Modeling Risk

Massoud Moussavi

1. Introduction

When we speak about risk we are often concerned with the negative consequences of an event in a particular context. The following list provides examples of events and some of their possible contexts (shown in italics):

- earthquake (*city*)
- a new drug in the market (*patients*, *doctors*, the *pharmaceutical company*)
- losing a tennis match (the *player*, the *coach*, the *team*)
- a terror act against a *country*
- a money laundering transaction (*banks*, *country*)
- loss of a senate seat (a *senator* or a *party or the constituents)*
- failure of a project (*project team*, the *team leader*, *investors*)

Notwithstanding many definitions for risk, we define *risk as the expected value of the outcomes of an event in a context*. This expected value normally is in terms loss of something. Risk of an earthquake in a city can be determined in the context of damages to properties and life; risk of a new drug for a pharmaceutical company is in terms of financial loss in case of negative side effects on patients; risk of losing a senate seat in an election in terms of expected loss of income or prestige if the context is the senator and in terms of expected political loss if the party (e.g., democrat or republican) is the context; and in the case of a project, say a carbon finance project, the expected economic loss in the event the emission reduction requirements are not met.

Broadly speaking, two elements contribute to occurrence of an event and thus to risk: *weaknesses* and *threats*. For example, risk of a terror act is influenced by a country's open borders (i.e., its weaknesses) as well as the existence of terrorists (i.e., the threats). As another example, a tennis player's weak backhand could lead to losing a tennis match but the same tennis player is less at risk against an opponent who doesn't play to his backhand. In the latter case, while the weakness (i.e., weak backhand) remains the same, the level of threat is different.[1]

To reduce the risk, we have to deal with the causes of weaknesses and threats. But we can also establish *control mechanisms* that reduce the chance of the occurrence of the event and take *mitigating actions* which deal with reducing the expected loss in case the event occurs. Thus, in analyzing risk, we develop a causal model that considers all the elements that influence risk: weaknesses, threats, control mechanisms, and mitigating actions. See figure 1 for a graphical representation.

[1] Alternatively, we can say one is vulnerable to an attack (i.e. threat) given one's weaknesses. For example, a tennis player with a weak backhand would feel more vulnerable against an opponent who plays to his backhand than an opponent who doesn't.

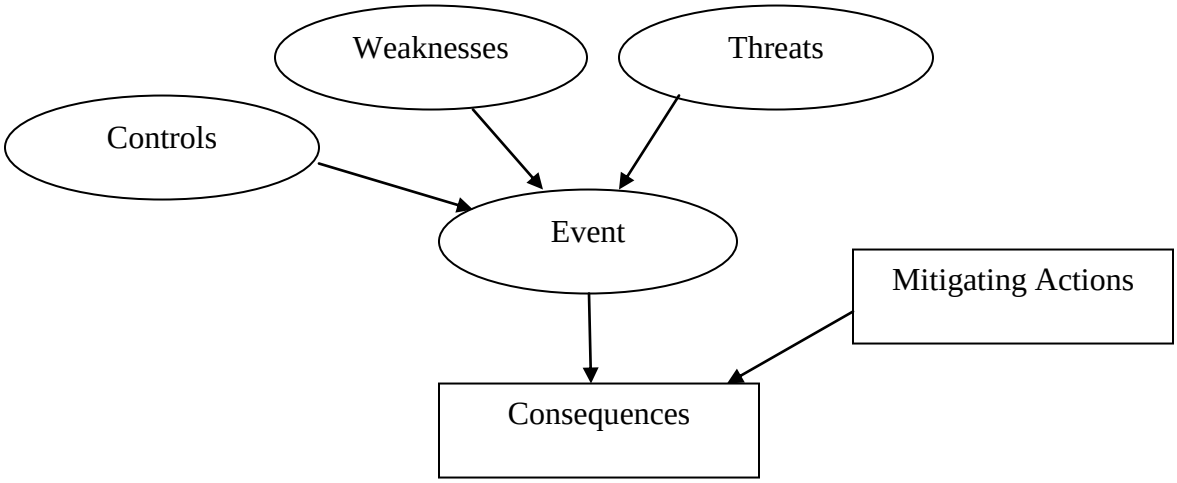

Figure 1: Elements of Risk

2. Constructing a Risk Model

In order to model the causes and sources of the risk, it is important to consider the context within which risk is defined. For example, in a neighborhood in which the number of burglaries has increased, *homeowners*, *the city government* and *insurance companies* will all be concerned with the risk of burglary. *Homeowners* in the neighborhood want to protect their assets. The *city government* would be concerned with the increasing number of calls to the police. *Insurance companies* would want to reduce the risk of increasing number of claims. But each group is concerned with a different set of causes and effects.

