Feature

Ataraxia and Premeditation as Elements of Judgment in the Risk Analysis Process

David Eduardo Acosta R., CISA, CISM, CRISC, BS 25999 LA, CCNA Security, CHFI Trainer, CISSP Instructor, OPST, PCI QSA, is an information security consultant and a lieutenant of the National Army Reserve of Professional Officials of Colombia. Currently, he works with Internet Security Auditors in Barcelona (Spain) and is the principal editor of PCI Hispano, a Spanish web site focusing on Payment Card Industry Data Security Standard. He can be reached at *dacosta@ieee.org.*

También disponible en español
www.isaca.org/currentissue

On 11 September 2001, at 8:46 a.m., as part of a premeditated terrorist attack, an American Airlines airplane crashed into the North Tower of the World Trade Center (WTC1) in Manhattan, New York (USA). At 9:03 a.m., (approximately 17 minutes later) and under the stunned watch of thousands of people, a second airplane (this time from United Airlines) crashed into the South Tower (WTC2). On that day, no previously defined emergency or contingency plan was 100 percent effective. Hundreds of businesses (the majority of which were law firms, banks and stock exchange operations) declared bankruptcy and many others could not recover. Some because they did not have a business continuity plan; others because this plan was based on a redundancy/backup plan with a main hub in one tower of the WTC and an alternate hub in the other; and others because they simply did not assess the possibility of this threat occurring and opted to assume the risk, presumably forgetting that this was not the first attack that these buildings had undergone.

Today, more than 14 years after this event, the side effects and failures caused as a result of this terrorist attack are presented as clear examples of the strategic faults in the definition of disaster recovery planning (DRP) and business continuity planning (BCP).[1] However, can one foresee such actions? Is it really necessary to identify these devastating and almost impossible scenarios to establish an optimum and effective strategy for the continuity of the organization?

In 2011, Eran Feigenbaum, security director of Google, described in an interview, "...part of our disaster recovery plan is to assume that the worst of it has occurred. In last year's scenario, Google was attacked by aliens and California was erased from the map. We asked ourselves: What will we do? How will we maintain the execution of our infrastructure? ...."[2] In July of the same year in Bristol (England), the local town hall presented its contingency plan for handling zombie outbreaks, in which it defined a series of actions in case of infections or pandemic outbreaks that convert humans to the "living dead," detailing the necessary equipment, knowledge, training and preventive actions focused on the minimization of potential damage that could be caused.[3] Along the same lines, in Las Vegas, Nevada, USA, a paramilitary organization called the Zombie Eradication Response Team (Z.E.R.T.) has been created, which offers asymmetric military war training to its members to respond in the event of a zombie apocalypse.[4]

The previous examples present two extremes. First, those who did not assess the potential risk of devastating and statistically unlikely actions that did, in fact, happen, and second, those who prepared themselves for these acts, investing time and money, but who will most likely not see a return on investment (ROI) given the implied uncertainty of the occurrence of these risk. So, which of the two approaches is correct in order to avoid surprises and be prepared for the possibilities, minimizing losses and guaranteeing continuity of services?

THE ATARAXIA OF EPICUREANISM AND THE PHENOMENON OF POSITIVE THINKING

In ancient Greece, Epicurus of Samos (341 BC–271 BC)[5] founded one of the most important schools within philosophy: Epicureanism. Under this doctrine, the purpose is the search for happiness through pleasure (hedonism) and the rejection of all pain.[6] His thinking can be summarized in the following way, "Of two evils choose the lesser, of two goods the best," indicating that the human being is predisposed, by nature, to cling to positive thoughts and reject and isolate those thoughts that can cause pain or suffering. Through the application of these mental exercises, the individual is able to diminish the instability caused by desire, devoting him/herself to the enjoyment of the pleasures under an environment of emotional imperturbability, also known as

ataraxia, very similar to the equanimity (called "Upekkha") sought by Buddhists.[7]

Currently, this philosophy has permeated multiple contemporary schools of thought within which positive thinking is found, which is the basis for a multitude of books about self-improvement and emotional improvement. In general, many psychological treatments and self-help methodologies, such as those based on Neuro-linguistic Programming,[8] attempt to realign any behavioral deviation directed by negative thoughts by making the patient try to visualize and mentally project positive ideas into their future (optimism) and facilitating their way to happiness by overcoming these pessimistic thoughts. Many studies have been carried out thereon, including those by Martin Seligman and Mihaly Csikszentmihalyi,[9] in which the advantages of these methodologies have been converted into the theoretical and practical foundation of a new psychological school of thought called Positive Psychology.

