Risk Based Approach to Critical Infrastructure Protection

Kamal Thalib

Introduction

In 2005, I was the first Loss Prevention Manager for The Ritz-Carlton Jakarta. The hotel was nearing its completion when I got on board and I was part of the opening team. It was the first time that I work for a hotel. I didn't stay long at The Ritz-Carlton, I was there only for about a year and then I moved on.

Around two years before my employment with The Ritz-Carlton, 05 August 2003, a car bomb exploded outside the lobby of the JW Marriott, just across the road; a dozen people died and dozens other were injured. It was the first time that there was such terrorist attack in Jakarta. A year before the Marriott bombing, on 12 October 2002, Denpasar experienced its first terrorist attack, the one with most casualties to date in Indonesia: multiple bombings, hundreds died and hundreds other injured. I was working security when our way of life was changing because of these horrific events.

Back then the approach to security was still straight forward. We were expecting somebody to attack us from the outside, such as suicide bombers with their explosive vests or a vehicle borne improvised explosive device or a VBIED, a car bomb. We put physical barriers up front, gates, vehicle inspection points, personnel inspection points with walk through metal detectors, and explosive vapour detectors; no X-rays deployed at that time as our assumption at the time was that somebody will come in with a bomb and attack us and this is what we were mitigating against. This view became the norm for most of the hotels and office buildings.

Didn't anybody ever consider any other scenarios? Consultants, security groups, and many others have discussed many other scenarios of attack. "What if" scenarios and how would you mitigate them. For example, what if the attackers took apart their bombs, snuck them in piece by piece, and then reassemble them in the toilet and attack from the inside? Nobody really had an answer then and there was no historical data that such an attack ever happened or any information that it could happen.

After the 2002 Bali Bombing and the 2003 Marriott Bombing, on 9 September 2004, a car bomb exploded outside the Australian embassy in Jakarta, killing 9 people, injuring more than a hundred, and shattering the glass of surrounding buildings. On 01 October 2005 Bali experienced its second terrorist attack, suicide bombers with explosive vests attacked tourist areas killing 20 people and injuring 100 others.

Within those 4 years, the methods were either VBIED or suicide vests, until 17 July 2009 when the terrorists actually checked into a room, snuck in the parts for the IED piece by piece with help from somebody in the inside, and assembled it there. The suicide bombers exploded the IED inside the lobby of the JW Marriott and the restaurant at The Ritz-Carlton Jakarta, there was an underground tunnel connecting the two hotels. The unthinkable happened and it changed how we perceived hotel security.

Actually, calling it the unthinkable is incorrect as somebody somewhere may have thought of it but the feasibility or the probability was deemed as low at the time, and herewith lies the challenge.

Risk Management

Merriam-Webster defined risk as “possibility of loss or injury”; loss could be a result of action or inaction. Generally, if we are talking about possibilities of things that could lead to loss, it is endless and with the limited resources that we have we may not very well be able to manage them all.

Before we go to any risk management strategy, we would first want to know what threats that we are faced with. It could be as simple as listing them down. How many? It could stretch as far as your imagination. It could be from a building fire to a nuclear meltdown, a bank rush to a full on economic fallout, an earthquake to a mega quake, a terrorist attack to a full scale invasion, a pandemic to a full blown zombie apocalypse.

We may think that a zombie apocalypse scenario is ridiculous but if we think about it, there are multiple scenarios in there that could be used for emergency preparations, crisis management, and even business continuity planning. In 2014 there was actually a bit of news coverage on “CONOP 8888” when the Pentagon actually used the zombie scenario as a fictional training tool. The CDC actually still has a page dedicated to zombies, because of its usefulness to educate people on preparedness.

Now that we have our list of possible threats, now we will need to assess them. In classic risk management, risk is a product of probability and impact, usually known as well as severity. It is a two dimensional model which could be turned into a matrix. We could use a numeric scale or other scales to rate from low to high probability and impact.

One of the ways how probability could be measured is by historical data or frequency of it happening. We could say that once in every 5 years is considered low probability and once a year is high, but this will depend on the organization of what is perceived as low or high. There are other ways of measuring probabilities, for example if we are talking of a terrorist attack we could look at the attractiveness of the target, e.g.: using historical information or other intelligence, and its vulnerability, e.g.: through security assessments, and use a scoring or a matrix to see whether or not it has a high probability of being attacked.

