

**Crisis Management
and
Emergency Response
in Banking Industry**

**Juan Carlos Acevedo
March 5, 2007
BADM 395
Project Proposal**

Overview

Even the most secure systems are vulnerable to fail. As we advance as a society, new threats and attacks develop on a daily basis. Each time in which we have a new technology developed and a way to protect many of its vulnerabilities, there is always a way that the system can be fooled, beaten, or forced to fail. Defining potential threats and attacks becomes a difficult task not only for businesses or organizations, but also among many normal pc and internet users. We have seen in the past few years that private information of clients has been lost due to many errors even though the maturity level in information security were considered to be adequate or even proactive. Even if a system is considered to be a trustworthy computing system, it is vulnerable to fail by inside or outside attacks. What then should a company or organization do if the system fails?

This research paper attempts to find about the Emergency Response and Crisis Management blueprints that top Banking Corporations have to protect both the information of their client and their financial statements/plans. It also attempts to research on the steps, software, plans, response, benefits and costs of putting an emergency response. Financial institutions are a major target for predators who each day become more intelligent and sophisticated in finding ways to steal, hack, or intrude into a system to cause harm or for personal gains. Financial institutions have been around for hundreds of years now. Their first business processes were to make money advances to trading companies who needed to buy inventory before they could gather any revenues.

Today, financial institutions make business transactions with the general population by providing checking and savings services. With the money gathered, financial institutions are able to make loans to private businesses or individuals who have an investment in mind. That is why by researching the financial institutions we can get a better understand of Crisis Management. Money transactions between financial institutions and the general population and businesses happen on a daily basis. There is a proportion of the population who is interested in finding ways to steal, hack, or intrude into a system to cause harm or for personal gains. By researching financial institutions we can also understand more about the emergency response plans that corporations use at this point in time, the new innovations and plans. Above all, we will be able to understand the approaches many financial institutions have towards crisis management and what plans they have in case of an emergency.

STRATEGIC MANAGEMENT

Every corporation or business alike needs to have a strategic plan and management style to survive the business world. Maintaining customer trust and confidentiality is the paramount responsibility in a successful banking relationship and a strategic plan that a banking corporation should follow. The Banking Industry should develop policies that specify the organization objectives yet also must assure that IT is aligned with the plans and objectives of the organization. Financial organizations also need to follow mandated rules, law, standards and acts which preserve the information of customers. By assessing the risk factors which may prevent the corporation to align the system with the organization expectations of the system, corporations usually rely on Risk Management.

Risk Management

The term Risk Management has been around in the business world, yet inside IT, assessing the risks to insure privacy has become a more tangible asset as years pass by. KPMG realizes that the substantial risks can include reputation, brand damage, litigation and enforcement actions, disruption of operations and even failure to achieve their strategic goals.¹ All may harm the business to the point that it can lose so much that it can go out of business. Here is where our concern lies. What should a financial corporation do in case these risks were not avoided, prevented, or managed? Can a Corporation continue business operations while it deals with recovery efforts caused by an intruder, hacker, or anyone else that caused damage to the organization? What kind

of Emergency plans do financial corporations have to deal with uncertainty, loss of data, litigation, etc?

Crisis Management

The field and subject of Crisis Management within the school of business is relatively new. When the unexpected happens, crisis management is a way to proactively manage activities that will lead to continue business as soon as possible after an attack, or disrupted event to the business occurred. Typically, proactive crisis management activities include forecasting potential crises and planning how to deal with them.

Crisis management tries to find the nature of the crisis, minimize the damage done, and finally recover from the crisis. Yet since information systems can also be social systems, damage done to a system often involves more dynamic factors within the organization. It seems every risk that may cause damage to a corporation reaches different audiences and a company must face these audiences different. The company must be always ready to fight for litigation processes, but it must also have precision strategies to reach each audience and control the situation. Market share may diminish as a result of all the litigation and in turn there could be a dramatic customer loss. Yet there are a few basic plans that a business must proactively approach to plan for the unexpected. It should consider that in case of an intruder stealing information, a hacker trying to access unauthorized data, or an insider acting maliciously or erroneously, the corporation should plan well ahead if it wants to continue business after the incident. It has been seen a few too many times how corporations have failed because they were inadequately trained, or

prepared to deal with a crisis within the corporation. In case of a crisis, a corporation should plan for litigation processes, communication to the public, market share, etc.

