Game of Threats

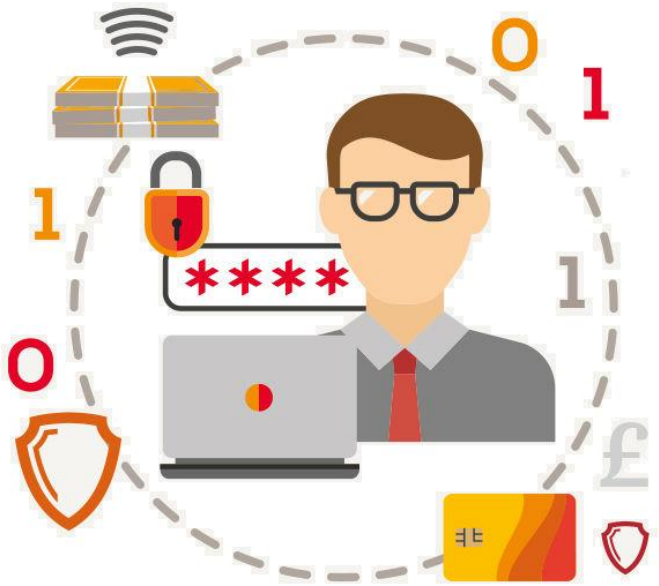
Cyber Security Risk - Stimulation Training

April 2018

Game of Threats™ - Overview

Game of Threats™ is a digital game that simulates the speed and complexity of a real-world cyber breach to help executives better understand the steps they can take to protect their companies. The game environment creates a realistic experience where both sides – the company and the attacker, are required to make quick, high impact decisions with minimal information.

PwC's Cybersecurity experts coach players through realistic scenarios with different types of threat actors and their preferred methodologies, and explain what they can do to better prevent, detect and respond to an attack.



Game of Threats™ – Cyber Threat Simulation

Our interactive cyber crisis workshop uses a head-to-head strategy game to challenge players to make quick, high impact decisions and assess their readiness to respond to a breach.

Interactive

Threat actor and company teams each have their own iPad controller. They see the impact of their decisions in real-time on a shared monitor.

Game Play Replicates Real-World Challenges

Actions are designed around the concept of a shuffled deck of "virtual cards" displayed onscreen. Players can encounter different options every time they play.

Detailed Play-by-Play Summary

PwC moderators provide a detailed summary of each game, reviewing both team's strategy, actions and missed opportunities

Game of Threats™ – Gameplay Methodology

Phase 1: Setup

- PwC trainers will explain the security, business and collaboration insights players will gain from the workshop.
- Trainers will explain the gaming system and its purpose, and preview what each team will experience during the course of the game.
- Participants will be divided into 2 groups as; threat actor and company teams, typically using 10-12 players per team during each game.
- Players will have the chance to ask questions about game mechanics, rules and outcomes and to become familiar with the GoT system.

Phase 2: Gameplay

- During gameplay a PwC trainer will coach each team, providing insights and advising on options as needed.
- Trainers will provide color commentary on gameplay and answer any players' questions about the system.
- Players will discuss the best options for each round of gameplay amongst themselves and devise the best strategies to defeat their opponents.
- Players will have time limits to simulate decision-making stress of a cyber crisis.

Phase 3: Lessons Learned and Summary

- When one team wins, PwC trainers will guide all players through a move-by-move dissection of the game, asking players and teams to offer context and rationale for certain decisions.
- Trainers will discuss possible alternatives with players and highlight technical, reputational, regulatory and legal impacts of decisions made during the game.
- Trainers and players can return to a specific round in the just-completed game to replay the game, armed with new lessons learned and strategic advice.

Game of Threats™ – A Decision-Based Crisis Simulation

In each round of the game, Threat Actor and Company players can choose one of several attack or response cards— the cards offered to a player in each round are dependent upon their decisions to date.

Threat Actor

Sample threat actor options:

- Launch a DDOS attack
- Conduct a spear phishing campaign
- Hire additional expertise

