Towards Cyber Incident Response Strategic Planning

Namosha Veerasamy, Thulani Mashiane , Kiru Pillay

Council for Scientific and Industrial Research

nveerasamy@csir.co.za

+27 12 841 2893

Abstract

With technological advancements and changing environmental conditions, organisations are continually faced with growing uncertainties. Being prepared to deal with uncertainties can help organisations establish good response mechanisms. Should these uncertainties materialise, organisations will be able to address the associated risks, states and outcomes more efficiently. Scenario planning is one such means of preparing for potential uncertainties. The use of descriptive brainstorming can help organisations plan for future situations. In this paper, three scenario planning processes are discussed. As adapted scenario planning design for cyber incident handling is then proposed. The proposed design takes into consideration the focal issues of identifying the critical role players, the communication channels, the response mechanisms and the required skills. This paper encapsulates a consolidated approach to carrying scenario planning for cyber incidents. This aims to provide a more co-ordinated effort that addresses the main responsive actions that should be carried out by stakeholders during major cyber incidents.

Strategically planning cyber incident responses can improve decision making in an organisation. With the use of scenario planning for strategic preparation of cyber incidents, organisations can help shape better outcomes. With scenario planning, organisations can look to understanding the future which is often filled with uncertainty. The future is unpredictable, but strategic planning can help propose plausible futures and outcomes. This helps with risk mitigation, response tactics, and overall planning on how to deal with potential scenarios of cyberattacks. During the process of cyber incident responses, the implications of actions and decisions will need to be assessed. The critical role-players need to be identified, as well as various envisioning aspects of the desired futures. In this paper, a more structured design for scenario planning for cyber security incidents is provided in order to help guide the process.

The paper covers a pertinent topic of cyber incident response handling which is one of the core themes of this conference. The paper aims to consolidate previous approaches of scenario planning and shows how it can be used for cyber incident handling. Overall, the design proposed can help deal with possible future cyber incidents, which are a particularly relevant topic in the field of cyber security.

Keywords: cyber incident handling, scenario planning, cyber incident response

Introduction

The National Institute and Standard Technology (NIST) *Computer Incident Handing Guide* (NIST.SP.800-61r2) (NIST, 2012) proposes the different phases involved in incident response (See Figure 1). The proposed phases are preparation, detection and analysis, containment eradication and recovery and lastly, post incident activity.

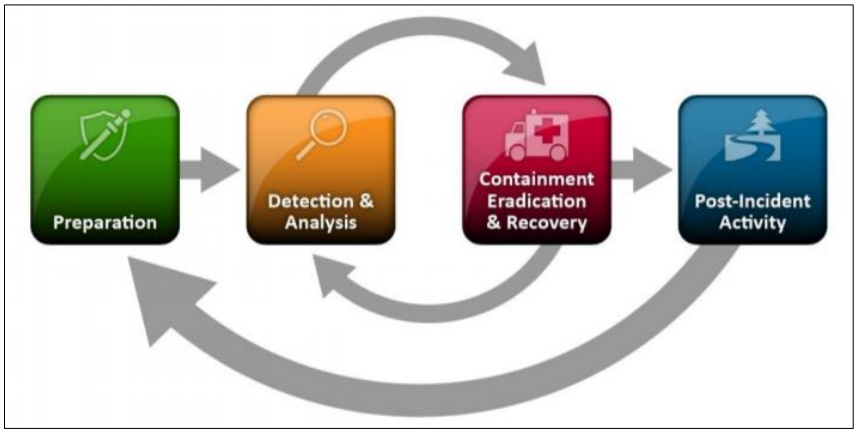

Figure 1 Incident Response Life Cycle (NIST, 2012)