Law and Litigation

One major risk that many corporations face is that of litigation and cases. In today's business world corporations have Digital Liabilities which may come to harm the business if not taken care of. Lawyers can file privacy invasion on behalf of employees, customers, business partners, and/or shareholders.² With the cases of Enron, Anderson, Worldcom etc of the past decade, law litigations have become increasingly worrisome for many corporations. Though these cases had very little to do with Digital Liability, the final consequence brought by the criminal acts taken by a few individuals of the corporations caused the whole business to collapse. It seems these corporations failed because of the act of a few individuals, but was it the litigations that made these companies fail? What if it was a financial institution instead of a public company or a service provider?

In the banking business there is a major law that requests information security and confidentiality of customer records. The Gramm-Leach Bliley Act of 1999 requires that depository institutions and their subsidiaries ensure "the security and confidentiality of customer records ... against any anticipated threats ... and protect against unauthorized access to, or use of, such [records]...." "It suggests steps to prevent unauthorized access by disgruntled employees - the primary source of systems sabotage - whereas the next installment addresses cyber-terrorism and other external threats to information security."³

The Act actually consists of three sections. The Financial Privacy Rule regulates the collection and disclosure of private financial information. The Safeguards Rule states that financial institutions must implement security programs to protect such information. Finally the Pretexting provisions prohibit the practice of pretexting (accessing private information using false pretenses). The Act also requires financial institutions to give customers written privacy notices that explain their information-sharing practices.

This is a major law that financial institutions should follow. Planning ahead of time would include covering these litigations by diminishing the effect of the crisis. A major example can be that of Johnson & Johnson where some Tylenol bottles had been tampered with and contained poison. Johnson & Johnson accepted that some bottles may have been tampered, and recalled all products made by Johnson & Johnson to avoid further injuries or damage to the customers. This in turn turned out to be a positive because society's perception of Johnson & Johnson was that of a responsible corporation who cared about their customers. Though the litigation costs were costly in the short run, Johnson & Johnson was able to diminish these costs in the long run by demonstrating responsibility. Ivan Schneider of Bank System and Technology states that it could be the same in financial institutions. Citigroup lost some data tapes during one routine delivery by UPS. With it, they lost the information of about 3.6 million customers. The cost to inform and help each customer was around \$75 dollars per customer. The cost of reaching out to customers can pale in comparison to the legal costs involved with responding to class-action lawsuits. "You're talking six figures to read the complaint, seven figures before you get to a court," asserts Kevin Kalinich,

national managing director for technology and professional risks, of Aon's (Chicago) Technology and Telecommunications Group.⁴ Therefore a corporation should be aware of the costs incurred for litigation expenses and prepare a plan that can pay these expenses in case a crisis occurs. Furthermore, a corporation should look forward into diminishing the impact by accepting liability for the damages occurred and be careful not to portray as having the situation uncontrollable. That takes us to how to direct communications to the general public.

Crisis Management Communications and Public Relations

When a European bank was targeted for abusive tax shelters and called before Congress, the audience it needed to reach included regulators, investors, and elected officials. Crisis management often includes strong focus on public relations to recover any damage to public image and assure stakeholders that recovery is underway. Crisis in corporations may threaten the image perceived by consumers or may even result in fines or jail terms. Usually the media might use corporate crises as the most important story of the day or period of time. A corporation may find necessary to hire a spokesperson or have a crisis communication plan to assure that all information given of the corporation does not further harm the business. A crisis communication plan though is only a blueprint that may specify the steps to assure that all communication given to the public is that which that corporation wants to express. It specifies needs for a spokesperson, for training, for message development, for identifying key media contacts, for recruiting supportive third-party media spokespersons. Yet, one has to be careful and acknowledge

that communication plans may change over time. The plan placed by an organization to deal with the public can be quite dynamic as reporters change jobs, new media streams are developed, and the blueprints and organization might make to deal with the communication may become obsolete as spokespersons may change jobs, directors move up or down the hierarchy of the company, etc.

All the factors should be taken into consideration to address the need to generate the desired outcome in a crisis. The plan should rely on diverse team members who in the crucial time will have their own contacts. Lawyers have their own backgrounds, employees, directors, etc. The plan then should be a strategic blueprint where it should pinpoint the questions you want the press to ask, how address each contact that the crisis touched, when the organization should fight back to those who caused the crisis, and what kind of message is the organization trying to portray. In general, the communication blueprint should primarily care about the reputation of the business and to diminish the impact perceived by different people whether they are directly or indirectly involved with the organization. Yet, the execution of the plan is what would count the most. A plan is only a plan if it is not executed. A financial organization or any sort of organization must be able to rehearse the blueprint in case of an emergency or crisis.

