial institution’s network is the modern equivalent of robbing a bank. Attackers can reroute funds, deface Internet facing endpoints, or collect classified information such as pending mergers and acquisitions.

To mitigate these risks proper network segmentation needs to be deployed, reducing the attack surface. For instance the front end web server should not have direct access to the backend top secret database. Instead there should be intermediate systems along the way that perform authentication, authorization and auditing.

A better solution would be to not allow never allow a less secure system to talk to a more secure and business critical machine (Hernandez, 2012). This can be achieved through IPSec policy and the use of Virtual Local Area Networks (VLAN) technologies (Goleniewski & Jarrett, 2007) (Morimoto, 2010).

# Conclusions

There are numerous vectors that can impact the McBride and cause them to lose business or potentially injure the employees. The list of attacks is ever changing and needs to be assessed on a regular cadence to make sure it properly reflects the current threat landscape.

During these evaluations it is important to look at the impact to the sustainability of the local environment and how chemicals and by products of the organization can negatively influence the area. Next a look at the risks to employee safety need to be discovered and mitigated.

After making sure the company is operating in a safe manner, the assessment needs to look at intentionally malicious attacks against the organization. These can come in general criminal activity or terrorism. Having these actors identified can make it easier to implement mitigations, such as proper training and response plans already defined.

# References

Goleniewski, L., & Jarrett, K. (2007). *Telecommunications Essentials. The Complete Global Source, Second Edition.* Pearson Education.

*Hazardous Substances and Hazardous Waste*. (2011, 8 11). Retrieved from United States Environmental Protection Agency: http://www.epa.gov/superfund/students/clas\_act/haz-ed/ff\_01.htm

*Health Effects from Chemcial Exposure*. (2014). Retrieved from Missiour Department of Health & Senior Services: http://health.mo.gov/living/environment/hazsubstancesites/healtheffects.php

Hernandez, S. (2012). *Official (ISC)² Guide to the CISSP CBK.*

Marchewka, J. (2012). *Information Technology Project Management. Providing Measurable Organizational Value, Fourth Edition.* John Wiley & Sons Inc.

Microsoft. (2013). *Security Intelligence Report Volumen 16.* Microsoft Corp.

Morimoto, R. (2010). *Windows Server 2008 R2 Unleased, 1st Edition.* Pearson Education, Inc.

Olson, P. (2013). *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency.*

Security Magazine. (2012, September 24). *Stolen Laptop Leads to HIPAA Violation and $1.5 Million Fine*. Retrieved from Security Magazine: http://www.securitymagazine.com/articles/83517-stolen-laptop-leads-to-hipaa-violation-and-15-million-fine

Stallings, W., & Brown, L. (2008). *Computer Security: Principals and Practices.* Pearson Education, Inc.

Whitney, L. (2009, August). *Utility Spotlight: SDelete*. Retrieved from TechNET: http://technet.microsoft.com/en-us/magazine/2009.08.utilityspotlight.aspx

Missouri Department of Health & Senior Services. (2014). Health Effects from Chemical Exposure. Retrieved from <http://health.mo.gov/living/environment/hazsubstancesites/healtheffects.php>

United States Environmental Protection Agency. (8.9.2011). Hazardous Substances and Hazardous Waste. Retrieved from <http://www.epa.gov/superfund/students/clas_act/haz-ed/ff_01.htm>

http://www.newfoundreaestate.com

http://www.mcbridefinancial.net

http://www.mcbridefinancialservicesco.weebly.com