Preparation is where the organisation implements a mitigation strategy based on risk assessments. An important component of preparation is ensuring that the skills level of the response team is adequate to respond to cyber incidents. Following preparation, detection mechanisms must be put into place. Early detection of an incident can result in the minimisation of the impact that the cyberattack has on the organisation. After an incident is detected, efforts must focus on the containment, and applying solutions towards recovery from the incident. During the attack the response team typically rotates between detection and recovery. This is done because the response team must monitor the effects of applying solutions, as well as look out for new behaviour due to the incident taking place. After recovery, the organisation must document the incident, the steps taken to recover from the incident, as well propose steps to be taken to mitigate the incident in the future. This must be recorded into the organisation's incident response plan. An incident response plan is a set of instructions to the Information Security staff and other stakeholders on how to act before, during, and after a cyber-security attack. It needs to address how to deal with a wide array of cyberattacks such as cybercrime, service outages, and data loss. According to Farhat, McCarthy, Raysman and Knight (2011), the important sections of an incident response plan are 1) description of the response team and the associated responsibilities for each member 2) a description of how incidents are reported 3) steps on how to initially respond to an attack 4) the investigation procedures 5) the recovery implementation, 4) steps on informing the public and lastly 5) the involvement of law enforcement, if necessary

To help organisations prepare for an incident, the current paper explores the scenario planning approach as a possible strategy for addressing incident response.

Scenario planning provides a means of ordering perceptions about how the future may play out and determining what strategic decisions today offer the best chance of success tomorrow (Global Business Network, 2008). Through the scenario planning process, assumptions and wider possibilities can be considered in order to identify specific risks and opportunities. For cyber incidents it is important, as it helps identify a critical threat and organise responsive action in order to mitigate the threat. Response actions may be applicable to a number of cyber incident examples and thus scenario planning can help plan for multiple futures. The strategic thinking carried out during scenario planning can thus help prepare an organisation for a variety of cyber threats.

Scenario planning allows for the exploration of plausible futures. The forecasting that is carried out during scenario planning can help provide foresight with regard to potential future situations. Foresight is seen as (Conway, 2003):

- an attribute, competence or process that attempts to broaden the boundaries of perception
- assessing the implications of present actions, decisions, etc.
- detecting and avoiding problems before they occur (early warning indicators)

- considering the present implications of possible future events (proactive strategy formulation)
- envisioning aspects of desires futures (normative scenarios)

It enables strategic thinking, planning and development, in order to synthesise various choices, and then implements a suitable strategy in order to move towards a desired outcome. In the realm of cyber incidents, this is particularly relevant, as strategic thinking about an impending attack can help prepare and defend an organisation. Organisations can look at the trends or drivers that lead to cyber incidents and then develop more co-ordinated response procedures. In this process, issues, challenges and communication requirements can be formulated. Collectively, various stakeholders can collaborate to take individual foresight, and combine efforts to create a mutual strategic approach.

Scenarios are very helpful for strategy development, innovation, risk management, visioning and executive learning (Pastor, 2009). Through the use of scenario planning, voluntary adaptation and responses can be carried out. This can promote more welcome changes and make organisation more risk conscious.

The use of descriptive narratives in the form of scenarios can help describe a range of possibilities for future situations. The aim is not to be predictive but to take a predatory stance and so build a framework that can help guide response to critical events that can affect the organisation. This is particularly important as scenario planning can identify the key competencies, role players, and communication that is required in order to resolve a cyber incident that may be affecting an organisation's ability to operate.

Applications and benefits of scenario planning include:

- Shareholders can hold a shared vision
- Allows for creative thinking
- Innovation due to anticipated requirements
- Understand implications for strategic decision making
- Strategy and choices can be more sustainable due to consideration of driving forces and trends
- Minimisation of risk and identifying early warning signs

"Scenarios are stories. The reliability of (their content) is less important than the types of conversations and decisions they spark"- Adri de Geus, The Living Company (Global Business Network, 2008). The outputs of scenario planning may not necessarily be explicit decisions, rather constructive ideas, and recommendations, whereby facilitation is achieved.

Various scenario planning methodologies have been proposed and modified.

This paper summarises three mainstream approaches before proposing an adapted design for cyber incident scenario planning. The outline of the paper is an initial background to scenario planning methodologies, followed by the proposal of an adapted design and the discussion thereof.

