Deloitte.

Managing the Reality of Change: War gaming and risk modeling are key tools

Rapid technological development, increasing globalization, converging industries, shifting regulatory landscapes, and geopolitical tension are just some of the driving forces that bring an unending stream of both routine and increasingly novel risks right to your door. These forces amplify the already extant organizational constraints like poor communication, stovepipes (aka 'cylinders of excellence') and fear of change, leaving many organizations incapable of confronting strategic threats and challenges, ***or*** exploiting opportunities. The stakes are high: social and mass multi-media ensures that a poor decision or crisis response will be known around the globe in a nanosecond, putting an organization's reputation and bottom line in jeopardy, and driving them even further into a reactive and defensive posture.

The resulting new normal also renders obsolete the assumptions and biases that have traditionally guided decision-makers' perception of strategic risks. The Competitive Marketplace cemetery is littered with gravestone markers telling of high-impact events that were deemed unlikely and thus dismissed with the wave of a hand because leaders were not open to at least considering alternate scenarios or undesired/unintended consequences; nor were these leaders committed to relentlessly scanning the horizon for the first signs of the next potential disruption. For example, the unforeseen rapid decline in the price of oil crippled British Petroleum's plans to restructure, thereby making large projects

What is War Gaming?

War gaming is a rigorous analytic process that enhances risk-informed decision-making through immersive experiential learning. Plausible, interactive scenarios bring diverse stakeholders together to challenge biases and assumptions, identify critical gaps and vulnerabilities, and provide insights into emerging threats and opportunities. Players are encouraged to ask “What if?” and allowed to experience failure in pursuit of these insights, all without facing real-world reputational and financial risk.

unprofitable; sanctions in response to Russian military action along its periphery brought Exxon's Russian operations to a halt; a confluence of e-commerce, innovative rental business models, and the advent of streaming video brought on Blockbuster's demise; and, Uber disrupted the taxi and city transportation industries with innovative technology that many thought would never be widely adopted.

How does a company, agency, or government not only survive, but ***thrive***, in such a dynamic and uncertain world? For centuries, generals and statesmen have utilized ***war games*** to make sense of arguably the most volatile, complex, and risk-laden environment of all—the battlefield. A war game's unique ability to stimulate cross-silo thinking, challenge existing biases and assumptions, and assess the effectiveness of proposed strategies make it an invaluable tool for organizations trying to navigate today's teeming marketplace. Through the exploration of both hypothetical and real-world scenarios, this brief will show how war gaming and risk modeling can assist public and private sector leaders in confronting and eventually overcoming strategic risks and crisis events.

Cyber Attack

The scenario—things that go "boom" in the night

It's a Sunday evening in Los Angeles. Brand X Gas Company's CEO receives a distressed call from his Chief Security Officer (CSO): a gas pipeline in downtown LA appears to have over-pressurized, causing an explosion. The extent of damage is currently unknown, but fatalities and serious property damage are likely.

While the c-suite is trying to ascertain the facts and communicate with their local government counterparts, the utility's staff opens lines of communication with first responders. An initial investigation is launched that night as Information Technology (IT) professionals scan the pipeline's remote control systems, and engineering staff begin testing the pipeline's physical integrity.

The next morning Brand X's C-Suite is informed that the entire gas distribution network in LA County will need to be shut down due to an intricate malware program which is embedded in the utility's internal control network. Millions of customers will lose access to gas in the Los Angeles Metro Area. Media scrutiny, lawsuits, and unanticipated additional second- and third-order consequences of the cyber attack are likely. Strategic communications must be fine-tuned to take control of the narrative, inform stakeholders, and mitigate reputational risk. In addition, coordination with the relevant federal, state, and local entities is necessary to contain the incident and prevent further physical damage.