This type of thinking also governs human decisions at the time of anticipating potential risk and preparing for the definition of controls for their future management. The disadvantage arises when, under this perspective, there is a skewing of the holistic vision of the risk and a focus of efforts only on less negative scenarios, fully excluding those which, at first glance, are catastrophic or unlikely due to the subjective critical sense—aligned with positive thinking—used for this analysis. As a result, decision making is framed in a predefined mental model composed of a subset of exclusively positive alternatives. If this model gets out of control when, for example, a previously excluded risk occurs, one can enter a phase of frustration, guilt and depression because of the idealization of expectations based on the idea that everything will be okay. This vision has been profoundly analyzed by Barbara Ehrenreich in her book *Smile or Die: How the Relentless Promotion of Positive Thinking Has Undermined America* and applied to the media manipulation carried out through positive thinking.[10]

STOIC PREMEDITATION AND PROBABILISTIC DARKNESS

The Stoic movement, led by Seneca (4 BC–65),[11] developed a mental exercise named *praemeditatio malorum,* or premeditation of misfortunes, which consisted of a rational principle and purpose for the preventive identification of future events, leaving aside any human emotion. Using this technique, the individual:

- Mentally places him/herself in the most negative scenario possible without considering the interference of any probability (first premise)
- Considers that all possible evils occur as if they were happening at that precise instant (second premise)
- Based on this environment, defines the potential controls that are considered necessary to address in the event that the scenario becomes tangible, preparing the mind in advance to face adversity without intending to withhold or justify it (third premise)

This first theoretical exercise of anticipation of thinking based on assumptions was called *malete* by the Greeks, with reference to meditatio (meditation).

The second part of this mental exercise is known as *gymnasia* and involves practical training to address such situations in real life, even if they have been artificially induced.[12] Both *malete* and *gymnasia* make up part of askesis, or exercises for the development of knowledge though maxims *(dogmata)*.[13] In other words, through the use of techniques of *praemeditatio malorum*, one can meditate rationally on the impacts and results of future events and anticipate shaping the actions that will be undertaken if these events really occur.

However, if this technique is taken to the extreme, it usually carries with it a series of disadvantages. Since the exercise is based on a mental location in catastrophic scenarios, without proper contextualization, the individual can develop offensive actions or exaggerated defenses in normal scenarios with a large stress load. Michel Foucault said it well: "The meditation on death is the culmination of all these exercises,"[14] indicating that there is no sense in trying to anticipate certain things. Due to this, it is necessary to clearly define the thresholds of action under which the exercise will be developed.

INFORMATION SECURITY AND THE RISK ANALYSIS AND MANAGEMENT PROCESS IN A RATIONAL CONTEXT

The dichotomy of the philosophical exercise of mental preparation has been presented—that which is based on positive elements (ataraxia and positive thinking) and the other on negative elements *(praemeditatio malorum)*—showing their advantages and disadvantages, especially when these practices are taken to the extreme. The intention is not to discredit these ways of thinking in any way. To the contrary, the purpose is to take the virtues of each one of these mental exercises, allowing true critical objective thought to develop at the time of identifying future risk, focusing on the area of information security, a field with a high level of uncertainty.

One of the key elements in information security is the risk analysis process. This activity attempts to identify the potential future risk that could affect the assets of an organization and, based on this, to proceed with the establishment of a series of actions focused on its management. This estimation is carried out through the identification of the assets of the environment, the analysis of the magnitude of the potential impact or loss, and the probability that this damage could occur. Due to the particular case study of this analysis in which there are no specific values, such as a specific figure or number, the variables that affect this evaluation are often estimated subjectively. It is precisely here where the human element can be influenced by either of the two previously described behaviors (ataraxia and premeditation), which can imply overestimating or underestimating in decision making.

Similar to any other activity that entails the preparation for future events, the mental exercise of staging in information security is indispensable. Questions such as, "What would happen if...?" or "How would you act if...?" are fundamental to defining a security strategy in an organization and are common elements in selecting alternatives for risk management as a result of a correct previous identification. If this risk identification fails (for being too lax or pessimistic), the risk management process will be impacted, leaving the organization at the mercy of potential negative situations without an associated response or an evaluated investment.