Background

The initial research of compiling an approach for co-ordinated cyber incident handling looked at existing scenario planning processes. Three main processes were studied and are as follows:

- Mats Lindgren and Hans Bandhold while working at company Kairos Future wrote a book "Scenario Planning the link between future and strategy" (Lindgren & Bandhold, 2003)

- Royal Dutch/Shell organisational approach to scenario planning (Royal Dutch/ Shell Group, 2005)

- Peter Schwarz who describes the process in the book "The art of long view" (Schwartz, 1998)

In the next section, the main points of each of the three processes are discussed. Thereafter, the three different processes are summarised and a short discussion follows on how they compare to each other. The adapted design of cyber incident response planning is then proposed.

Schwartz's scenario planning process

The first process was developed by Peter Schwartz in 1991. His career was based on scenario planning. He wrote various books about scenario planning strategies, the first of which was "The art of long view' (Schwartz, 1998). In this book, he explains in a step-wise manner the process of scenario planning. The steps initially proposed by Schwartz are shown in Figure 2 (1998):

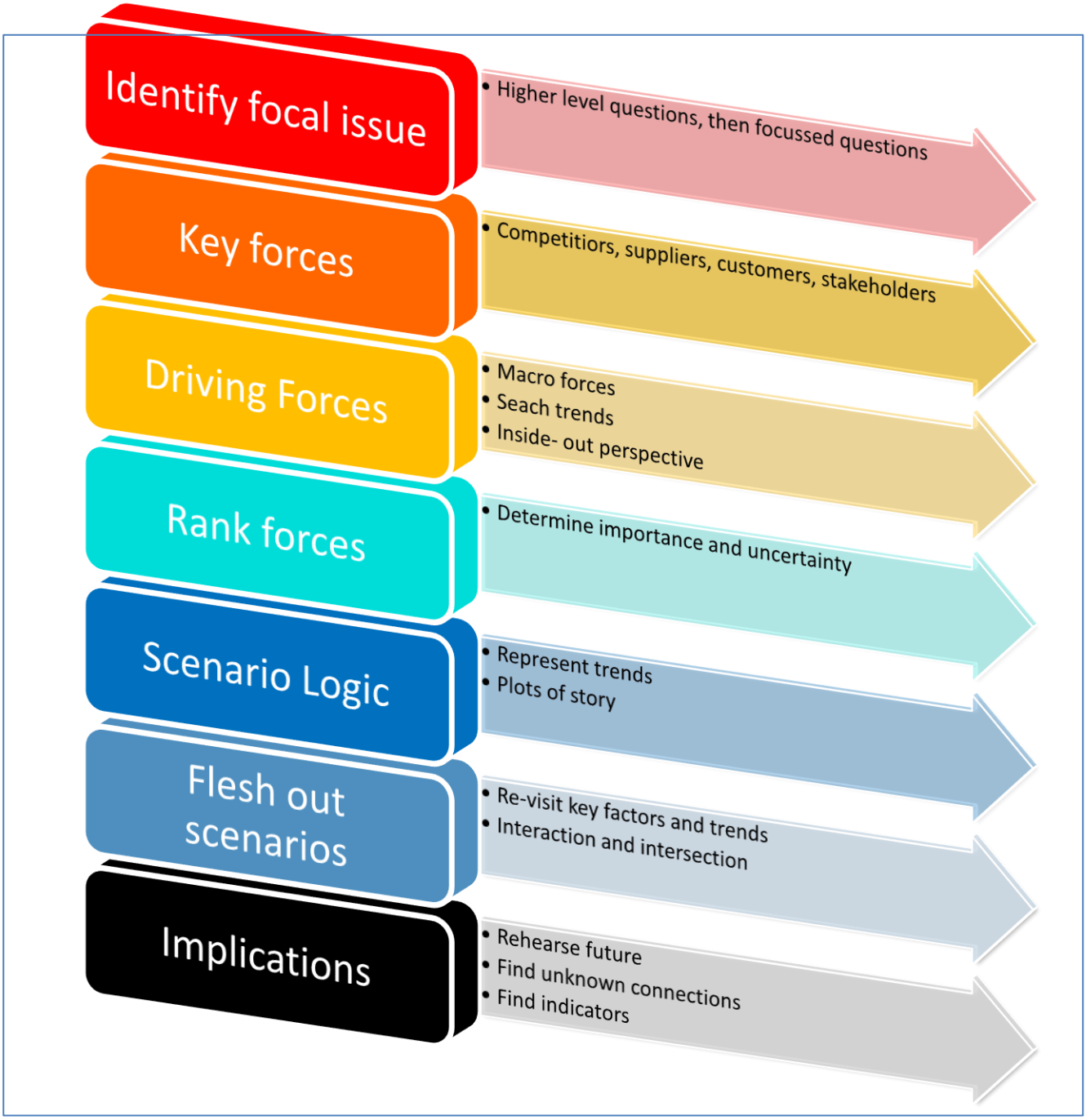

Figure 2: Summary of Schwartz's Process (Own Compilation)