In order to reduce their risks, *homeowners* would be mostly concerned with reducing the vulnerabilities of their homes (e.g., poor lighting, broken windows, etc.), better protecting their homes (e.g., installing security systems, forming volunteer watch groups, keeping guns at home, etc.), and taking mitigating action like buying more insurance.

The *city government*, on the other hand, would be concerned with lack of enough police force, lack of good street lighting, and the control measures that they can implement (increase penalties for such crimes, better surveillance, etc.), and some mitigating actions (e.g., creating a special emergency force). They would also be concerned with the sources of the problem and the causes that might have led to the rise in burglaries (e.g., poverty, unemployment, etc.)

Insurance companies would be concerned with a yet another set of vulnerabilities, control mechanisms, and mitigating actions.

The main point here is that risk has to be analyzed in the context of a stakeholder. For each stakeholder, we would need to understand the sources and causes of the risk and assess the control mechanisms that are place in place.

To illustrate, figure 2 graphically represents some of the causes of burglary. A house can be vulnerable to burglary for many reasons: unlocked windows or doors, poor street lighting, having front and back entrances, location of the neighborhood, etc. The threat is increased burglaries in the neighborhood. Control mechanisms could consist of security system in the house, installing better lighting fixtures around the house, keeping a dog, etc. If a burglary indeed takes place the consequences can be loss of valuable items. An example of a mitigating is taking additional insurance.