Combining the Epicurean and Stoic models described in the previous sections, each of the phases of the risk analysis process is analyzed from a rational perspective, describing which parts of each tendency can be applied, as a referential model in this process. The key in this process is to minimize as much as possible any emotional interference arising in the individuals associated with the process to maintain a holistic view and critique, avoiding the placebo effect of positive thinking and the excessive pessimism of Stoicism, and balancing both elements according to the cost/benefit for the organization according to the following steps:

- **Identify and list potential threats**—In this phase of the process, the recommendation is for the person or persons responsible for the analysis to start by performing a mental exercise based on the three Stoic *malete* premises, mentally placing themselves in the worst possible scenario and listing any threat visualized, no matter how irrational it may be, so as not to discard any threat and leaving aside any emotion that may arise as a result of the identification. This task is essential since it is the basis for all actions that will result in the definition of a holistic and effective framework.
- **Mentally visualize the impact caused by the identified threats**—Based on the previous results, for each of the threats found the impact must be defined in the event they occur at the present time. Again, do not discard any result without considering any associated possibility (for now).
- **Incorporate and create a threat catalog**—Based on a detailed analysis of all identified threats, try to define common characteristics among them that allow them to be cataloged according to the type of asset they affect; the administrative, logical or physical dimensions impacted; and any other criteria deemed necessary, and group them based on these common elements.
- **Put the results in a current context**—Having defined a threat catalog, the next step is to apply an objective filter and introduce the real and current variables of the process, which allow granting a determined value to the associated degrees of uncertainty: historical behavior data for each threat in the organization (if they exist), benchmarking analysis results extracted from comparing the risk of the organization with other similar entities, etc., which will allow the rational factor to be added to the result. At this point, a complete risk inventory will be available (risk = impact × probability). It is in this step that the use of positive thinking may contribute its value as a form of catharsis and equalize the balance.
- **Establish a management strategy**—Taking advantage of the previously developed catalog, management alternatives must be established. For each risk, a decision tree must be created

that describes the actions to be taken to manage it if the risk arises. This action coincides with the Stoic *gymnasia* phase. At this point, similar courses of action among the different risk can be identified with which global actions aimed at simplified management may be established.

- **List behavioral patterns regarding any exception**—Finally, a set of action strategies must be defined in case anything occurs that was unexpected or unforeseen in the identification exercise. The policy to follow in this phase is "no expectations equals no frustrations." Nothing must be taken for granted, nor must risk behavior under an established model be assumed, since it would contaminate the result with subjective elements.

It is important to note that decisions have not been made in any of the described phases. Simply, the universe of risk and alternatives has been outlined as objectively as possible, and subsequently—based on a cost-benefit analysis—the prioritization and implementation of each task should be undertaken. This task should be performed by the management of the organization.

In addition—and to lend a greater level of objectivity to the results—the exercise may be performed jointly by an interdisciplinary team of internal and external persons who must know the basis of the exercise in advance.

A PRACTICAL EXAMPLE

Suppose that due to operational factors within an organization, it is necessary to deploy a new infrastructure of servers in a new data processing center (DPC). Within a standard risk analysis, the starting point would be a predefined bank of threats, including catalogs provided by tools or methodologies and arising from the company's own experience. Nevertheless, the intention is to identify potential threats that can be discarded by the subjectivity of the individual performing the risk analysis and that usually have a high impact and a frequency that tends toward zero—in other words, the highly unlikely, but catastrophic situations that tend to be overlooked due to their uncertainty.

The difference between a standard risk analysis and the model described here comes in the implementation of the supplementary exercise for threat identification on the basis of the worst-case scenario (Stoic *malete*), omitting any emotional restrictions. For this example, a meeting of the interdisciplinary team involved in the project is convened and any participatory tool for group work would be implemented (e.g., brainstorming, brainwriting). The greatest amount of threats that could affect the project would be listed without discarding any of them. Here are some examples:

- Solar storm that affects the operation of the deployed computer systems and their communications and data
- Electromagnetic attacks that could affect storage devices
- Impact of meteorites in the geographical location where the servers will be physically located
- Collateral effects of global warming (floods, freezing of different geographic areas, etc.)
- Massive displacement of personnel
- Terrorist attacks against personnel or infrastructure
- Spillage of dangerous chemical products
- Nuclear attack
- Heavy artillery bombing
- Pandemics caused by unknown diseases and/or the existence of Patient Zero
- Unidentified flying object (UFO) attacks
- Political/legal events such as expropriations and dictatorships

In the first instance, all these threats would be highly hypothetical to a subjective critical position, as their frequency would be close to zero, and it is at this point that the discarding caused by positive thinking would be the action that is intended to be eliminated. The result of this first exercise would have the complement of the standard threat catalog with the new identified threats, organized according to the affected asset or assets, as well as their impact.