Schwartz's steps start with identifying the focal issue. To do so, broader questions can be initially posed and then the ideas need to be narrowed down to find the focal question. Next, the key forces are considered by looking at competitors, suppliers, and customers. Thereafter, the driving forces

are examined. Various macro forces (like social, economic, political, environmental and technological) as well as the micro environment (demographics, public opinion, etc.) can play a role. The various trends are also searched for.

Next, the various forces are ranked to assess importance and uncertainty. In order to craft the scenario logic, the trends are represented in a selected format (spectrum with one trend/axe, Matrix- two trends/axes, and Volume- three trends/axes). The interaction and intersection of these forces are then considered.

During the Implications stage, the future is rehearsed to determine how to respond. The scenario is once more considered, to look for connections that might have been overlooked. Finally, indicators are monitored for.

The next scenario planning process to be discussed is the Shell method.

Shell scenario planning process

The Shell company was one of the first companies to utilize scenario planning as part of its strategic capabilities. Since then it has been developing critical scenarios in order to prepare for changing environmental conditions. Figure 3 provides the main steps in the Shell Method for Scenario Planning. The Shell Method commences with the Preparation stage in which the main purpose of the scenario planning is identified. This entails identifying the main users of the scenario, the expected results, the time horizon that the scenario is valid, and the key responsibilities of the stakeholders.

The next stage is Pioneering, during which the main themes with driving forces and uncertainties are compiled. This helps formulate the focal question. From here, branches are created to form the consequences of uncertainty. The scenario outline is developed and establishes a story with branches of uncertainty.

During Map-making the stories are told. It can be represented in various forms like tables, videos, photos, graphs, and diagrams. The unfolding stories can then be presented to the primary recipients.

The Navigation stage consists of the communication and analyses of scenarios in order to refine them. The scenarios can be critiqued and examined to identify additional inputs.

The last aspect is the Reconnaissance stage during which the future implications are considered. Thereafter, the environment will be scanned for any signals indicating the scenario being realised.

In the next section, a discussion follows on another of the pioneer scenario planning processes from Kairos.

Figure 3: Summary Shell Method (Own Compilation)

Kairos Future

Figure 4 encapsulates the key steps in the Kairos Future approach. There are five main stages: Tracking, Analysing, Imaging, Deciding and Acting, as well as a pre-stage for Preparation. It begins with the definition of the purpose and generation of the focal question. This ties with identifying the key system that will be studied. During the preparation stage, the time horizon for which the scenario planning will be valid for is also identified.

The next step is the Tracking stage in which the trends, driver and uncertainties influencing the focal question are proposed. The trends and driving forces are considered. This helps to predict and anticipate changes in the environment. Different media-based methods and interview methods can be used to gather information about anticipation of changes in the environment. Trends covering various disciplines may emerge.

During the analysis stage, the trends are linked into groups in order to study interrelationships. The Scenarios can then be built using the two most critically identified uncertainties. This helps to carry out the Imaging stage in which a picture is created of the desired future.

Thereafter, during the Deciding stage, various strategies can be proposed and evaluated. Associated terms can be grouped together. This will lead to the implementation of the strategies and the monitoring of any changes that could create an alert for the activation of a scenario.

