January 2012

Wargaming for Chief Information Security Officers

A White Paper

By Nitin Kumar, CMC, C|CISO, CISSP, PMP, CGEIT

EC-Council

www.eccouncil.org/ciso

Wargaming for Chief Information Security Officers

Introduction

The life of a modern day, CISO (Chief Information Security Officer) is getting more complex and demanding as time progresses. They are asked to adapt to ever-changing business needs with lesser resources and budgets. The advent of game changers like mobile apps, social media, cloud computing and the likes have breathed new meaning into the risk landscape. The traditional way of developing an IT Risk strategy understanding risk, managing, mitigating and monitoring becomes very difficult. The ever-growing list of new regulations and compliance needs are like never before adding complexity to the environment.

To excel in this new business landscape, CISOs need to look at a new strategy development process, which will help decision-making by keeping it realistic at minimal risk and with full strategic and operational alignment. Wargaming has been a popular tool in the military and off late is being adapted into business environments.

Business Wargaming is an adaptation of the art of simulating moves and counter-moves in a commercial setting. Unlike military war games, or fantasy war games which go back hundreds of years to the days of Prussia and H.G. Wells, business war games are a relatively recent development, but they are growing rapidly. The time has come for CISO organizations to adopt this technique in order to stay ahead of their game.

The CISO organization itself has several stakeholders internally (Business, IT, Legal, Internal Audit, Risk Management, HR, Board, etc.) and externally (customers, suppliers, vendors, business partners, regulators and policy makers, etc.). This adds several layers of complexity for a CISO than most traditional functional roles.

Wargames can help forecast future scenarios holistically and help build a proactive strategy and a better reactive strategy.

Challenges with conventional CISO strategy

The businesses are increasingly dependent on technology to help them manage and integrate the components of the business model be it managing the supply chain, automating core activities, increasing longevity or revitalizing core assets, managing customer relationships, reaching new customers and even enhancing customer experience. This phenomenon demands that the CISO be a very savvy business executive who not only protects but also creates value for the organization.