When at Fault

A big part of crisis planning and communication is that one should anticipate the possibility of going through a crisis or emergency. Some involve the organization directly and society's expectations to resolve the problem might be high. Yet sometimes organizations deal with a crisis that does not directly blame the organization because of an action taken, but because a third party, or out-of-control factor involved the company to find itself in a position of a crisis. When at fault, simple methods should be use to insure that the reputation of the company is not at stake. Levick, a company for strategy communications suggests that a company or organization should follow simple house rules within the organization.

- Tell the truth.
- If you make a mistake, apologize immediately.
- Be sincere in your apology.
- If you are explaining you're losing. Explanations drown out the apology.
- Really fix the problem.
- Blaming the other person does not score you any points.
- Ignoring the problem does not mean it goes away.
- You are always being watched, especially when you are not at your best.
- Crisis abhors a vacuum. If you don't fill the void with leadership, someone else will.
- Listen to your mother [those on top of you]. If you can't justify to your mother what you are doing, don't do it.

This could in turn lead the public to believe that the organization is honest and is concerned about the problems. Ignoring the problem or blaming others may not win points, but in some cases one needs to be careful not to accept all liability for parts that the organization is not at fault because the costs would be greater than what they actually could be.

When not at Fault

As stated before, there are natural disasters, third party mistakes, intruders, hackers, or insiders who were not ethically trained that can cause the organization to crumble. To plan for these situations, an organization should be aware that these factors can actually happen. For financial institutions, it could be a case of identity theft, external factors such as the stock market, inflation, etc. The organization should deal with these factors to the same degree that it would when a crisis occurred because of an error made by the organization. Though it would be less likely that the organization be faced with litigation, one can use the crisis to assure its customers that there is a backup plan for these events as well. It provides a place of comfort zone for the public and the reputation of the organization stays intact or sometimes even betters itself.

Common Operation Picture and Information Flow at all levels of the Organization.

When planning a crisis management blueprint, one must have some key features that the whole organization understands at all levels of the organization. The National Incident Management System by the Homeland Security department gives us a great look at how

communication between the organizations is essential in actually executing the plan. Key Decisions must be made to ensure that everything all information is running organized among all levels of the organization. When planning the organization should set up a team of executives or personnel that would advise and assist the organization in making executive decisions and directing the response and recovery operations. They should be in charge in commanding the incidents, and be sure that all flow of resources and information is running accurately and as planned. They should be careful that at each level of the plan there has to be a person-to-persona interaction and should be directed by area experts. Political coordination should be addressed by functional areas and all planners and decision makers should be integrated with constant communication. They should have a routine simulation of the crisis so when the crisis occurs there is a smooth command transition process. Keep in mind that there are multiple levels of the plan as well as all people may be in different areas and time zones at time. There should be an awareness that not the same people may be in control at different points in time. Finally key groups should inform the executive group of all changes of the crisis and how the operations are being followed so there can be a central location. The blueprints of the crisis management in general should include all possible ways crisis that financial institutions can have. These are

- Financial crisis - short term liquidity or cash flow problems; and long term bankruptcy problems. These include criminal actions taken by employees, executives, or even third parties that have contact with the organization. We have

seen cases such as Enron, Anderson, Worldcom, etc that ended up not being able to continue business when the crisis of their organization hit.

- Public relations crisis - More commonly called "crisis communications," is the negative publicity that could adversely affect the success of the company.
- Strategic crisis – The changes in the business environment that call the viability of the company into question. For example the introduction a new company is born with a new technology that makes the one in your organization obsolete.
- Natural Catastrophic crisis – Is the changes in the natural environment that can destroy, alter when and where your organization does business, stop your organization in some way, or involve part of your organization. These could include from fires in the database center, to a major catastrophic event in the locations your organization does business. One major example can be that of Katrina. Local businesses were great affected, yet major businesses were hit such as Wal-Mart, Home Depot, etc. These organizations were able to use their resources to aid the people affected by Katrina and in turn were able to gain reputation in a time of crisis.

