Using Identity Theft To Teach Enterprise Risk Management – Make It Personal!

Norma C. Holter, Towson University
W. Michael Seganish, Towson University

INTRODUCTION/ABSTRACT

This article introduces an innovative way to teach the Enterprise Risk Management (ERM) Integrated Framework (as developed by COSO), while at the same time informs the student of a real personal risk -- identity theft. This example of assessing and managing a real risk will enhance the student's understanding of risk management, thereby increasing the skill set of the student. The student who gains an understanding of the ERM concepts can then apply this tool to all of the disciplines of business. The ERM framework can be tailored to any discipline, as shown by the following examples: presented in connection with the Balanced Scorecard; evaluating different organizational strategies in a Business Policy class; case analysis in Management or Marketing (particularly a new product or new market); in an Auditing class with discussion of internal controls; in Finance to evaluate the decision to invest in derivatives or capital project, and in an Entrepreneurship class.

Keywords: Enterprise Risk Management; Auditing; Management education; identity theft; risk assessment; risk management; risk evaluation; risk identification; teaching risk management

BACKGROUND

Regulation of business in the United States dramatically changed with the passage of the Sarbanes-Oxley Act. An emphasis is now placed on risk -- how to identify, assess and manage risk, which flows from management's strategic decisions and objectives -- is now a corporate priority and a major management function. It is the Chief Risk Officer's role to champion the Enterprise Risk Management (ERM) initiative by bringing together disparate risks, whether they are operational, market, financial, or credit risk, to insure that key strategic objectives are met.

This focus on risk was heightened, in particular, by Section 404 of Sarbanes-Oxley Act[1] which dictates management's obligation to establish and maintain adequate internal control structure and procedures for reliable financial reporting. In addition, management must include their assessment of the design and operating effectiveness of internal controls with the annual report filed with the SEC. Section 404 forced management to identify and document relevant controls related to financial reporting, with an objective of identifying areas where the organization's financial statements could be exposed to a risk of material misstatement. This documentation lead to identification of areas of weakness, formerly unrecognized, where fraud could occur. The independent auditor must also express an opinion on the effectiveness of the organization's internal controls.

A business operates within the context of an industry in a global economy, subject to regulatory and other external factors, as well as internal environmental factors. In response to these factors, management defines strategic goals and objectives, which will change over time, in response to these environmental factors. Business risk flows from these actions and decisions.

Management establishes processes, policies, and procedures within the organization in order to provide reasonable assurance that the organization's objectives are met. The way in which these internal controls are defined and implemented varies with the organization's size, industry, and complexity.

The basis or framework for internal controls was established by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and is the recognized international standard. There are five interrelated components:

(1) Control Environment (example: setting the tone at the top, a code of ethics);
(2) Risk Assessment (identifying and analyzing all relevant risks and how they should be managed);
(3) Information and Communication (exchange of information within and outside the organization necessary to enable people to carry out their responsibilities);
(4) Control Activities (actual policies and procedures established by management to assure the objectives are met); and
(5) Monitoring (continuous monitoring over time of the quality and effectiveness of internal controls).

In view of the numerous high profile business scandals and failures that occurred in the recent past, it became obvious that the framework of internal controls needed to be enhanced or integrated into a more robust model which included risk management.

COSO initiated a project to develop a framework for ERM that would be readily usable by management. The goal was to provide a model for management which would provide key principles, a common language, and guidance to identify, assess and manage risk. This model incorporated the five components of the internal control framework and introduced three new components:

(1) Objective Setting (a process should be in place to set objectives which align with the organization's mission statement and are consistent with the organization's risk appetite);
(2) Event Identification (internal and external factors which identify potential events affecting achievement of the objectives); and
(3) Risk Response (a decision by Management to avoid, accept, reduce or share a risk). COSO defines ERM as a "multidirectional iterative process in which any one component can and does influence another"; a "continuous iterative interplay of actions that permeate an entity".[2]

TRANSLATION OF THE CONCEPT TO THE CLASSROOM

Knowledge of risk assessment and management is another skill for the business student's toolbox. This framework for evaluating risk can be applied to any of the business disciplines. However, risk assessment and management are not readily understandable concepts to many students. The only risks students have evaluated were perhaps amusement park rides and extreme sports like bungee jumping. If a student had an internship, it is unlikely they would have been involved in the ERM development process because their employment was temporary. Unfortunately, if a student doesn't understand a concept, then the concept simply becomes a memory exercise. Many students are kinesthetic learners – they learn by applying the concepts. The pedagogical challenge was to identify a business-type risk that the student could experience. If a generic model could be developed which the students could understand, then hopefully the students could transfer this knowledge to particular circumstances in their various classes.