The next step is the application of *gymnasia*, where the strategies for facing the previously identified threats are developed, which may include the following:

- Hiring independent private security teams
- Using content replication technology in the cloud
- Deploying an alternative data center in a remote geographical location
- Using analog communication technologies
- Taking out insurance policies with coverage of damages not initially contemplated

The result of this exercise is the definition of management strategies for each of the identified threats, no matter how strange they may be. They must all have an associated preventive action (where applicable) and mitigation plan.

This same exercise can be applied in test processes for management plans of incidents, disaster recovery and business

continuity, since the starting point would be the standard threat catalogs complemented with the application of techniques of *praemeditatio malorum.*

CONCLUSION

The typical postincident cliché assumes that misfortunes are opportunities. Instead, one can methodically prepare using the correct tools to implement a realistic and objective perspective without engaging in unjustified pessimism or optimism in the management of the uncertainty associated with risk. A correct mental exercise in which risk is visualized, completely excluding any emotion arising from the subjectivity of the individual who performs the process, will allow the organization to develop a range of alternatives for the proper selection of strategies, balancing the placebo effect of positive thinking and Stoic excessive pessimism.

ENDNOTES

[1] Virgona, T.; "September 11, 2001: Lessons Learned for Planning Disaster Recovery," Pace University, USA, 8 May 2009, *http://csis.pace.edu/~ctappert/srd2009/e2.pdf*

[2] Swan, G.; "Taken Over by Aliens? Don't Worry; Google Has It Covered, *ComputerWorld Australia*, 22 August 2011, *www.computerworld.com.au/article/398051/taken_over_by_aliens_don_t_worry_google_has_it_covered/?fp=4&fpid=1398720840*

[3] *The Bristol Post*, "How Bristol Would Deal With a Zombie Attack," 7 July 2011, *www.bristolpost.co.uk/Bristol-deal-zombie-attack/story-12896585-detail/story.html*

[4] Zombie Eradication Response Team, *http://zertnation.com/about-z-e-r-t/*

[5] Internet Encyclopedia of Philosophy, "Epicurus," *www.iep.utm.edu/epicur/*

[6] *Ibid.*

[7] O'Brien, B.; "Buddhism and Equanimity: Why Equanimity Is an Essential Buddhist Virtue," About.com, *http://buddhism.about.com/od/basicbuddhistteachings/a/Buddhism-And-Equanimity.htm*

[8] Tosey, P.; J. Mathison; "Introducing Neuro-linguistic Programming," Centre for Management Learning and Development, School of Management, University of Surrey (UK), 2006, *www.som.surrey.ac.uk/NLP/Resources/IntroducingNLP.pdf*

[9] Seligman, M.; M. Csikszentmihalyi; Authentic Happiness, Positive Psychology Center, University of Pennsylvania, USA, *www.authentichappiness.sas.upenn.edu/seligman.aspx?id=157*

[10] Ellmann, L.; "Smile or Die: How the Relentless Promotion of Positive Thinking Has Undermined America by Barbara Ehrenreich," *The Guardian*, 8 January 2010, *www.guardian.co.uk/books/2010/jan/09/barbara-ehrenreich-smile-lucy-ellmann*

[11] Internet Encyclopedia of Philosophy, "Lucius Annaeus Seneca," *www.iep.utm.edu/seneca/*

[12] Robertson, Donald; *The Philosophy of Cognitive-Behavioural Therapy: Stoic Philosophy as Rational and Cognitive Psychotherapy*, Karnac Books, UK, September 2010, *http://philosophy-of-cbt.com/the-philosophy-of-cognitive-behavioural-therapy/*

[13] Olssen, M.; *Michel Foucault: Materialism and Education*, Greenwood Publishing Group Inc., 1999

[14] *Op cit*, Robertson