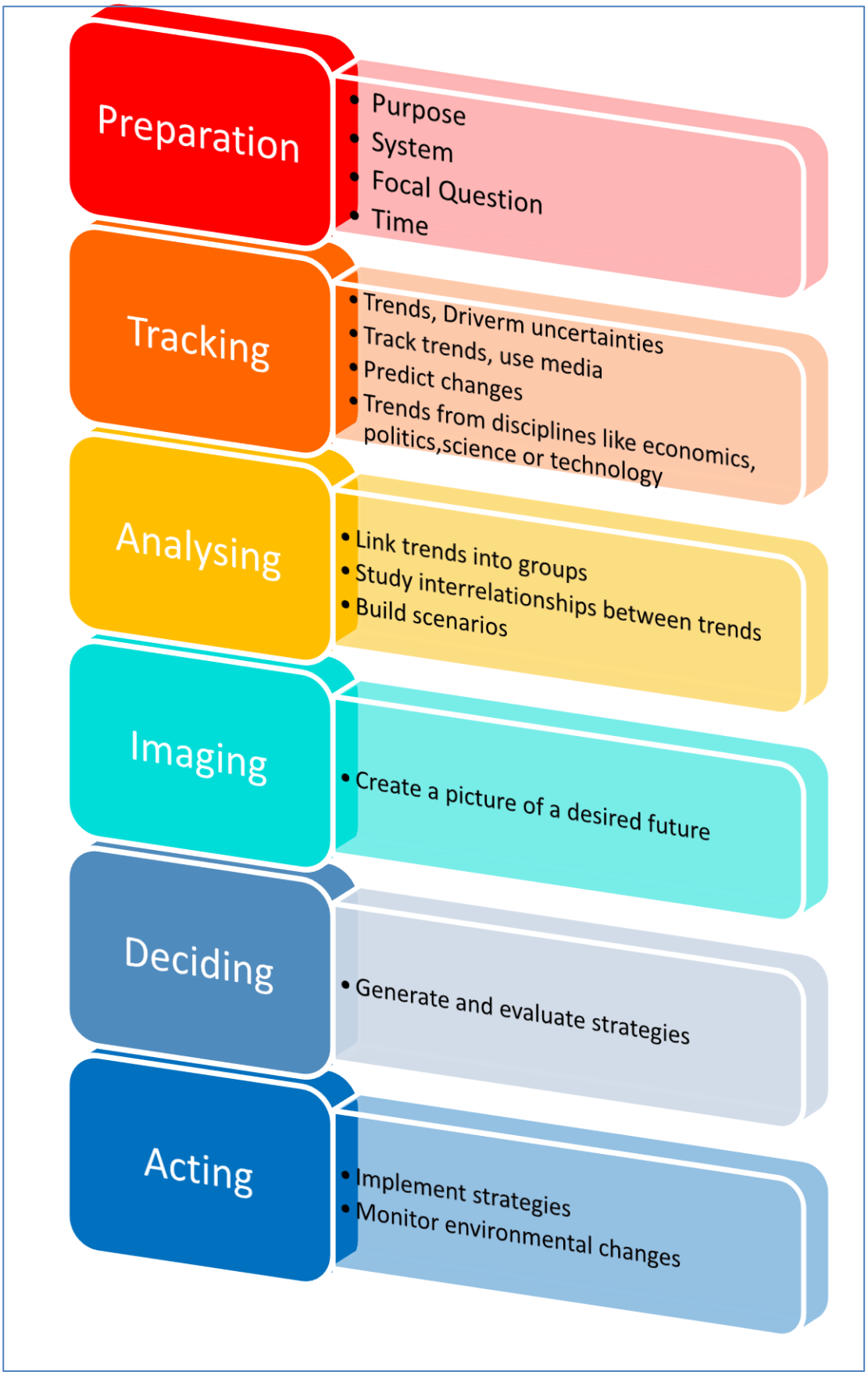

Figure 4: Summary of Kairos Future Process (Own Compilation)

Scenario Planning Process Summary

After an analysis of three scenario planning processes, the core stages and activities were mapped onto each other. This is shown in Figure 5. The different scenarios were compared to each other in order to identify useful steps, lessons learnt, and approaches that can help streamline the process for cyber incident response. The review of the various scenario planning processes found that the context of scenario planning for broad spectrum issues differs somewhat to scenario planning for cyber incident response. For cyber incident response, the macro factor is mainly the technological effects and thus the development of the scenario should be based on the technical and managerial outcomes stemming from these circumstances. However, some fundamental points of mainstream scenario planning can still be applied to cyber incident response. This will be discussed next.