Finding the right scenario was the initial challenge. The authors had previously written in the identity theft area and were aware that there is a victim of identity theft every four seconds. The crime of identity theft is costing the American economy $15.6 billion a year.[3] Experts say one out of every eight Americans has been a victim in the past five years.[4] "As many as 88 million Americans – more than one in four – had digital data exposed in the past 18 months".[5]

College students are being targeted by identity thieves because by obtaining a student's identification number (usually designated as a student ID number on campus) a thief can use the number to apply for student loans and perform other fraudulent acts.[6] The advantage of stealing a student identity is that the student's credit history is normally a clean slate. This risk thus became the perfect scenario for explaining the risk concepts.

RELEVANCE OF IDENTITY THEFT RISK TO STUDENTS

Students should be made aware of the risk of identity theft because of the severe consequences associated with this white collar crime. The consequences include not only the monetary loss sustained (charges made to credit cards or by bank accounts being emptied), but also the costs to correct the damage to one's credit and reputation as a result of the identity theft. Further, the costs not only involve the time that will be required to rectify all the financial devastation but will also impact the victim's lifestyle. Until all records are corrected, the victim will be unable to obtain credit (evidenced by the inability to purchase/lease a car, to buy a house or rent an apartment, or something as basic as the inability to obtain electricity or cable without a large deposit). The more perilous situation is if the identity thief has used the victim's name in the commission of a crime. The conviction, under an incorrect name, is then included on a criminal database such as NCIC (National Crime Information Center, FBI) and the victim could have a felony conviction on his/her record and be totally unaware of this.

THE EXPERIMENT

Initially, the risk of an unreliable supplier was used to introduce risk assessment, (unreliable being defined as not delivering at appointed time, not delivering the requested quantity, not delivering the material specified on the purchase order, and delivering a product not up to specifications). Following the lecture (which included several examples of each component as it was introduced) and notes, the students were asked to evaluate this risk, using the COSO risk components, as a class exercise. The first item they were to identify was the strategic objective. After several minutes and inappropriate suggestions, we finally agreed that a dependable supply chain could be a strategic objective and that this supplier was indeed a risk to that objective. Strategy was identified by the students as simply "return the unacceptable stuff". During this class exercise, the answers/ suggestions were superficial at best. Lecture and notes did not seem to promote sufficient understanding, even though numerous examples were given during the lecture. It appeared that the undergraduate students, having little or no experience in the corporate environment, simply viewed this as another conceptual model that they would memorize. The next step pondered was, if given a personal example, would the student response, ability to understand, and participation in the class exercise be improved.

Another section of the same class was given the handout (Appendix A) as part of the lecture, explaining the components through the personal example of identity theft risk. As the class worked through the various components, their responses and proper identification of the processes reflected understanding. By the time we had reached the end of the identity theft exercise, the students were comfortable with the ERM model because they had helped to develop it. Their confidence was evidenced in the responses to the unreliable supplier example which was presented next. This class was more responsive. Their answers were more comprehensive and numerous, indicative of reflective thought, and there was a greater willingness and participation in the exercise on the part of the students. The difference in the attitude and depth of answers in the class that received the handout, repeated over several semesters, seems to indicate that if you relate the concept to the students, (make it personal or familiar and encourage the students to participate at this basic personal level) the students are more interested and are more receptive to learning and understanding the new concept. The students had gained confidence through the personal example and could easily adapt the concept to other applications.

As preparation for the introduction to the ERM model, the students were familiarized with the definition of identity theft and the ways it can be perpetrated.

DEFINITION OF IDENTITY THEFT

The Association of Certified Fraud Examiners defines identity theft as: "There is no one universally accepted definition of identity fraud. Identity fraud or theft refers to the illegal use of personal identifying information – such as name, address, social security number and date of birth. Identity theft is a crime in which someone wrongfully obtains and uses another person's personal data in some way that involved fraud or deception, typically for economic gain."[7]

WAYS AND MEANS OF IDENTITY THEFT

Identity theft may be accomplished by a variety of means. A thief can obtain one's social security number, date of birth, information about parents, income, and even access to checking and savings accounts by "phishing" on the Internet where an unsuspecting person is sent an official looking email in connection with a credit card or an account at some financial institution. Many times the bogus email will copy the financial institution's official logo. The email will indicate that hacking has been occurring at the financial institution and the email (from the thief) asks that you "verify" the information to assure the institution that your information has not been altered. The victim has unwittingly provided the identity thief with the information to commit the crime.