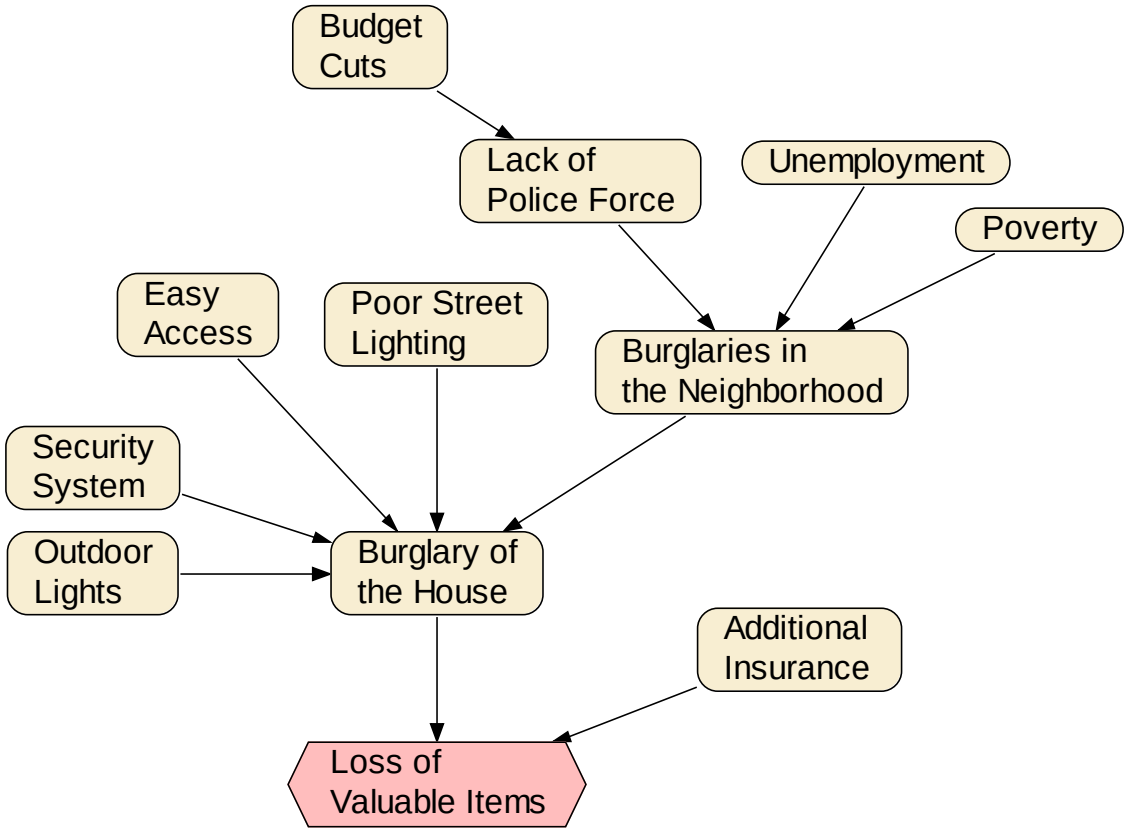

Figure 2: Risk of Burglary

As discussed above factors such as lack of police force, unemployment poverty, budget cuts will be of concern to the city government but not to homeowners. That is, if our objective is to compute the risk a homeowner faces we would not need to consider or evaluate such variables.

In order to compute the risk we need to assess the chance of occurrence of an event, say a burglary, given the weaknesses and threats.[2] We use a Bayesian network model [1] to represent probabilistic relationship among the causes of risk. A Bayesian network is a graphical representation of variables represented as nodes and their probabilistic dependencies represented as links or arrows. The direction of a link between two

[2] This chance is how we measure *vulnerability*. For example, when we say a house is vulnerable to burglary, we mean the chance of the house to be burglarized is fairly high.

variables indicates how one variable probabilistically affects another. Once the relationships between variables are quantified, Figure 2 would be an example of a Bayesian network. In this network, we might say that the probability a house would be burglarized given that it has no security system is 0.1 or 10%. Or the probability that a house would be burglarized given that it is located on a street with poor lighting might be assessed as 20%. These probabilities are assigned based on experts' judgment or statistical data available from police records.

Using a model like the one shown in figure 2, we can calculate the chance of burglary against a house given many factors that affect the safety and security of the house. Based on this probability, we can then compute the expected loss. For example, given that the chance of burglary is calculated to be 25% for a particular house, and assuming that the total amount of valuable items in the house is $100,000, then a rough estimate of the expected loss is $25,000. Among other things, this figure will be helpful in deciding how much additional insurance to buy.

In what follows we describe the construction of a model and a tool for assessing the risk of money laundering in a country.

3. Example: Risk of Money Laundering

In assessing the money laundering risk for a country, a good understanding of fundamental causes and sources behind money laundering is needed [2]. We develop a Bayesian network model that considers the vulnerability of the country to money laundering; the control mechanisms that are in place, as well as the level of threat. This model specifies the complex relationships among the following components, each represented by a set of state variables:

- The country (e.g., governance, culture, laws, etc.)
- The industries and sectors in the country, their vulnerabilities and control mechanisms (e.g., regulations, and level of compliance in the Banking, Insurance sectors)
- The money launderers (local and international proceeds from various crimes).
- The geopolitical environment.

Construction of the Model

Consider the task of a developing a simple risk model to represent the following:

Law enforcement and level of regulation both affect the level of compliance with Anti Money Laundering (AML) standards. Level of compliance affects ease of placement as well as ease of layering[3] *both of which in turn influence the vulnerability of the banking*

[3] Placement and layering are two stages of money laundering. An example of placement is the entry of large amount of money (cash) generated through illegal activities into a financial system. Layering refers to the creation of complex layers of transactions to conceal the source and ownership of funds.

sector. In addition, assume that international connectivity affects ease of layering and substantial cash transactions influence ease of placement.

Deciding on the topology of the network is the *first step* in building a Bayesian network. The diagram shown in Figure 3 represents our simple model.