Days later, a cyber forensics team finishes their preliminary assessment, finding that unidentified hackers, operating from multiple IP addresses in Central Asia, exploited a third-party vendor's backdoor access into the utility's internal network. Once inside, the hackers were able to plant malware that disrupted the pipeline monitoring systems. With these safeguards eliminated, the

malware then accessed the pipeline control systems, increasing pressure within a segment of the line. This ultimately caused an explosion which ripped through a commercial area, claiming lives and causing hundreds of millions in property damage.

The real world

While a cyber attack of this nature has not occurred in the United States—yet—it *is* technically feasible. 85% of critical infrastructure is run by information technology systems connected to the internet[1]. This vulnerability has been exploited by intelligence agencies in a number of high profile cases, perhaps most notable of which is the *Stuxnet* attack on the supervisory control and data acquisition (SCADA) system controlling Iran's nuclear centrifuges. More recently, hackers were able to take control of a German air defense missile system in Turkey[2].

Systems in the United States are no less vulnerable. A recent report written by University of Cambridge and Lloyd's of London assessed a major cyber attack on the electric grid spanning from New York to Washington, DC, to be 1 in 200; that is, within the benchmark return period against which insurers must be resilient[3]. Such an attack would leave 93 million without power, causing a rise in mortality rates, decline in trade, disruption of water supply, and severe impairment of logistical networks.

Recent history has plenty of actual examples of similar attacks, albeit not targeting the electric grid. In November 2011, hackers penetrated a Springfield, Illinois, water district SCADA system and were able to repeatedly turn a water pump

on and off, which over the course of a day caused its destruction[4]. The same year, another attack on a water utility's SCADA system in West Milford, New Jersey, caused 60 homes to lose water pressure on 3 occasions and triggered numerous sewage spills[5]. More ominously, hackers were able to breach a British Petroleum pipeline's control station in Turkey, causing a segment of the line to explode in 2008[6]. The attackers penetrated the pipeline's control system by hacking a third-party system networked into the pumping station—in this case it was the security cameras... sound familiar?

How war gaming can help

Governments, manufacturers, and critical infrastructure providers—those entities managing electric grids, manufacturing plants, upstream oil and gas facilities, or nuclear power facilities—need to understand both the impacts of an attack,

1 "Cyber attacks on critical infrastructure reach U.S.," Homeland Security News, http://www.homelandsecuritynewswire.com/cyber-attacks-critical-infrastructure-reach-us-bf?page=0,1

2 "'Hackers' give orders to German missile battery," The Local, July 2015, http://www.thelocal.de/20150707/german-missiles-taken-over-by-hackers

3 "Lloyd's report highlights implications of major cyber attack for insurers," Out-Law.com, July 2015, http://www.out-law.com/en/articles/2015/july/lloyds-report-highlights-implications-of-major-cyber-attack-for-insurers/

4 "Water utility hackers destroy pump, expert says," The Register, 2011, http://www.theregister.co.uk/2011/11/17/water_utility_hacked/

5 "Homeland Security to look into attacks on West Milford water, sewer services," NorthJersey.com, 2011, http://www.northjersey.com/story-archives/homeland-security-to-look-into-attacks-on-west-milford-water-sewer-services-1.1216757

6 "Mysterious '08 Turkey pipeline blast opened new cyberwar," Bloomberg Business, December 2014, http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

as well as the best ways to mitigate associated risks. War gaming provides a methodology for probing and assessing current crisis response capabilities. By immersing a diverse group of stakeholders in a realistic crisis scenario, biases and assumptions can be challenged; existing plans and capabilities can be explored for gaps and vulnerabilities; and new and innovative ideas can be stress-tested without the expenditure of real-world capital.

Some of the questions that may arise from this simulated experience include: are IT security and engineering personnel sharing disparate information that could, when pieced together, provide a more coherent picture that shows indications of an impending attack? Are lines of communication open with relevant first responder entities to ensure rapid reaction and containment? Do our existing plans, policies, and procedures take into account enough of the disruptive events we are trying to prevent? These and other questions are just some of the many questions war games can answer in order to streamline and increase effectiveness of crisis response and recovery.