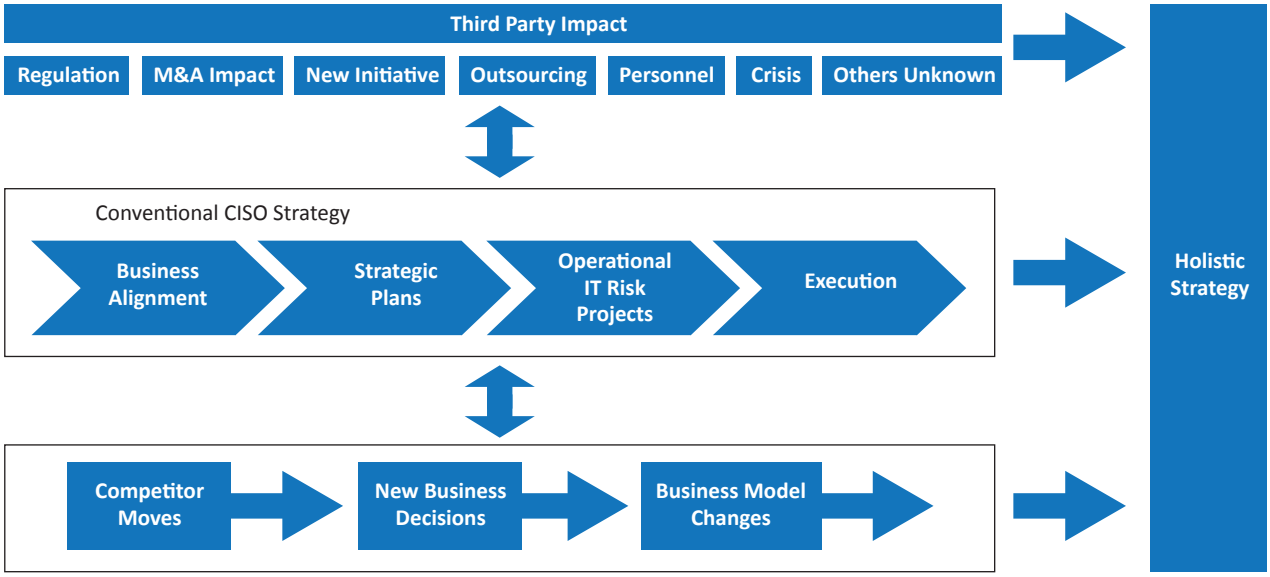

Figure 1: A Holistic CISO Strategy

The mere fact that the business has to live with so many uncertainties puts pressure on the CISO organization to build and develop a strategy that is agile, flexible and can change with the business direction, thereby demanding a new approach to building a strategy.

The challenge with conventional CISO strategy is that it is linear in nature and follows simple steps that are based on historical data, experience and a set of assumptions that are then projected into the future to draw up a futuristic strategy. This approach accounts for only known business scenarios that are then supported by a normal IT Risk strategy that operates catering to known scenarios. Given the changes, the rate and direction of those changes in the environment, businesses (and risk related functions) have to adapt and be prepared for the uncertainties and the implications of those uncertainties on the organization.

The new way of building a strategy has to extend conventional CISO strategy in such a way that it is prepared to counter any moves by competitors, any changes in the regulatory environment, any surprises that show up in terms of new ground breaking technologies or products.

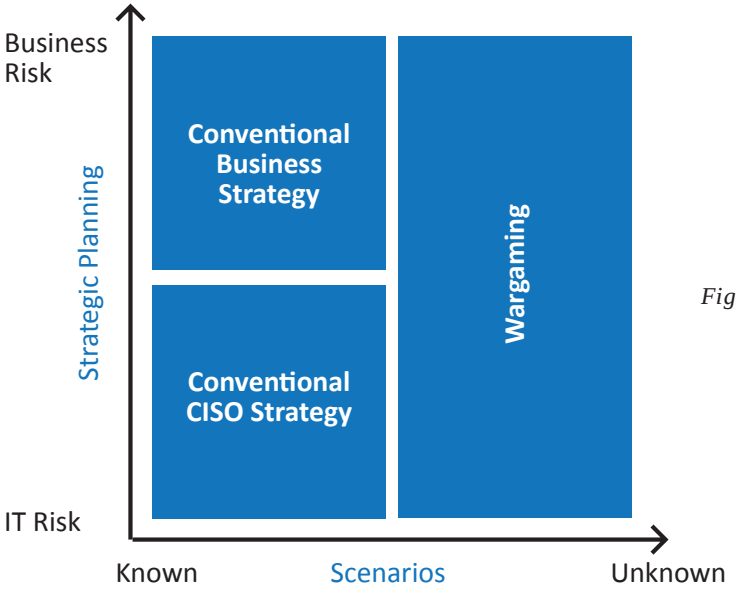

Figure 2: Extending Conventional CISO Strategy

Figure 2 depicts where Wargaming can extend a conventional strategy to cover unknown scenarios and enable CISO to be prepared for counter moves as responses to external changes and threats.

Every Infosec decision has some impact on the business, internally and externally. For example, implementing a new technology, say a smart phone app, could have a lot of touch points starting with business owners, developers, legal, privacy, audit, risk management and end customers. One has to factor in changes in competitive landscape, new regulations, economic scenarios and other unforeseen impacts keeping in mind the known areas of risk within the realms of the 4 A's (Access Risk, Accuracy Risk, Availability Risk and Agility Risk). These sorts of scenarios with a few decisions and multiple outcomes, and a certain level of uncertainty, tend to expose the limitations of conventional strategy that does not factor in moves and counter moves or such a rapid and dynamic business environment.

Wargaming creates a perfect window of opportunity for the CISO organization to look past some of these limitations, align with the business and prepare well to address these uncertainties. This is not limited to the example we cited here, but to several scenarios and combinations of scenarios that are discussed in the next section.