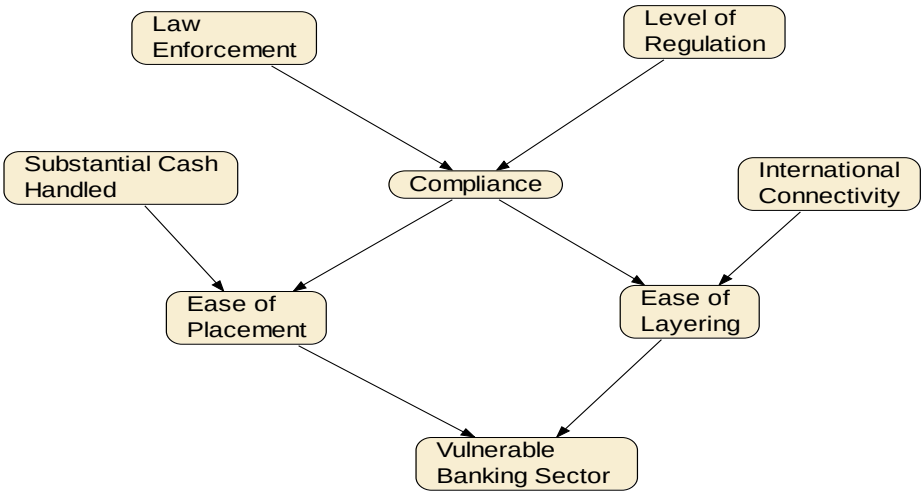

Figure 3: A simple model

The *next step* is to specify a conditional probability distribution for each node, given its parents[4]. This is where we rely heavily on data, research as well as experts' judgments. (In the case of AML, as there is limited data available, we would rely mostly on experts' inputs.)[5] For example, an expert might indicate that strong law enforcement would *highly* influence the level of compliance, and the existence of good regulation would *moderately* influence the level of compliance. These qualitative assessments would then be turned into quantitative conditional probabilities, say 90% for high influence and 50% for moderate influence. It is important to note that Bayesian network is very robust to imperfect knowledge and quite often these subjective probabilities yield very good results. Experience has shown that often it is sufficient to ask experts to state their degree of belief in terms of *high*, *moderate*, and *low* assessments rather than exact numbers.

Note that in constructing this network we use a degree of approximation through selection of variables to represent the domain. For example, in this model we have included only two variables that affect compliance. The degree of approximation can be improved if we introduce additional relevant information: factors including management commitment, staff integrity, staff training, etc. In building a model, we need to decide on a reasonable level of approximation as for many factors we would have no reasonable way to obtain the relevant information.

[4] This may seem too many numbers to specify, but some efficient methods for representation of conditional distributions exist.
[5] If good data is available, conditional probability estimates can be automatically learned from data.

A major benefit of a Bayesian network is that it works with whatever information is available. As more information is acquired, it is reflected in the updated probability distribution of variables. The construction process of the network also benefits from this adaptability. The network can start small with a limited knowledge of the domain and grow as more knowledge is acquired.

A User Interface

Once the model is constructed, it will be used within a risk assessment tool to make inferences. Given some observation (i.e., obtaining new information) about a set of variables, all the probabilities are automatically updated. A user-interface will enable users to analyze the impact of various policies and also to examine the trade-offs among different interventions. Figure 4 shows a simple user interface for our model. The top of the screen includes the observable factors: level of regulation, law enforcement, international connectivity and whether substantial amount of cash is handled. For example, the likelihood that law enforcement is strong has been entered as 30% in this screen. The bottom part of the screen shows the factors that are dependent on the observable factors and their values are inferred in the model. For example, the likelihood that banking sector is vulnerable is determined as 64% given the values for the observable factors.