Pandemic

The scenario: there's something going around

Two months ago, several of the staff called in sick with the flu. They have yet to return to work. The same goes for the other 150 people who have become ill at your organization. Productivity is dropping. The Board of Directors is worried.

Weeks later, major news networks begin reporting that approximately 30% of the U.S. workforce is sick, and the death toll is beginning to rise. The rest of the world is not doing much better, and in the emerging and frontier economies, the situation is even more dire. Many of the workers who have fallen ill are the medical and first responder staff who were exposed to the initial waves of infection before the full extent of the virus's contagiousness and lethality were known.

Cogs in the global supply chain become disrupted as those responsible for international and domestic shipping fall ill. Food becomes increasingly scarce, stock prices plummet, and energy prices spike. Healthy employees stop coming into work and executive level leadership has no viable response. With key employees sick or not showing up to work, business continuity plans begin falling apart.

The real world

In the April 2015 edition of the New England Journal of Medicine, Bill Gates suggests that we should prepare for pandemics in the same ways we prepare for war; that is, conduct training exercises, run simulations, and develop early warning systems[7]. Indeed, the consequences of a severe pandemic can be as significant as war. The Congressional Budget Office estimates a severe pandemic would bring about a 4.25% fall in GDP—2.25% of this would occur on the supply side, where up to 30% of workers become ill; and the remaining 2% would occur on the demand side where fear and illness keep buyers at home[8].

7 Gates, Bill, The next epidemic – lessons from Ebola, New England Journal of Medicine, 372;15

8 Congressional Budget Office, A potential influenza pandemic: possible macroeconomic effects and policy issues, rev. July 27, 2006

To add to the darkness, FEMA assesses the effects of a pandemic in the U.S. would be catastrophic:

- Deaths ranging from the hundreds of thousands to many millions;
- Up to 40% essential services employees may not show up to work; this includes caregivers, nurses, doctors, law enforcement, firefighters and EMTs, and those responsible for transporting and distributing foodstuffs;
- Lawlessness related to a lack of law enforcement presence and access to basic services and resources;
- A lack of banking and financial services[9].

For any enterprise, the loss of staff and utilities presents a severe operational crisis. In any industry, the resulting work stoppage results in not only immediate losses, but also future costs due to a drop in client confidence, fines from regulatory compliance issues, and the cost of replacing lost capital stock. In addition, programs in progress will be delayed or halted if personnel cannot continue to work and collaborate on them from remote locations. The situation can quickly escalate to the strategic level if the organization in question is one that provides law enforcement, first response, or other basic civil capabilities.

How war gaming can help

Pandemics not only present an enterprise with a novel crisis—an emergency of unusual scale, unknown cause, or atypical combination of events, in this case the confluence of supply chain issues and a diminished workforce triggered by an unknown pathogen—but also a strategic risk, that is, a risk which can disrupt value creation or market position and existentially threaten a company. Not only should an enterprise be prepared to deal with the immediate crisis, but its leadership must constantly try to keep one eye on the horizon, scanning for the next indicator or disruptor, as well as envisioning their strategy for recovering and maintaining market position, post-pandemic.

A war game is an excellent vehicle for assessing immediate crisis response capability. In carefully scripted scenarios based on in-depth data gathering and stakeholder involvement, participants are able to explore whether or not their own enterprise is able to ensure the continuity of operations, physical security of valuable property and information, and safety of employees. By engaging in a purposely contentious simulated environment designed to evaluate and assess existing capabilities, players are able to experience first-hand if their current business continuity plan includes all the right components; if there are succession plans to account for primary responders being unable to perform their assigned tasks; or if decision-makers have the right "asks" in place to help ensure they will be receiving the necessary type and pace of information to form coherent operating pictures. These types of questions are tough enough in the real world; the presence of overconfidence, biases, and other external pressures only exacerbate the ability to make honest assessments of inherent strengths and weakness of preparation and response plans.