Unauthorized hardware or software installed onto or within the computer systems of legitimate businesses (mostly retail) have become the tool of choice for savvy hackers to steal debit and credit card information. Recently, unauthorized software was placed on TJX Company computers and over a period of several years, the hackers stole at least 45.7 million credit and debit card numbers. The thieves were so proficient that they could collect the information as the transaction was being approved at the various T. J. Maxx and Marshall's stores.[8] Hackers have become so proficient that names, addresses, account numbers, even social security numbers, and other identifying information are sold through underground internet sites for as little as five dollars each.[9]

In almost half (47%) of the instances, the identity theft is perpetrated by friends or neighbors, someone known to the victim.[10] It is usually in a social setting where there are many people present: a library, stadium, bar, or party; an airport, bus terminal, or train station. Students should be particularly careful when carrying backpacks and luggage as a back pocket containing a wallet or an open purse with a wallet visible are the moments the thief seeks. This carelessness/casual behavior thus presents the thief with the opportunity to steal and thereby obtain information to commit fraudulent acts.

THE ERM MODEL

The reference for this part of the course is the two-volume set of the report: "Enterprise Risk Management – Integrated Framework" by the COSO.[11] A copy of the entire two-volume set is kept on reserve in the University library and is available for student use and reference.

STRATEGIC OBJECTIVE/STRATEGIES

A handout (Appendix A) is used as a supplement to introduce the components of the model. After an explanation of identity theft (Most students have some level of awareness.) and how pervasive it has become (This surprises the students.), we agree that a good **strategic objective** is to avoid becoming a victim of an identity theft crime. Objectives are set at the strategic level, (thus establishing a basis for the operating, reporting and compliance objectives), after considering a range of strategy choices and the organization's risk appetite.

To identify/develop the **strategies,** the class is asked: "What needs to be done so that the objective can be accomplished?" Appendix A presents some of the acceptable answers. The organization's mission statement and strategic objectives are generally stable. However, Strategy and many related objectives are adjusted for changing internal and external conditions so that they are always aligned with the strategic objectives.

RISK APPETITE

To introduce **risk appetite**, the class is asked the obvious question if anyone wishes to become a victim. Since no one wishes to become a victim, it means no one wishes to accept the risk or that there is no appetite for the risk. Risk appetite defines the tolerance for the risk. A risk is measured by its impact (consequences) and likelihood. Many organizations will assess the risk appetite by a "risk map"[12]. The risk map is a graphic way to express a company's (or individual's) risk appetite by plotting the impact (vertical) and likelihood (horizontal) of a risk factor on a graph from low to medium to high. The risk map can be applied to any decision. To reinforce this

point, the students are reminded that this tool can be used in management, marketing, and finance classes. It can be part of case analyses in the capstone course.

EVENT IDENTIFICATION

Event Identification requires management to identify what potential events, if they occur, could affect achievement of the objective. As a result of this process, potential events with positive outcomes represent opportunities while events with negative outcomes represent risk. Events with positive outcomes, which could become opportunities, are reconsidered to see if they should more appropriately be classified as a strategy or even possibly an objective. Identifying these events is not easy. There are several factors/measures that help management pinpoint these events. **Internal and external leading event factors** that could affect the objective are defined by both quantitative (interest rates, price of fuel, number of visits to an Internet site, turnover of inventory) and qualitative (staff use of a particular program; changes required in a program or schedule) measures. Certain **escalation triggers,** which focus on day-to-day operations, are also examined. Escalation triggers are events which are reported to management on an exception basis -- when a certain parameter or pre-established threshold has been passed (example: when sales of a product drop more than 5%). Management will then filter this information to identify the most relevant potential events that could affect achievement of the objective. Facilitated workshops, questionnaires, event inventories, interviews, and process flow analysis can also be used to understand how an event will affect an objective. In Appendix A, we establish the external and internal leading factors but the escalation triggers help us to focus more clearly on the potential events.