For impact or severity, it’s usually broken down to economical, reputational, and people. If the institution is governmental, you may want to consider political impact which is sometimes the same as reputational. The economical impact of an attack is the financial loss which could be measured in dollars and cents. Reputational is how we are perceived in the eyes of the public, it could be a loss of trust for example; not just the public, it could also be from the government or regulators. Loss of people is usually attributed to death or injury, but at times it does not have to be so bleak, it could also be how key people are unable to come to work because of a major flood. This could also be presented as a scale, how low or high an impact is would depend on the organization’s risk appetite.

We will need to assess each threat of its probability of happening and its severity when it does. In doing this initial exercise it is best to look at it inherently, without thinking of the mitigations or interventions that we have in place. In other words the gross risk that we are faced with prior to our mitigation plans. As we have two coordinates now, the probability and the impact, we could map it out in a two dimensional risk matrix. There are many ways of how we would map this out, how low, medium, or high is perceived will again depends on the risk appetite.

The risk map is a useful tool to prioritize your risks. We could even use a three dimensional risk map, adding another dimension such as how well we could detect a particular threat or event. We are then able to see, based on our assessments which ones are low risk, which we could put aside, and

focus on the medium and high risk. For example, a threat with low impact but high probability and high impact but low probability could be seen as a medium risk; medium probability and high impact would be seen as high risk; we would want to put our resources to mitigate these risks.

Risk Treatment

With risks in most cases we could not eliminate them because there is no such thing is zero risk, well unless you are able to avoid that particular activity completely that is, meaning not doing the particular business or product. At most times we are looking at reducing or mitigating the risks, trying to reduce the impact or the probability of it happening. We could share or transfer the risk such as by outsourcing it or having insurance, or that we are comfortable with a particular risk that we decide to accept it.

The protection to our facilities, the design, policies, procedures, should take these risks into considerations. The concept of deter, detect, delay, respond, or permutations of that concept is a way to mitigate security risks. There is also crime prevention though environmental design to built in those mitigations into the facilities. There are many methods to do this, but again our resources are limited so we will need to prioritize which risks that we want to spend our resources upon. One may want to focus first more on the medium and high severity but with a higher probability of occurring. Those with low probability but with high impact may come second.

The availability of resources may come as a challenge as there is a finite amount of it. This could eventually drive the decision whether the risk is worth the gain that the activity provides; if it is then there should be an effort of putting more resources to manage those risks.

Take into consideration the story that I had given earlier. From 2002 to 2005, the major terrorist attack in Jakarta and Bali involved VBIED and/or explosive suicide vests. There is historical data to back this up and if my facilities are part of those attractive targets I would actually put the effort to make those facilities harder to attack, target hardening, making it less vulnerable and less attractive. But there is only a certain amount of data that you have, so you may only be able to justify your decisions to certain types of threats.

Another example is the active shooter scenario; take the November 2008 Mumbai attacks, the November 2015 Paris attacks, and the mass shootings that happened in the US. Prior to 2016, we in Jakarta may not have thought of these happenings. But terrorists in Indonesia have a tendency to copycat or to mimic attacks in other places. After Paris I thought that there is a probability that it could happen here in Indonesia. It is not easy to obtain firearms in Indonesia and materials for explosives have become more difficult to obtain over the years, but again that doesn't mean that there is no risk of this happening. The probability may be low, but there is still a probability, we may want to put it up on the map. We may not spend a lot of resources on it, but we could simply start with training for an active shooter scenario and have a procedure if such a situation should befall our facilities. On 14 January 2016, Jakarta experienced its first terrorist attack involving a combination of shootings and IEDs. Though it was not as big as Mumbai or Paris, it was definitely a wakeup call that such attack could occur in Jakarta. They say that hindsight is 20/20, after the incident occurred everything becomes so obvious.

We don't know what we don't know. To be fair, there is only a limited amount of data available to us to drive a decision. We may have gut instinct or even psychic visions, but it is difficult to justify our decisions if we are unable to utilize verifiable information. Risks are instinctive but we will need to do the research and assessment in order to verify those risks and hence be able to mitigate them.