When the next big event happens, whichever firms are most prepared for such circumstances will be best positioned to capitalize on the market vacuum left by unprepared competitors. Rehearsing and practicing *before* a crisis can lead to greater success in responding and recovering *afterward*. Effective crisis response is essential to preserving shareholder value.

9 Federal Emergency Management Agency, Catastrophe readiness and response course – unit 13 pandemic scenario, https://training.fema.gov/hiedu/docs/crr/cat%20-%20session%2013%20-%20pandemic%20power%20point.ppt

What is Risk Modeling and Simulation?

Risk modeling and simulation leverages quantitative and qualitative models to identify, assess, and prioritize risks to populations, missions, programs, and operations. Modeling approaches include system dynamics modeling, agent-based modeling, discrete event process models, "event based" scenario analysis, and machine learning for analysis of unstructured data.

High Value Physical Infrastructure Construction

The scenario…which took place in the real world

Governments and large corporations often own and develop permanent, high-value, physical infrastructure, sometimes in hostile or adversarial environments. The following describes one of the more infamous cases that demonstrates the risks associated with facilities construction taking place in high-stress, high-visibility, and politically-charged atmospheres: the U.S. Embassy in Moscow.

In August 1985, work in Moscow on the U.S.'s new office building (NOB) was suspended when Soviet listening devices were discovered embedded in the building's structure. Accusations, rancor, and debate followed. What could the U.S. Government do? Costs sky-rocketed as the nearly completed building essentially sat vacant for almost a decade. The situation was made worse when, in 1991, the embassy staff, while still working in the old office building that had fallen into disrepair as costs continued to be diverted to the halted NOB, barely escaped a large fire that engulfed much of the complex.

Finally, in the mid-1990s, a new remedial construction program for the compromised NOB launched, nicknamed "Top Hat". Its aim was to achieve tight informational security only in the upper floors of the NOB, while consigning much less sensitive work to its lower floors. It was not until after the turn of this century, almost 40 years after initial ground-breaking, that the NOB finally opened for business.

How and why did this happen, and what are some lessons that can be learned from this unfortunate episode? Usually, this story is cast as a failure to consider the risks of Soviet espionage and protect against them. While true enough, deeper examination reveals that there were, in fact, concerns beforehand about Soviet construction of the NOB and the possible bugging of it. In fact, the follow-on negotiations of the conditions for construction to the 1969 sites agreement dragged on for three years. However, in the hierarchical decision-making setting of the times, those concerns were silenced.

… conducting war games as an integral part of the planning cycle can bring value to any decision maker planning to allocate large resources to a fixed and strategically vital piece of infrastructure …

One reason this occurred appears to be due to geopolitical factors: in 1972, President Nixon was about to have a Summit with the Soviets. This created pressures to get the U.S. to sign off on the embassy construction agreement as an additional way to show bilateral progress. However, typical of all embassies constructed in the old Soviet Union, the agreement text called for the host country to perform the basic structural work. The Soviets even had the right, as a provision of the agreement, to review and approve the architectural drawings for the building's frame. *In other words, the agreement itself facilitated Soviet espionage.*

Furthermore, there seems to have been chronic over-confidence that the KGB did not have the sophisticated technologies necessary to compromise the NOB. Despite claims to the contrary by Soviet defectors, this deeply ingrained—yet painfully false—assumption prevailed and construction continued on the NOB unchanged for years thereafter.

How war gaming *could have* helped

As alluded to above, historical analysis shows there were systemic problems with the rigid hierarchical decision-making structure which silenced concerns of Soviet espionage and stifled solid analysis. While there are many lessons to be learned from this page in history, the need for more a robust horizontal dialogue and analysis, a commitment to challenging preexisting notions (and the commitment to protect those individuals who *do* challenge them), and a rigorous methodology of identifying and weighing risks and rewards *before* a defining action is taken (e.g., the signing of the construction agreement) is clear. Similarly, using hypothetical scenarios that explored the "what if" of the Soviets having a higher technological capability for electronic eavesdropping might well have led to alternate courses of action that could have prevented or at least mitigated such damaging results.