Wargame scenarios for CISOs

Wargaming could be used as a strategic tool by CISOs in a number of scenarios. This will enable foresight into a several external and internal factors on how the business, internal organizational units and external stakeholders would act/react to the strategy. Depending on the maturity of the CISO organization whether it is initiating a formal strategy for the first time, conducting a periodic strategy exercise or evaluating strategy based on a specific situation, Wargaming could be conducted at different levels as described in the subsequent sections.

Following are some of the scenarios for CISOs where Wargaming can be applied effectively to enable foresight within the CISO organization. These could be individual scenarios or a combination of situations that arise in any organization which have significant business impact.

Build versus buy decisions

Organizations could be venturing into new "Line of Business" or enhance the existing business with new functions and features whereby CISO organization need manage and mitigate the risks. These could be situations like opening a new distribution channel or enabling the intranet portal to be external facing etc. and "build versus buy" decision needs to be evaluated based on factors like time to market, competitor capabilities, availability risks, access controls, compatibility with existing systems and industry maturity of products available. Involving representatives from business, operations, and other risk related functions along with the CISO organization representatives to simulate scenarios will help uncover a lot of unknowns and make decisions which are competitive for the market and right for the organization.

New initiatives

When organizations undertake initiatives like new ERP implementations, new operational processes or enabling mobile technologies, there are a lot of uncertainties that surface within organizations. Conducting a Wargame will help uncover unforeseen risks related to process, people, technical architecture etc., due to the impact of changes. This might even warrant core business processes to be re-engineered. Based on inputs from various stake-holders, CISO organizations will be able to build a strategy that accommodates various risk and response scenarios.

New regulations

Government regulation dictates changes the way business is conducted and in turn warrants modifications to IT systems. Be it regulatory mandates like Sarbanes Oxley or Safe Harbor from early part of the century, or healthcare reform of recent times, they require response from CISO organizations toward meeting these business challenges. CISOs and their organizations need to understand the impact to their systems and factor these as part of their high level strategy. Bringing the impacted business executives to a Wargame exercise will help to analyze situation in a much more comprehensive manner and identify options for required response.

M&A impact

Mergers & Acquisitions or resulting Divestitures introduce a plethora of uncertainties within organizations. In most practical situations, CISOs and their organizations will be reacting to financial or compliance objectives that drive the changes within and outside the functional realm. The resulting integration will involve decisions on aligning processes, sunset systems, aligning leadership and consolidating teams. This could also include outsourcing scenarios which will bring additional layers of risk. Conducting a Wargame would help uncover concerns and uncertainties from various business units, operations organizations and internal functions. The resulting strategy will be able to support efficient business processes and ensure minimal interruption to business as many of the external and internal behaviors could be considered. Wargames take into account market responses, analyst responses and personalities of people, which are usually not considered.

Crisis Management

Business Continuity Planning is a critical component to IT risk strategy as more and more of the business processes are being enabled by IT applications. CISO organizations should be prepared to handle the crisis situations that could challenge the status quo be it a natural disaster, a virus outbreak that paralyses the internal IT operation or a product recall due to a business situation. In many situations, IT organizations work in isolation to put together a reactive recovery strategy which might not accurately depict the critical business areas to be addressed in a crisis situation. Engaging various business and operations stake-holders in a Wargame will help simulate the challenge and lead to better preparedness.

Business model changes

As part of the growth strategy, organizations plan to venture into new business models or alter their existing models. This could be situations like building new retail channel for distribution, enabling online channel for sales, enabling an exchange platform, building a new CRM system to conduct business between entities, partners or interact with customers etc. These changes could bring forth a lot of evident as well as hidden risks. A simulation based exercise involving impacted parties within the organization by CISO organizations would help identify the right strategy to address the requirements based on risks and countermeasures.

The "how much" decisions

Several situations arise when CISOs tend to ponder as to how much time, energy, resources, efforts and money is necessary in order to find solutions to business demands. Special situations or projects that have never been undertaken before have no precedence or experience to go by or a traditional risk assessment yields limited results. Too little of anything can cause business risk, while too much of anything can add complexity and create wastage. In order to get an estimate around the same, it is common for CISOs to conduct small scale war games to arrive at the right range and figure out "how much".