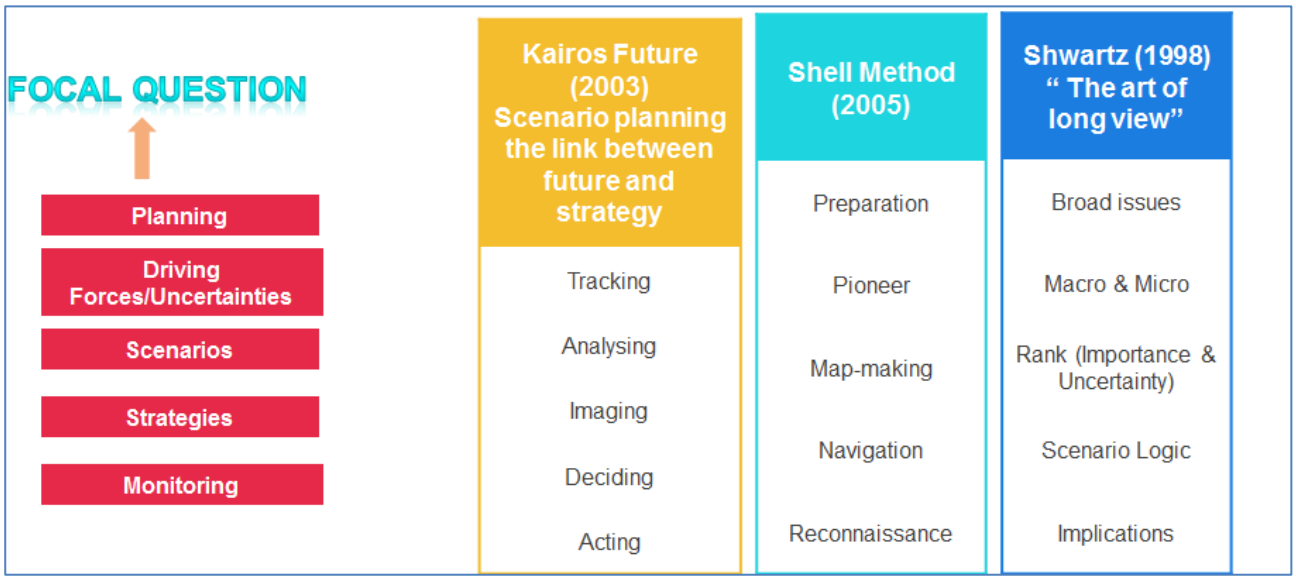

Figure 5. Summary of Scenario Planning Processes

All three analysed processes entailed a form of initial planning. During this stage, the main purpose of the exercise is identified. The broader issues are ascertained and then narrowed down in order to identify the focal question. An analysis of the different scenario planning processes revealed that a key aspect of the process entailed looking at the driving forces, trends, and uncertainties. The effect of macro driving forces are a critical component of the process. Thereafter, the key driving forces and trends forming the uncertainties can be grouped together and rated in order to find the core issues. The scenarios can then be developed through story-telling and consideration of the interaction of the identified driving forces. Strategies can be created based on the navigation of the scenarios. This forms the building of the Scenario Logic. This eventually leads to the monitoring stage whereby indicators of the scenario can be scanned for. This helps to provide early warning by monitoring for environmental changes.

Now that the various processes have been discussed and the main points explained, the discussion moves on to the proposed design for cyber incident response planning. The proposed design was adapted from the three main processes summarised in previous sections.

Adapted Design for Cyber Incident Response Planning

In the context of scenario planning for cyber incident response, strategic planning is required. Therefore, drawing from the various scenario planning processes, a strategic design was proposed that incorporates key aspects relevant for cyber incident response.