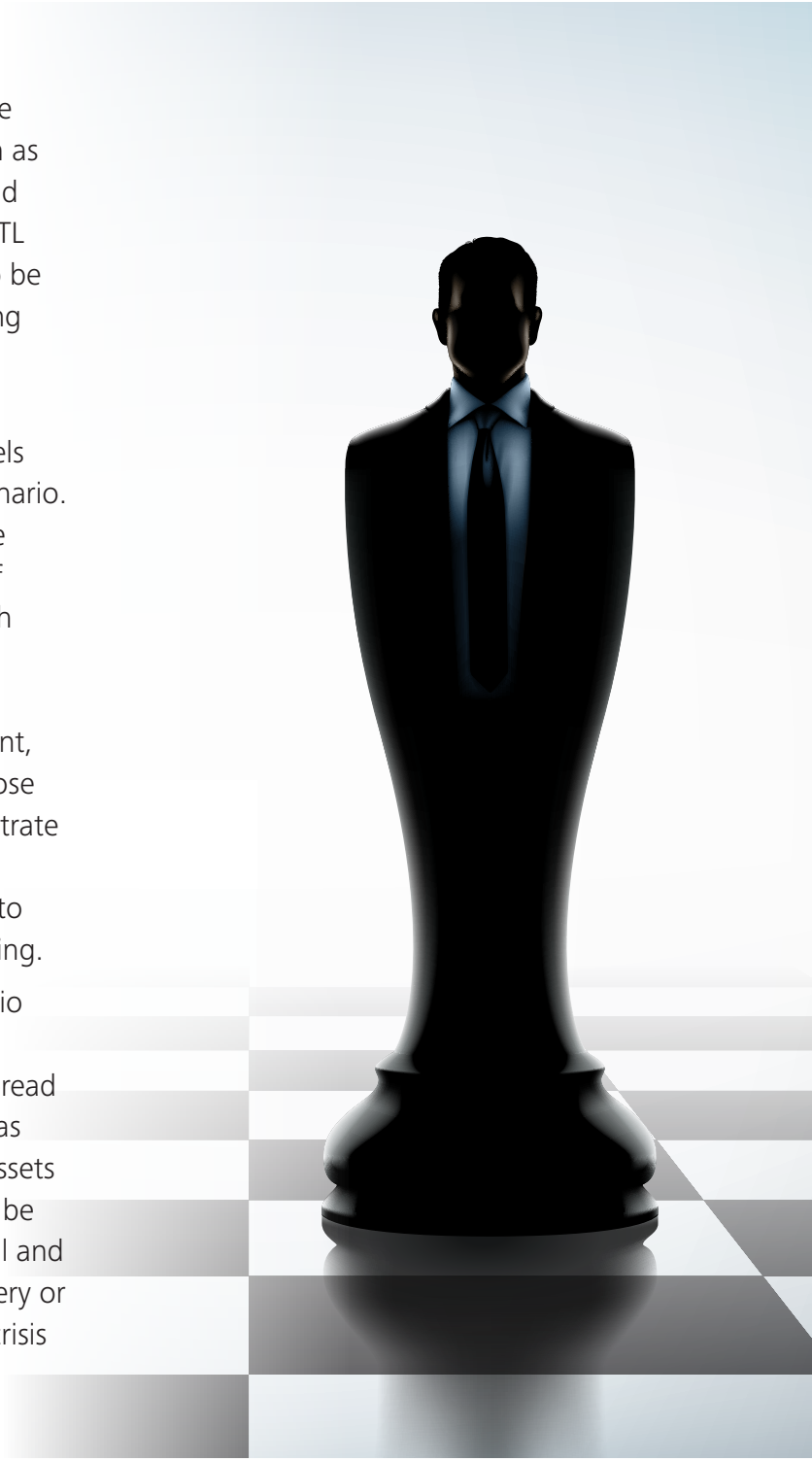
War gaming, as a specific tool and discipline, can meet this requirement and can greatly enhance the value of existing analysis. In this case, an immersive scenario with a dynamic and free-thinking adversary with capabilities greater than prevailing biases and assumptions allow, could have helped force organizations to confront undesirable and unintended consequences, yielding insights that could have enabled better preparation and anticipation of future crises and risks. As such, conducting war games as an integral part of the planning cycle can bring value to any decision maker planning to allocate large resources to a fixed and strategically vital piece of infrastructure, be they government buildings, corporate headquarters, energy pipelines or grids, or other similar high-cost, high-vulnerability projects.