Making Wargaming Work

Ideal situation for Wargames

A wargame is most appropriate when the level of uncertainty is moderate. If uncertainty is too great for example like the impact of nanotechnology on the design of next generation servers and IT architecture of the future, it makes things very difficult for planners and strategists to plot outcomes.

Wargames are best used in conditions when two or three results seem viable along each strategic option. In these scenarios analysis tends to be very complicated and yield limited results. Therefore wargames bring forth all the range of options that are available to executives for strategic decision making.

Refer to figure 3 below, when the uncertainty is low to moderate and the outcomes are few, it is the right zone to bring in a wargame. The narrower the options and uncertainty, the more successful the wargame would be since we know what the game is and then have to play to win it.

On the other hand if the degree of uncertainty is too high and the options are several or even infinite then we have to first engage in scenario planning to define the game in the first place. These situations are not suited to deploy wargames to win.

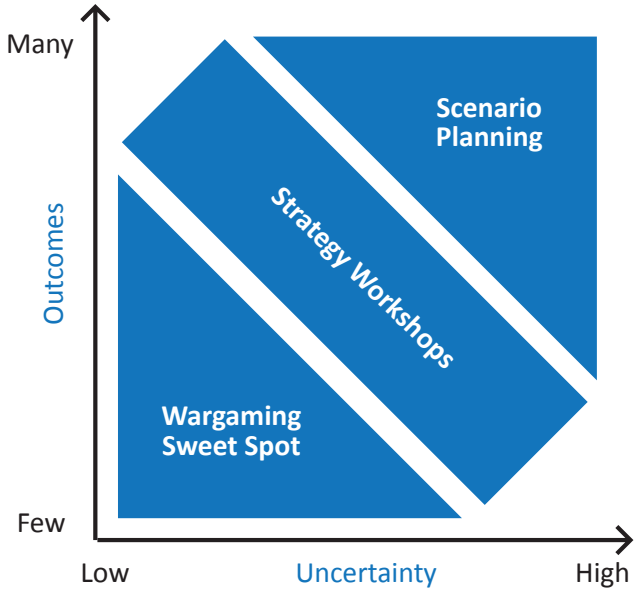

Figure 3: Situations suitable for Wargaming

The area in between the two spectrums of uncertainty would entail strategy workshops to plot the trajectory of moves and to narrow the options from several to a finite few choices. You now know what the game is, but still have to define where to play it. This would still be out of reach from the Wargaming sweet spot.

Once we have made the decision to deploy Wargaming, the next decision is what sort of a wargame should one play?

Wargame Types

Grand Strategy (GS)

This sort of a Wargame considers the entire resources of the CISO organization and focuses on a long term (2-3 year roadmap) along all possible dimensions. The focus is not on any one particular issue but a broader range of business implications based on risk management decisions. Individual issues may not be represented in isolation.

This simulation considers macroeconomic factors like political, economic, and technological impact. This might involve several roles and teams like regulators, R&D teams, businesses, multiple competitors, strategic partners, vendors, outsourcers and other parties as deem fit. Focus is on risk induced due to shift of economic logic of the industry, risks due to new technology, any possible regulations and developing counter moves to mitigate risk issues.

Landscape (L)

Landscape Wargames are designed to consider changes in the operating landscape like industry regulations, business model changes or M&A activity. These sorts of Wargames also help CISO teams prepare for various outcomes and cope with best ways to launch and integrate new and improved controls, replacement and retirement of end of life products and decisions around "how much" effort. All of these geared

Test (T)

Test Wargames are designed to test an already developed strategy against surprises and uncertainties stemming from likely responses of competitors, business changes and unplanned moves from regulators, hackers, internal breaches, business outages and insider threats. These are usually the most popular types of Wargames because the timeline of decisions in most companies is more suitable to building a strategy at a product, business unit or regional level and then testing it upfront.