RISK ASSESSMENT

Risk assessment is an estimate of the extent to which potential events will impact the achievement of an objective. At this point, having utilized the risk map as part of developing the risk appetite, management tries to hone the estimate of the impact and likelihood of a potential event from an inherent and residual risk perspective. Organizations use any number of different methods – some arriving at quite precise numbers while others seek a range. **Inherent risk** is the risk to an organization, in the absence of any actions management may take to alter the risk's likelihood or impact. **Residual risk** is the risk that remains after management's response. In Appendix A, inherent risk considers a greater economic impact than the residual risk estimate and a high likelihood. However, the economic loss will be minimized if credit and legal problems are detected and resolved early, as reflected by the measurements of residual risk. In addition, early response minimizes the timeframe for the thief to sell or pass the information on to other thieves. A recent on-line survey of 1,097 victims revealed that half the victims discovered the identity theft on their own.[13]

RISK RESPONSE

The response to a risk is made after assessing the impact and likelihood of a risk versus the costs and benefits of various risk responses. An organization will choose to avoid, reduce, accept or share a risk. If an internal risk is accepted, internal controls may be designed or heightened in an area of the organization. In some industries, the risk is shared or passed on to another party; for example, many insurance companies will pass on some of the risk through re-insurance, asking other insurance companies to cover some of the properties in a particular area where they may cover a majority of the properties; banks will pass on mortgages. In the example of Appendix A, the decision is to avoid the risk and various responses are listed.

RECOVERY FROM A RISK OCCURRENCE

The **recovery from a risk occurrence** has been added to the handout because there are times when an organization is not aware of a risk until some event has occurred, perhaps a change in technology or a regulatory change. This is why organizations then develop corrective controls and have back-up and recovery plans in place. This is also why monitoring is important. Appendix A lists the steps, recommended by the Federal Trade Commission, which should be taken after an identity theft has occurred.

MONITORING

Monitoring is necessary. Over time, parts of the risk management plan change. Responses that were once effective, are now outdated and inappropriate. Changes in technology can ripple through a risk management plan and cause many changes.

A change in upper management could bring an entirely different perspective. An outsource provider company may decide to close. Just because a risk has been identified and steps have been taken to mitigate or lessen the likelihood and impact of such an event occurring in the future, any system or strategy for achieving objectives needs monitoring to assure that the objectives are continuously being met. Appendix A suggests the steps that should be taken to monitor one's credit reputation.

CONCLUSION

Risk assessment and risk management are management tools that have a high priority today. By using identity theft as the vehicle to teach the COSO

ERM framework of risk assessment and management, the student has gained an understanding of these concepts through a personal example, enabling the student to transfer this knowledge to other applications. Understanding the integrated framework for Enterprise Risk Management adds to the students' skill set and will help the student to analyze, evaluate, and plan to make better decisions. The most appealing aspect of learning this tool is that many students will be using risk assessment in their jobs after graduation, with an accounting firm, a consulting firm, a large corporation, or a large nonprofit organization. This is relevant to their future. This tool is easily adaptable to any discipline in the business college.

APPENDIX A
RISK ASSESSMENT EXERCISE

(Handout as part of lecture on COSO Enterprise Risk Management Model)

STRATEGIC OBJECTIVE:

Do not become a victim of Identity Theft

STRATEGY:

Annually obtain free credit report from three major credit bureaus
(Equifax, Experian, and TransUnion)
Develop awareness and understanding of identity theft crime
Become sensitive to how my personal information can be stolen
Do not answer "phishing" emails
Develop habit of checking credit card bills and bank statements for possible unauthorized transactions

Risk Appetite:

0 occurrence - Even one occurrence is considered unacceptable
and exceeding the risk appetite
High impact/high likelihood on risk map

Risk Tolerance:

0 occurrence

EVENT IDENTIFICATION:

Identify the potential events, if they occur, that could affect achievement of the objective. Leading risk indicators (internal and external) provide insight into what potential events could occur:

External:

Opportunistic thieves seeking the right moment to steal.
Minimal crime deterrence: Prosecution for identity theft is less than 1% and the penalty/sentence is light.[14]

Internal:

Leaving purse/bookbag/luggage unattended
Transaction using debit/credit card
Providing information to questionable party through email or telephone

Escalation Triggers:

(events which cause risk to become escalated)
Public places: airport, stadium, bar, train station – where thief can readily mix into the crowd
Phishing
Transaction on an Internet site that is not secure
Too much information displayed through personal blog

EVENT IDENTIFICATION: POTENTIAL EVENTS:

Leaving bookbag/purse unattended – to do something or to go elsewhere, even momentarily
Being in a crowded environment
Not checking bills & bank statements for unauthorized transactions
Being careless with credit, debit cards
Transactions on insecure Internet site
Answering phishing emails/telephone calls
Posting too much personal information on blogs

RISK ASSESSMENT:

Assess extent of potential events on objective achievement. Hone estimate of impact and likelihood of risk

Inherent Risk (risk in absence of any actions to alter risk's impact or likelihood):

Impact:

Economic loss due to theft; credit destroyed; inability to obtain credit because credit destroyed; conviction of a crime; time, money and stress to correct/undo identity theft damages. $500 and up.[15]

Likelihood of Risk:

Maryland ranks #11 in terms of identity theft crimes[16]
9.9 million victims in 2006
A victim every four seconds

Residual Risk (risk that remains after implementing your response to risk):

Impact:

Economic loss minimized; credit problems identified/resolved in early stage; less time involved to correct identity theft damage.