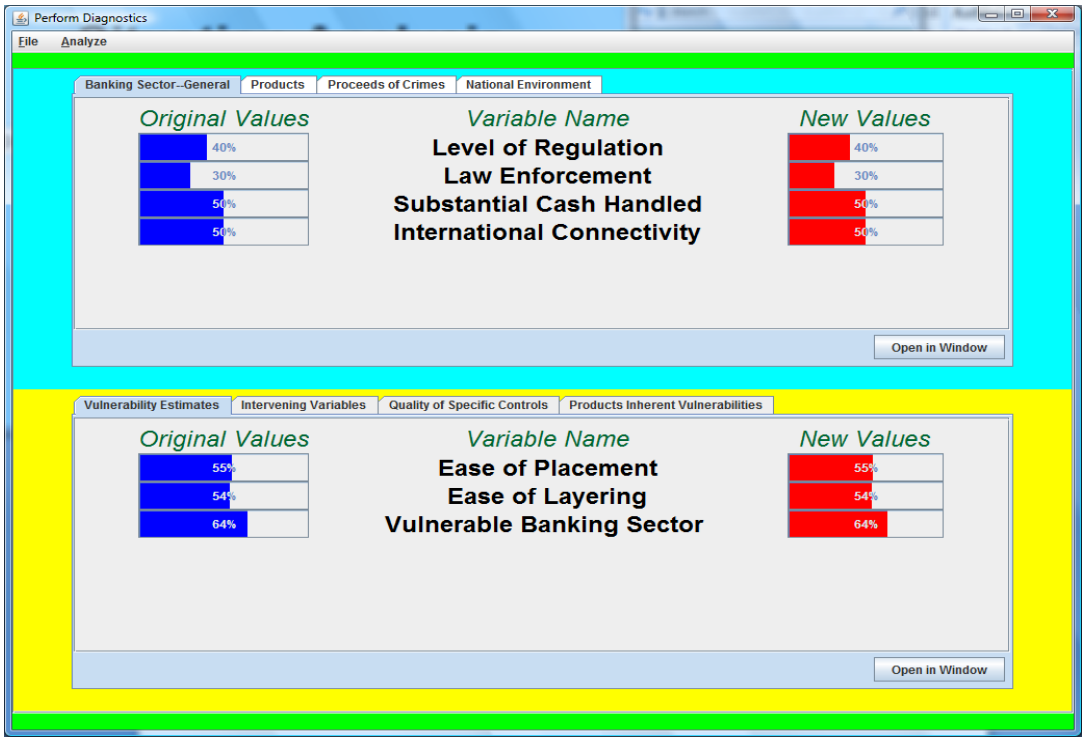

Figure 4: Initial Situation

Now assume that the user updates the likelihood of strong law enforcement to 65%. (see Figure 5). Note that the probabilities for all dependent variables in the bottom half of the

screen have now been updated. For example, the likelihood that the banking sector is vulnerable decreases to 57%.

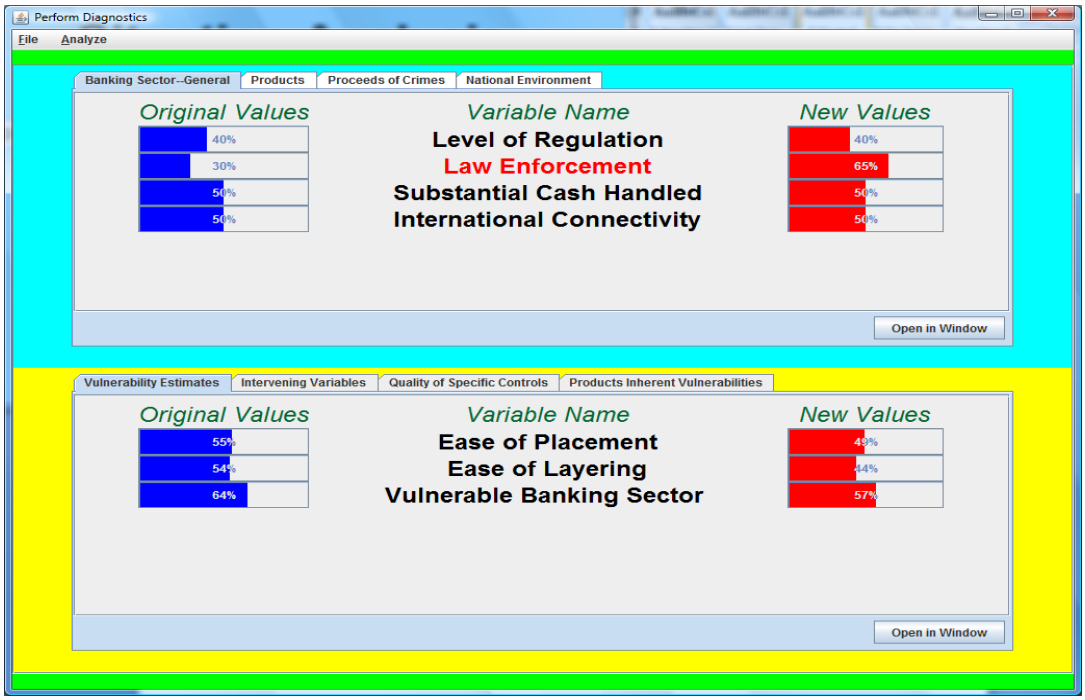

Figure 5: The situation after the change to law enforcement

4. Conclusion

Risk modeling involves considering the context of the risk and the perspective from which risk is to be calculated. Bayesian networks provide an intuitive yet robust mechanism to understand many factors that contribute to risk. A major utility of developing a probabilistic risk model is that it would enable one to calculate the differential impact of various possible interventions on the risk level in order to help guide where to place resources and effort most effectively.

References

1. Pearl, J. 1988. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference.*

2. Campos, E. (Editor), Pradhan, S. (Editor). 2007. *The Many Faces of Corruption: Tracking Vulnerabilities at the Sector Level*. The World Bank.