Wargame Levels

While working with CISO organizations, it is important to understand that this exercise can be conducted at several levels, based on our experience we classify it into four levels Level I, II, III and IV. In addition to picking the right situation, it is also important to determine the right level for the game.

Level I

This is the simplest, most basic level of Wargame and usually involves tackling one particular scenario, based on a specific situation. Usually undertaken when there is a significant level of change being introduced and multiple scenarios are possible. More than likely this will fall into one of the aforementioned scenarios from the previous section. A new process implementation or major change to existing process is a good example of Level I Wargames.

Level II

A Wargame at this level is often designed to serve as a "consciousness raiser" by helping participants to understand key issues and concerns related to their own organization and capabilities. The Wargame is customized to reflect an organization's specific architecture, technology landscape, business model alignment and competitors, and typically involves multiple sessions across a couple of days. Evolution or choosing between two technologies or vendors is an example of Level II Wargames.

Level III

A Level III Wargame is more intensive and aimed at helping develop and/or evaluate strategies to deal with a multitude of issues occurring in tandem. For example, an outsourcing decision could arise triggered by an M&A impact aimed at reducing overall risk and costs, hence this game would have to factor in M&A risk, outsourcing risk, third party risk, people risk, resource allocations etc. It involves the preparation of a significant amount of background material and extensive customization to reflect as much as possible the real personnel, skills, products, competitors, vendors and the "uncontrollable". Level III Wargames could easily last for a few weeks encompassing of multiple (4 or more) moves.

Level IV

This is the most intensive level of CISO Wargaming and often involves two or more separate sessions, each two to four days in duration. This Wargame is usually designed to help conduct a very detailed evaluation of the overall IT Risk strategies and supporting operational level plans before a company makes a final commitment to implement them. This is commonly used in information intensive industries like financial services and technology based industries like media and entertainment where production is becoming synonymous to technology. IT enabled business models, of organizations which use platform based business models need to run this periodically to stay ahead of the game. An organization's overall IT Risk, Security and Privacy strategy is a good example of Level IV Wargames.

CISO Wargame Characterization

Based on the level and type of the Wargames, we can come up with a framework as below to help CISOs pick the right type and level of Wargaming. Various scenarios can be mapped onto this framework to determine the level of effort and depth required. A sample illustration is depicted in the figure below.

Remember that every situation may not accurately fit into these slots, but so long as it is approximately in the right zone, custom designs can create successful outcomes. These are also a function of the industry, organization size, industry dynamics and the current state of the business; hence we recommend that the above framework be used only as a guideline.

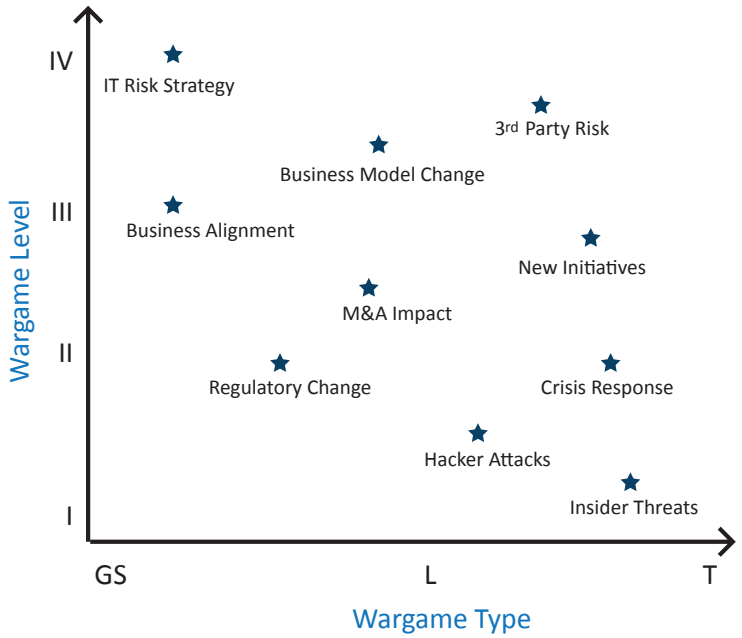

Figure 4: CISO's Wargame Characterization Framework

Additional factors for CISO Wargame design

For a CISO, to determine if a Wargame is the right way to go, a few things need to be taken into perspective. Every situation is unique and comes with its own set of challenges, however some factors to consider would be:

- Should be in the zones of low to moderate level of uncertainty
- Outcomes should be limited to a range of options rather than infinite
- There needs to be a limited number of stakeholders bearing quantifiable impact through each other's actions
- Third parties such as outsourced vendors and other strategic partners need to be considered
- Should not be undertaken during times of high change and flux, for example during a merger or reorganization
- The core business representatives must be involved during the game
- Strategy and operational aspects of the CISO role must be separated during the exercise and both must be handled appropriately
- Assess competitive blind spots within the organization such as capabilities of CISO organization, business alignment gaps and culture related barriers and accelerators

Design & Execution of a CISO Wargame

The design and execution of a CISO Wargame would depend on the complexity of issues to be addressed, level at which it is conducted and the number of stakeholders involved. Duration could vary from 3 weeks – 12 weeks depending on level and type. Below is a generic framework that could be used to conduct a Wargame. It segregates the exercise into 4 phases.

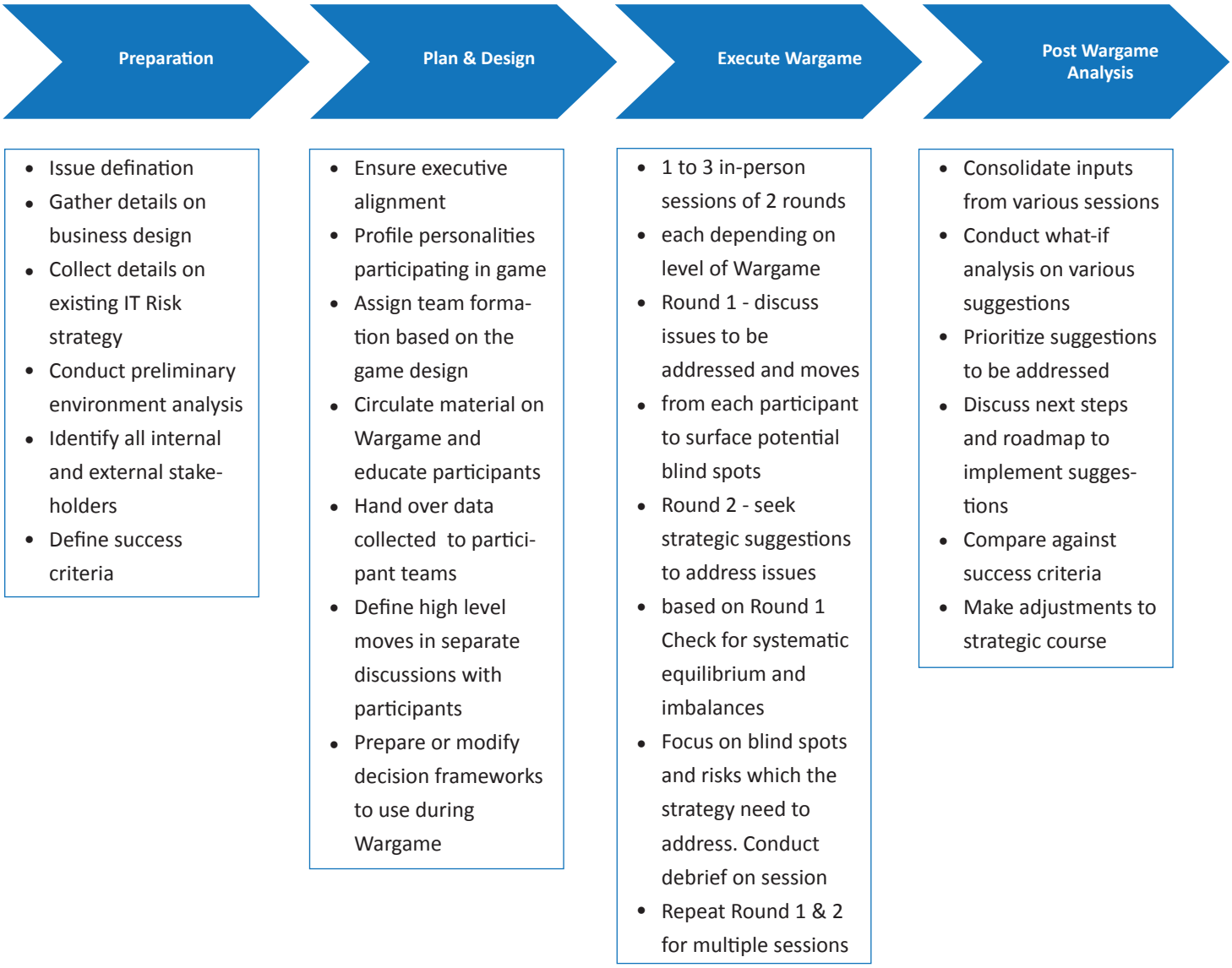

Figure 5: Wargaming Execution Framework

CISO Wargames typically have four teams playing, the home team, the control team, the business team and third parties. Depending on the nature and situation multiple numbers of these teams can also be introduced. An important aspect of successfully conducting a Wargame is to identify a 'Control team' which plays a key role in designing the Wargame by selecting right type and level. This team could be from within the organization or consultants who have experience conducting Wargames and could be viewed as neutral coordinators. This team could comprise of one or more individuals based on complexity and level at which the Wargame is conducted. They focus on keeping the game on track, introducing uncertain-

ties, changing the game dynamics and representing any entities that have not got adequate representation like the senior executives or customers or government officials.

The Home team consists of representations from teams which include sub functions of Information Security, security operations, incident response teams, internal audit or technology vendors and other supporting teams like legal and compliance etc.

The Business Teams comprise of business units, operating units, business analysts and could include customer and competitor roles where applicable.

The Third parties team includes regulators, policy makers, suppliers and other stakeholders. If the game is geared to a specific situation then this team could be split into multiple teams with adequate representation.