Execution

The execution of a crisis plan should be based on past rehearsal and previous communication of the people involved in the emergency response. If we take financial institutions, if they don't try to anticipate the possibility of ever being part of a scandal then they will always be vulnerable to fail even if they trust their systems. The execution in time of a crisis should be already planned. If we take another example, we have that of

the recent Virginia Tech shooting spree made by one single individual but has left a dramatic scar. What if VT had a system in how to respond to a situation like this? What if students knew that an individual had just killed a few classmates, would they had gone to the engineering campus or would they have avoided the risk of being in a situation that endangered their safety? Plans need to be thought well in advanced and executed in mock trial to assure the safety of all. What makes crisis management a successful part of the business if they organization proactively searches for risk management in search of risk and vulnerabilities in the organization. In financial institutions, where money transactions happen on a daily basis, are vulnerable to such attacks. What is it then that a financial institution can do to protect its organization, its system, and expect when the unexpected occurs?

A CASE ANALYSIS OF FINANCIAL INSTITUIONS

Over and over again we hear news about a laptop being stolen, or thousands clients whose private information has been stolen because there was a security breach or some one hacked into a database. Identity theft is on the rise, and all of us are at risk of having our identity stolen. According to the US, the loss to U.S. businesses and consumers is equivalent to the GNP of an oil-rich Middle Eastern nation: \$56.6 billion in 2005.

When identity theft happens to organizations, as seen before, they have an obligation by law or reputation to limit the damage for all involved and start helping in figuring out what happened and how to resolve it in the future. Here is where Crisis management can

play and perhaps has played a major role in reassuring customers that the organization will help to fix the problem even though the problem has already occurred. Crisis management in a sense is an art of foreseeing the future and trying to be ready to diminish the impact. Here we take the example of identity theft to see the difference between having crisis management and not having crisis management.

Crisis management in financial institutions that are getting ready to prepare for a security breach would not only assess the risk and vulnerabilities of their organization but start planning an emergency response in case one of the risks actually hit them. There is a difference though in anticipating a risk and that of accepting the risk. Anticipating would acknowledge the system is not perfect but would try its best to fix the most it can to the best of the knowledge of the organization. Accepting a risk would simply be accepting the fact that there is a mistake and nothing should be done to fix it. In these circumstances companies lose their reputation and many customers suffer for the irresponsibility of the organization.

As stated before, financial institutions should be aware of the litigations that may followed, or more than likely will follow, after an ID theft occurred. It is a public safety issue to a broad spectrum of audiences and creates a public education campaign that helps guard against ID theft. In conclusion, following this example case, the financial institution can make a promise to protect customers' personal data along with a credible sense of how that is going to be done after the crisis. It can also act concerned about the

welfare of the clients and situation, and convince that the business is learning fast from the mistakes done.

Conclusion

This paper attempted to reach a better understanding of what crisis management is and the types of factors that should be included within the topic. It is imperative that each organization have an emergency response to each crisis that they can foresee and plan ahead to better be equipped when a crisis hits. Some of the factors mentioned in this paper were that of trying to conform with the law and to possible litigations that may follow after an incident.

Another factor was that we saw was of how important it is to have a plan to communicate with a broad spectrum of audiences. As our mini case demonstrated, it is important that a company assure the public that they are learning fast, and that they are trying their best to keep everything under control. People are sympathetic to errors, yet want to feel assured that their assets are not in danger. They should plan a media strategy through all available resources such as employees, executives, third party members.

Above all, an organization should anticipate the to exposure problems they are likely to have a have a plan ready for the whole organization. They should not wait for the crisis to occur without being prepared.

¹ KPMG, A New Covenant with Stakeholders, Managing Privacy as a Competitive Advantage. © 2001 KPMG LLP, the U.S. member firm of KPMG International, a Swiss association. All rights reserved. 22650atl

² SearchCIO.com Leach-BlileyAct http://searchcio.techtarget.com/sDefinition/0,,sid19_gci951347,00.html

³ Marta Stern, Safeguarding customer information: The key to customer trust *Marta Stern*. ABA Bank Compliance. Washington: Nov/Dec 2001. Vol.22, Iss. 11; pg. 30, 10 pgs

⁴ [IvanSchneider](http://www.banktech.com/news/showArticle.jhtml?articleID=164904002), BankSystem&Technology . June 29, 2005. Available at <http://www.banktech.com/news/showArticle.jhtml?articleID=164904002>

Fitzgerald, Jerry. *Implications for Management*. Business Data Communications and Networking. 8th Edition. Pg. 405.

Oz, Effy. Management Challenges and Solutions. Management Information Systems. 4th Edition. Pg. 301.
<http://www.managementhelp.org/crisis/crisis.htm>