Risk modeling: revealing unintended consequences

War gaming is a dynamic methodology that can be easily integrated with other forms of analysis, such as risk modeling. This Risk Modeling-War Game hybrid is known as a Human-in-the-Loop (HITL) game. HITL games enable participant and adversarial action to be dynamically modeled, thereby realistically modifying the environment during game progression.

HITL games are comprised of human decision-making interspersed with computational risk models representing physical components of the crisis scenario. The decisions of the participants will determine the inputs to the computational models; the output of which will represent the new environment in which participants will make their next decisions. The overall results of the HITL will highlight the effects that decisions have on the surrounding environment, and the inherent vulnerabilities associated with those effects. Using risk modeling to realistically demonstrate a decision's second- and third-order effects adds rigor and objectivity to the war game, in addition to allowing greater exploration of contingency planning.

In the case of a government agency with a portfolio of programs at different stages facing a pandemic scenario, relevant simulations might include the spread of the pandemic through the office environment, as well as the consequences of the pandemic on IT assets and network access. Similarly, risk modeling could be used to realistically demonstrate the environmental and physical impacts of a disaster at an oil or gas refinery or pipeline, thereby enabling the gaming of specific crisis scenarios.



Conclusion

Channeling the great Prussian Field Marshal von Moltke, "No plan survives first contact with the enemy." Whether that enemy is a group of hackers on the other side of the world, a lethal virus or bacteria, an adversarial nation state, or disruptive market forces, one of the worst things an enterprise can do is be willfully unprepared.

But just having a plan is not enough—organizations should commit to a program that periodically and rigorously tests it. War games allow leaders and decision-makers to experience the uncomfortable reality of a crisis, but do so in the relatively safe confines of a simulation, thus allowing them to fail fast and without expenditure of real-world resources. War games, particularly when combining the powerful element of risk modeling and simulation, are one powerful tool in the larger crisis management and strategic risk toolkit that enable risk-informed decision-making through immersive experiential learning. They achieve this through tailoring plausible scenarios to enable clients to explore a current challenge, assess their capabilities against established processes, or anticipate future risk by recognizing indicators and warnings. As a result, leadership teams can emerge with a stronger understanding of the problem and solution set, and may be able to better manage uncertainty to best position their organization to confront and even exploit future threats, challenges, and opportunities.

Contacts
Meet the Contributors

Linnea Gavrilis
Director | Deloitte Advisory
Strategic Risk
Deloitte & Touche LLP
lgavrilis@deloitte.com
Mobile US: +1 202 230 7744

Patchin Curtis
Director | Deloitte Advisory
Strategic Risk
Deloitte & Touche LLP
patcurtis@deloitte.com
Mobile US: +1 410 963 4028

Elton Parker
Specialist Leader | Deloitte Advisory
Strategic Risk
Deloitte & Touche LLP
ecparker@deloitte.com
Mobile US: +1 202 279 1545

Holly Russo
Specialist Master | Deloitte Advisory
Strategic Risk
Deloitte & Touche LLP
hrusso@deloitte.com
Mobile US: +1 571 230 7558

Josh Shapiro
Consultant | Deloitte Advisory
Strategic Risk
Deloitte & Touche LLP
josshapiro@deloitte.com
Mobile US: +1 845 489 2782

Deloitte.