The 'Control team' coordinates with the teams separately to plan various moves and counter-moves keeping teams and discussions in isolation to avoid decisions being influenced prior to actual Wargame. The execution is an iterative process and could be planned across 1 to 4 Sessions based on complexity and levels. It is important that de-brief is conducted and factored into the game for subsequent sessions (if applicable) so that outcomes accurately represent the incremental learning from the rounds and sessions. Each round comprises of at least one strategic move. Normally, Wargames are designed for at least 3 strategic moves across any given timeframe.

Key Benefits

Picking the right scenario and designing the Wargame with the right people, right level and ingredients has several general advantages like involvement of top management as well as next line of managers in the exercise who "live" the strategy and the consequences of the decisions.

Wargaming also makes learning from mistakes easier, it tests reactions to different situations and can bring forth the capabilities and strengths of the organization that are usually hidden behind assumptions. One other advantage is that radical moves are possible, that can challenge the very economic or the current operating logic of core business.

Closer alignment to the business model and simulating competitor moves could bring out innovative approaches using technology with assets that were previously under tapped or underutilized. Similarly, underperforming assets can be quickly identified and a course correction can be undertaken.

Given below are some very specific benefits of CISO Wargaming

New Technology implementation	Analysis of Stakeholder Landscape	Acquisition Integration	Outsourcing Risks
Identify value drivers and high level risks	Understand cultural and technical barriers	Live the acquisition process, understand challenges and opportunities	Dry run for the actual outsourcing operational scenario
Assess risks in dynamic environment	Gather business requirements, understand enablers and obstacles	Identify synergy areas and prioritize quick wins	Ascertain true cost savings, value addition and understand risks
Capture interaction with business, market, users and third parties	Optimize operational parameters like timing, costs, resource allocation	Take into account "personalities" of other players	Understand people, process, technology and sourcing risks

Concluding Thoughts

Although Wargaming has been around for many years, it is just about catching up in the business context and is highly under leveraged within CISO organizations. Given the increasing dependence of businesses on IT, the ever-growing threat landscape, the growing importance of information in decision making and the evolution of CISO from a heavy operational executive into a strategic business partner, life is about to change a lot.