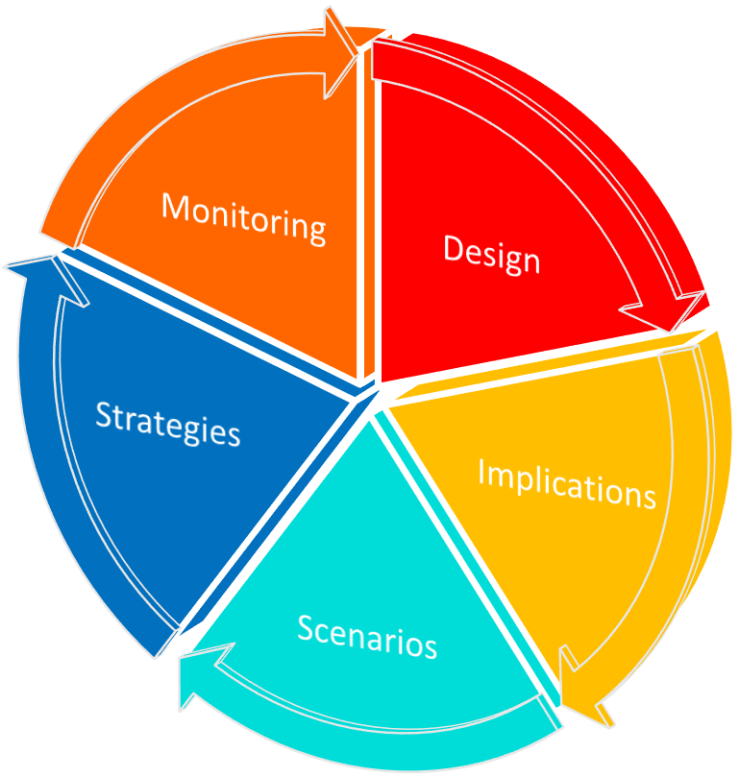

Figure 6. Main Steps for Strategic Cyber Incident Response (DISSM)

Figure 6 shows an outline for the main steps proposed for strategic cyber incident response planning. It is encapsulated as DISSM (Design, Implications, Scenarios, Strategies, and Monitoring). Each of these steps is explained next.

Design

In general a work group should be established that leads the main activities for strategic cyber incident response. Initially the team will commence with some overall design and planning. During the initial design the focal question of the cyber incident response planning will be unpacked. The focal issue represents the question about the future that the organisation is confronting (Pudget Sound Future Scenarios, 2005). Defining the focal question is a crucial part of the scenario planning process as it acts as a conceptual boundary and is a key determinant of strategic intent (Serious Insights, 2010). It helps define what will be explored, researched, and specified.

For cyber incidents, the focal question helps to define more precisely what the intent of the scenario planning will be. After studying the various requirements for cyber incident response, the main focus proposed to be addressed will cover the aspects of the stakeholders, forms of communication, response mechanisms, and required skills. This is shown in Figure 7.

Figure 7. Focal question for Strategic Cyber Incident Response Planning

Typically during the design step, the main parameters and assumptions of the scenario are decided upon. This may entail the scope of a typical attack- attack vector, source, target, initial effects. This will serve as input when determining the implications, and fleshing out of the scenarios and strategies.

Implications

With regards to implications, the process can entail carrying out a PESTEL analysis (see Figure 8). PESTEL is an acronym for Political, Economic, Social, Technological, Environmental and Legal. PESTEL analysis is a strategic framework that looks at the impact of various macro-economic factors that also affect strategic planning (ProcessPolicy.com, 2019).

During this stage, the role-players can identify the possible impact on macro factors (Political, Economic, Social Technological, Environmental, and Legal a). This will help assess the effect of a cyber incident on key macro factors, and whether any additional actions need to be taken to cater for the effect. (PESTEL analysis is comparable to the trends that emerge in Kairos Future approach and Schwartz's process).