Company

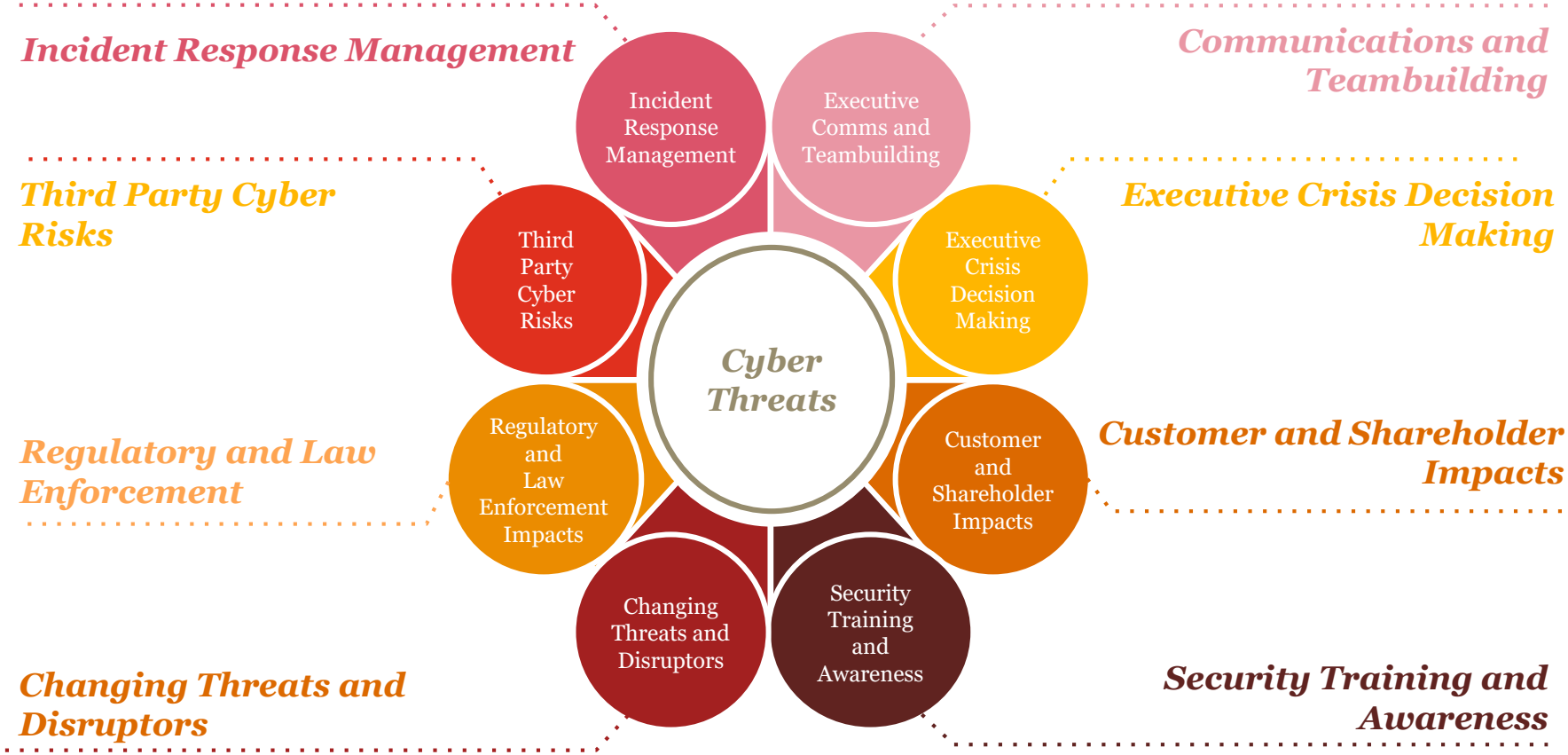
Sample company options:

- Invest in security infrastructure
- Conduct network scans
- Assess data vulnerability

Game of Threats™ is designed to reward good decisions and penalize sub-optimal decisions; each player's card options are based on choices made in earlier rounds

Game of Threats™ – Scenario-Based Business Insights & Case Studies

Game of Threats™ simulates the experience that executives must go through in the midst of a cyber-breach. Using scenario based insights, players are educated on cybersecurity issues and threats that are a key component of today's corporate agenda



Game of Threats™ – Questions we will help the participants find answers for

Strategy

- What macro-level business drivers will impact your business strategy over the next 3 to 5 years and what are the implications on the security posture of the organisation?
- What level of cyber risk is your business willing to accept and are risks knowingly being accepted? How are risks re-evaluated as the threat landscape changes?
- What are the most relevant threats actors, vectors and tactics both today and in the future; how will you anticipate and adapt?

Structure

- How should your security program evolve to better enable and protect business initiatives and objectives?
- How will you maintain an integrated approach to 'front, middle and back office' security in the face of a crisis?
- What is the optimum security structure and organisation to execute your business strategy successfully?

People

- What cultural changes are necessary to build awareness and drive sustained commitment to cybersecurity?
- What skills and talent do you need to hire or train to improve the security posture?

Process

- How should you balance multiple global regulatory obligations with business agility and customer experience during a cyber crisis?
- What process changes do you need to consider to enhance your prevention, detection, and response capabilities?

Technology

- What security technology do you need to efficiently and effectively respond to a cyber crisis AND manage business operations?
- What are the priorities (gaps, dependencies) to enhance your current technical abilities and respond to likely future cyber events?

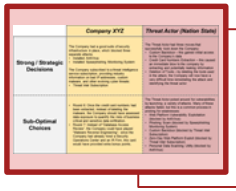
Game of Threats™ – Client Deliverables

The primary deliverable is the feedback provided during the Client session and during Simulation Summary.

Game Simulation Summary

- Graphical summary of gameplay
- Review of decision making, resource allocation, and impact
- Ability to restart from critical suboptimal decision-making points

After each workshop, PwC will prepare a deliverable comprised of analysis of the simulation summaries, gameplay decision making observations and analysis and recommendations.



Gameplay Analysis

- This document is a synopsis of the games, and provides an analysis of strong /strategic decisions, sub-optimal choices and relative impacts
- Key observations in the areas of strategy, structure, people, processes and technologies

Recommendations and Divisional Analysis

- Gaps and opportunities identified during gameplay
- Next steps for improving stakeholder strategy, structure, people, processes and technologies
- The report provides observations regarding existing capabilities and potential areas for improvement, does not contain a formal assessment of controls
- Optional: Comparative trend analysis of game play during different stakeholder groups to identify potential divisional trends in cybersecurity awareness and collaboration

Key takeaways for Participants:

- Learn lessons about your company's ability to respond to a cyber attack
- Understand the potential ramifications and remediation options after an attack
- Understand what your company can do to prevent an attack
- Gain insight into the mindset of Threat Actors
- Learn key cyber security trends and terminology
- Spark a leadership discussion about your cybersecurity readiness

Let's talk

Nishan Mendis
Director | PwC
nishan.mendis@lk.pwc.com
Office: 011 771 9700 Ext- 1001

Vengadasalam Balagobi
Senior Manager| PwC
Vengadasalam.balagobi@lk.pwc.com
Office: 011 771 9700 Ext - 1601