The more accurate the data, the more accurate the risk calculation, therefore better resource management.

No matter how well we could identify the risks and mitigate them, unless we avoid the activities entirely, there is no way that it could go all the way down to zero. There will always be a residual risk, meaning that the risk that we are mitigating against could still happen albeit with lower probability and/or lower impact. This residual risk, if it's low enough, will usually be accepted. At best, we may be able to manage up to 99% or even to 99.9%, but there is still a 1% or a 0.1% chance that it could still happen.

We may have done all we can to reduce the probability ad/or the impact of the said risks, we may have put systems and procedures in place, put manpower, electronic detection and so on but now we still need to prepare on what to do if it does occur.

Emergency Response and Business Continuity Planning

Every organization should have emergency response, crisis management, and business continuity planning. Though these terminologies at times are used interchangeably, they are not the same thing. An emergency may not necessarily be a crisis, but it could if it was mismanaged. A crisis does not necessarily trigger the activation of the business continuity plan if it does affect the four pillars of business continuity, i.e.: loss of workplace, loss of infrastructure, loss of data, and loss of people.

The emergency response scenarios should be based on the risks that we have identified, e.g.: earthquake, floods, fire, blackout, terrorist attack, etc. Emergency response is part of the mitigation to reduce the severity of an incident during the event itself because at this point whatever risks that we have on our list is already happening.

Prior to 2016, perhaps most of institutions in Jakarta would not even thought of having an active shooter scenario as part of their emergency planning, but now perhaps more organizations would consider it. These emergency scenarios should not be static; they should be reviewed regularly to include emerging risks. Your business continuity scenarios are also affected the same way.

The goal of business continuity, ideally, is to have business as usual at any given situation. That is the golden standard of business continuity but then again depending on the resources you have these standards could be a luxury that we may not have. For example: not every business could have identical facilities on different locations providing the same service so if when one is down the other could take up the load until the business resumes on that facility. Take power plants, if one is down, would another power plant be able to provide 100% power to the city? Usually, this is not the case. There will be load sharing and scheduling, prioritizing which areas would receive electricity. Well, at least that was what I have experienced so far. This is a continuity plan to ensure at least that there is still some power to the city. Not a single point of failure, there is a backup plan.

Loss of power is a common occurrence where I'm from. Most buildings have their own generators. This has become the norm. It is an example when we have an unstable infrastructure and the mitigations have been embedded in our daily lives. How often that there is a blackout in our area and how long? But this has gotten better in the past five years or so, we don't get blackouts as much as we used to, at least in the Greater Jakarta area.

Floods are not an unusual scene in Jakarta. Our facilities may not be affected by the flood itself, but our employees are and they are unable to come to work. This would affect the facilities' operations significantly if there are a lot of the employees affected and they happened to be key personnel. A loss of people scenario does not necessarily have to mean that the person died, but a number of key

people are unable to come to work. In this scenario, the organization may want to explore how the knowledge and the workload could be taken up by a number of staff.

There are some events are so widespread and so severe that there is little that we could do in terms of emergency response and business continuity. These are the black swan events, they are rare but devastating, the unexpected ones or those that even if we have considered them there is no feasible way of mitigating them; such as the Aceh Earthquake and Tsunami 26 December 2004 and the Tohoku Earthquake and Tsunami 11 March 2011. We still may be able to manage some aspects of the threats with what information and resources we have. As there is a history of the event, we could actually learn from it and include it in our risk assessments.

Conclusion

There are many methodologies of risk assessments, but our assessments of risks are only as good as the accuracy and updated information that we could have. At most times we could only have secondary information that is readily available to us from public sources. Sometimes we have that information because we own it or we are able to do our own field surveys and find out the information first hand. We use the information that we have to map out our risks in doing our business. Risks are not static, they change. It is quite important to review them regularly and include emerging threats.

There is also a finite amount of resources therefore its allocation will need to be based on priority for mitigation. Even after mitigation there will still be a lower probability of the event occurring. We also have to put this into consideration by putting them into emergency response, crisis management, and business continuity planning.

We manage our risks based on what we know or what we could find out to the best that we can with the circumstances presented to us. Plan the best that we can because if not then we have already failed, “Failing to plan is planning to fail.”