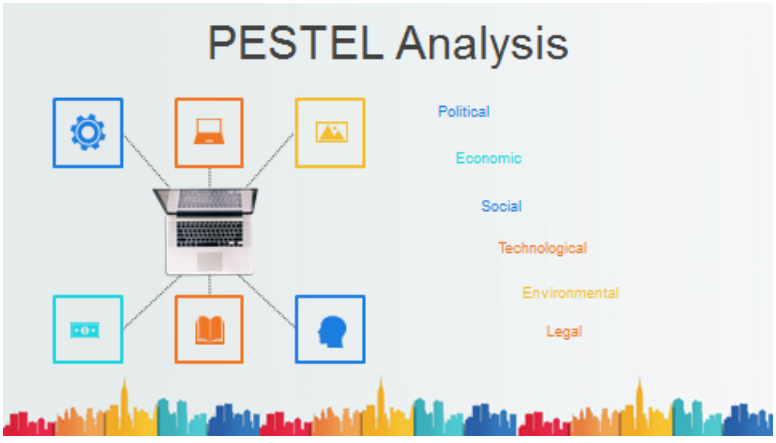

Figure 8. PESTEL analysis for strategic cyber incident response planning

Scenarios- during the scenarios process, the approach would be to convene work groups whereby the various stakeholders discuss response mechanisms and communication protocols. This is a fundamental part of the process as it is here that the key reactive measures and points of information transfer to be adopted can be deliberated upon. Practically, during work sessions, the various scenarios will be proposed and considered in order to find the optimal response actions.

Strategy- One of the main outcomes of the process is the strategies that are devised in order to address the scenario. During the strategy development, new thinking and exploration of ideas can be carried out. This will help make the organisation more risk conscious. The options generated can be evaluated, and implementation strategies formulated. When dealing with various suggestions, strategies can be clustered. This can help find patterns between strategies or classify them accordingly. The participation of key role players is a key aspect of developing the scenarios and strategies. Specialists can contribute as well as stakeholders working in the discipline. It is crucial that the various constraints are considered, as well as looking at the environment from new perspectives. This will help form more innovative solutions. Due to the visionary approach followed, the organisation can prepare for critical threats, as well as identify useful opportunities to respond resourcefully as well.

Monitoring – To close the process, triggers or signals of the scenario will have to be monitored for. This will help alert of the occurrence of the scenario and that we look at the implementation of the devised strategies and response actions.

Conclusion

The current paper presented an adapted design to carry out strategic scenario planning for incident response. The overall goal is to collaborate with critical stakeholders in order to identify the key response mechanisms and communications channels that are required in the event of a critical cyber incident. The approach followed in this research was to evaluate current scenario planning strategies and then design a customized design applicable to cyber incident response handling. In the research the main steps identified to be carried out are termed DISSM (Design, Implications, Scenarios, Strategies, and Monitoring.) It is envisaged that this adapted model can be used to plan and prepare strategically for cyber events that have the potential for larger-scale impact. The scenario planning approach is aimed at helping decision making and response preparation.

References

1 Bibliography

Conway, M., 2003. *An Introduction to Scenario Planning.* Foresight Methodologies Workshop: Thinking Futures.

Farhat, V., McCarthy, B., Raysman, R. & Knight, L., 2011. Cyber attacks: prevention and proactive responses.. *Practical Law,* pp. 1-12.

Global Business Network, 2008. *Introduction to Scenario Planning.* s.l.:Monitor Group.

Lindgren, M. & Bandhold, H., 2003. *Scenario Planning: the link between future.* New York: Palgrave Macmillan.

NIST, 2012. *Computer Security Handling Guide: National Institute of Standards and Technology Incident https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf?inline=true.* [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf?inline=true
[Accessed 18 April 2019].

Pastor, F. M., 2009. *Exploring Scenario Planning Process- Differences and similariies.* s.l.:Lund University.

ProcessPolicy.com, 2019. *What is PESTLE Analysis?.* [Online]
Available at: https://processpolicy.com/pestle-analysis.htm
[Accessed 10 April 2019].

Pudget Sound Future Scenarios, 2005. *Scenario Bulding.* United States of America: s.n.

Royal Dutch/ Shell Group, 2005. *Shell Global Scenarios to 2025 - The Future Business Environment - Trends, Trade-offs and Choices.* s.l.:s.n.

Schwartz, P., 1998. *The art of long view: Planning for the future in an uncertain world.* England: Wiley. First edition published 1991 in the USA by Doubleday..

Serious Insights, 2010. *Scenario Planning: The Focus of the Scenario Planning Focal Question.* [Online]
Available at: https://www.seriousinsights.net/the-focus-of-the-focal-question/ [Accessed 10 April 2019].