Likelihood:

somewhat reduced

RISK RESPONSE:

(Decision to avoid/reduce/accept/share the risk)

In order to develop the best risk response, an assessment of the effect on impact and likelihood of a risk is weighed against the costs and benefits of the response.

Decision:

AVOID RISK

Guard your wallet; do not freely give out your social security number; guard your mail; shred personal information, including mail with your name & address; never provide personal information over the phone or Internet; use passwords for credit cards, bank and phone accounts and constantly monitor those accounts; go to www.optoutprescreen.com to remove your name from mailing lists of three credit reporting agencies which means you will no longer receive the "prescreened" offers; go to www.privacyrights.org/fs/fs24-finpriv.htm to prevent the sale or sharing of your financial information by your bank, credit card company, insurance company or investment firm; inquire if your bank or credit card company provides identity theft protection; purchase identity theft insurance.

RECOVERY FROM RISK OCCURRENCE:

Establish a record of all persons/agencies contacted; Contact three credit-reporting agencies and have a fraud alert put on your file by filing a ID theft report; file a police report (if police are reluctant, ask to file a "Miscellaneous Incidents" report) emphasizing that it may be necessary to correct some of the credit damage; contact all banks and establish new accounts, new PIN/password; contact all your creditors and ask for the company's fraud dispute form; contact State Department of Motor Vehicles; contact the Social Security Administration; file a complaint with the Federal Trade Commission.

MONITORING:

Annually obtain a free copy of your credit report from all three major credit bureaus (Equifax, Experian & TransUnion); pay close attention to billing cycles & call if a bill does not arrive; actively protect your credit and debit cards by being aware of your circumstances in public places; protect other private information by asking why it is needed when it is requested in connection with a transaction. (Many times it is not required.)

ENDNOTES

[1] Sarbanes-Oxley Act of 2002. Federal Government. Enacted July 30, 2002.
[2] The Committee of Sponsoring Organizations of the Treadway Commission. (September 2004). *Enterprise Risk Management – Integrated Framework Executive Summary Framework*. 6, 17.
[3] *Dateline,* (television broadcast). March 27, 2007: New York: NBC. Federal Trade Commission, 2005 Report.
[4] Yue, Lorene. (2004, January 14) An Identity Theft every 79 seconds. *The Sun* Baltimore. 3-D
[5] Foust, Dean. (2006, July 3) ID Theft: More than Hype. *Business Week.* 34-36.
[6] Bigda, Carolyn. (2006, April 2) Identity Theft is Harder on Youth. *The Sun,* Baltimore. 4-C
[7] Association of Certified Fraud Examiners. (2000) Conducting Fraud Examinations Proving The Case. Austin, Texas: Author
[8] Abelson, Jenn. (2007, March 30) Hackers Stole 45.7 million Credit, Debit Card Numbers, TJX says. *The Sun,* Baltimore. 1-F
[9] *Dateline*, March 27, 2007.
[10] Council of Better Business Bureaus and Javelin Strategy & Research. (2006 January 31). The 2006 Identity Fraud Survey Report. San Francisco: Author
[11] The Committee of Sponsoring Organizations of the Treadway Commission. (September 2004). *Enterprise Risk Management – Integrated Framework Executive Summary Framework.* And *Enterprise Risk Management – Integrated Framework, Application Techniques.* 2 volume set, www.cpa2biz.com.
[12] *Enterprise Risk Management – Integrated Framework*, Application Techniques. 17
[13] "Identity-theft victims find that they are often on their own, new survey shows. (2005 July 29) *The Sun*, Baltimore. E-3
[14] *Dateline*, April 3, 2007.
[15] Conkey, Christopher. (2007, November 28) Assessing Identity-Fraud Costs. *The Sun.* Baltimore. D3.
[16] Federal Trade Commission. www.consumer.gov/idtheft. And Privacy Rights Clearinghouse. www.privacyrights.org