CISOs cannot build their IT risk strategy in a vacuum and cannot be linear as yesteryears. It needs to align with the business strategy (including other related functional strategies). Given then uncontrollable factors and uncertainties in business landscape, and this is bound to percolate into CISO organizations at a much deeper level than before. CISO decisions have a very high degree of impact on the businesses be it implementing a new technology, going into the cloud, a major outsourcing decision, responding to a crisis or building a new business platform.

All these decisions have several different risks, outcomes and impacts; thereby Wargaming becomes a very useful tool for CISOs to add to their arsenal in the years to come.

Best Practices and Pitfalls

It is well recognized that every situation is unique and there is no 'one size fits all' approach when it comes to Wargame design; however, there are certain practices which when followed will help ensure that the effort is worthwhile and effective.

Wargames generally end up with suboptimal results due to a variety of reasons, we have tried to identify some common pitfalls and best practices here:

- Wargames make more sense to larger CISO organizations, the more levels of complexity such as regions, sub-functions, countries etc will make the effort more worthwhile
- All roles and players need to have meaningful dynamics between them in order to generate the right counter moves
- Business leaders need to identify and pick the right situations to use Wargames
- The right level and type of Wargame has to be identified and corresponding number of moves be designed
- Involve the right roles and invite the right people from the organization to play those roles
- Do not use the "one size fits all" approach, every problem is different and so is every organization
- Automated software cannot replace human intelligence, decision making and intuition, avoid this
- Over engineering problems does not help the cause, they need to kept close to reality as far as possible
- Keep the games and moves simple, complicated games will sap energies in other directions
- Do not run the Wargame very close to the D-day, it might just not yield the desired results and in fact also be counterproductive
- Empowerment to ask questions and challenge assumptions is absolutely necessary, if organizations management and culture do not support this then stay away from Wargames
- Do not try to anticipate all possible moves from opponents, focus should be on the "most likely" moves

A CASE STUDY

A fictitious bank wanted to study the implications of a datacenter failure and the organization's ability to respond to the crisis.

OBJECTIVE

- Access the impact on infrastructure and ability to provide service in case of a datacenter failure.
- Assess effectiveness of organization's crisis response
- Impact of such a scenario on customers
- Overall technical implications of this outage

GAME DESIGN

- Consisted of two customer teams in different locations
- A Home team , reviewing and responding to the situation
- A control team to manage the Wargame
- A Technical team to assess the exact the impact on the infrastruc-

SURPRISES

The control team expanded the exercise with outages extended to multiple datacenters across several locations; this had serious implications to test the organizations response mechanisms beyond a traditional backup and recovery site.

KEY LESSONS

- Preparedness can always be improved
- Although crisis response was excellent on paper, actual "execution" was not smooth enough
- Identification of the crisis, quick co-relation and timing off contingency plan kick off were not well coordinated
- Communication management process with all stakeholders (especially customers) needed improvement
- Helped the bank be better, quicker and more efficient during a crisis.

About the Author

Nitin Kumar,

CMC, C|CISO, CISSP, PMP, CGEIT

Nitin Kumar is a global executive and management consultant with deep operational experience, has leadership experience in start-ups, turnarounds and driving exponential growth. Held several executive roles such as Consulting Partner, BU Head, Turnaround CEO, M&A Integration Leader and Start-up CEO focused on strategy, sales, delivery, growth and operational excellence.

He has spent several years advising CISOs and CIOs on strategic and operational issues and has enabled decision making through innovative approaches.

He is a certified management consultant, a certified chief information security officer, a certified information systems security professional, a project management professional and certified in the governance of enterprise IT.

Nitin also serves on the CISO and LPT Board of EC-Council and also on the NJ Board of Institute of Management Consultants.