OCEAN's 99

A GamingWorks Business Simulation

Cyber Security - Resilience

What's happening in Cyber Security world?

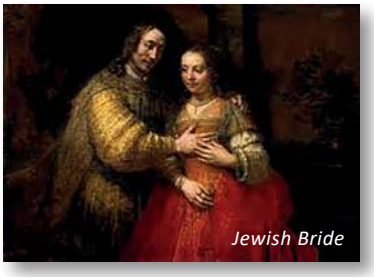
A report from an international Cyber Security Protection Alliance concluded that organizations do not have enough awareness and knowledge about Cyber Security revealing a need for 'more information and education'. An ISACA report '2015 global Cyber Security status report' revealed that only 38% of organizations said their organizations were prepared for sophisticated cyber attacks. Is it any wonder that the latest trends report from the Society of Information management reveal that 'Security' is a top scoring issue for CIO's?

This has prompted an explosion in Cyber Security education, certification and training with 'Resilia' being the latest offering provided by Axelos. However despite the investment in knowledge and skills it is the attitude and disciplined behavior of people that pose a significant risk. The latest Cyber Security findings from Cisco also reveal that attackers are shifting their emphasis from '…seeking to compromise servers and operating systems to seeking to exploit users ' (behavior).

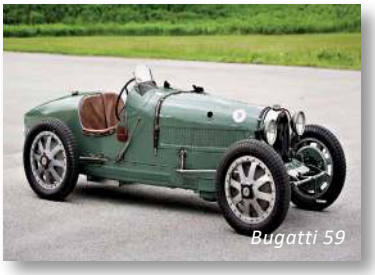
Ocean's 99 is our latest business simulation game that aims to support Cyber Security awareness and training programs – helping to change attitude and behavior.

OCEAN's 99

Star of Africa



Jewish Bride



Bugatti 59

About Ocean's 99

"The owner of the Bank of Tokyo has decided to exhibit three world renowned objects. The 'Star of Africa', the 'Jewish Bride' and a 'Bugatti 59'. Each of these objects must be transported from their current location to the Tokyo Museum and exhibited for a period of 4 months.
Your challenge is to bring the objects to Tokyo, on time, safely and securely, and to have them exhibited for the planned time. Each day too late, will cost money and will harm the image of the bank and the museum.
But, be careful. Ocean's 99, a criminal organization, is also very interested in the objects... Ocean's 99 and maybe other unforeseen threats can undermine your plans…"

Welcome to Ocean's 99 Cyber Security and Cyber Resilience business simulation.

Structure of the simulation

Introduction

The specific learning objectives for your organization will first be introduced. The team members will familiarize themselves with the materials and roles in order to identify who they are during the simulation. Each of the participants will be given a role and a set of responsibilities. The key players are: Bank of Tokyo, Tokyo Museum, Security Officer, Project Manager, IT Support, Transport Manager and the owners of the objects from the Amsterdam Museum, London Museum and Las Vegas.

Security Policy and Risk Assessment

The team will start with an exercise to define the Security Policy of this organization. Together they will agree on strategy, roles & responsibilities and processes. They will also define the key assets they want to protect.

After this the team will perform a Risk Assessment. They will investigate the threats and risks of the Tokyo Museum infrastructure, the Project Managers system to monitor the progress and location of the objects and the systems of the objects owners. The team has a limited budget to invest in advice or tests to analyze the vulnerability of the various systems. As a result, the team can decide to invest in improved systems, software, policy or procedures.

The team will design and agree the supporting processes and Cyber Security procedures to be used during the simulation.

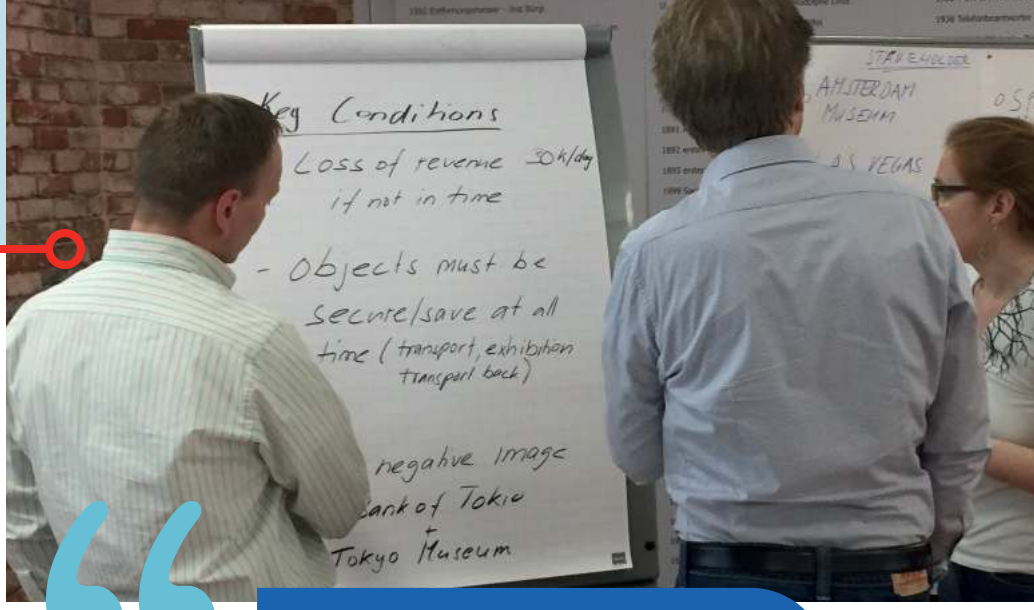
Awareness session

When the design work has been completed the team members will prepare themselves for the next phase of the simulation. They must decide what should be part of the awareness campaign and how to organize this.

Moving objects from the museum to the local airport

This is the first round of the simulation in which we will test the team's design. The team has to move the objects to the local airport. During this round the team will receive a series of realistic Cyber Security events which they must both recognize and deal with. To respond to the events, IT Support has a range of solutions. Some of the solutions may cause delay, others may be expensive to deploy. It is up to the team to find the right balance between the project (opening the exhibition on time) and security (minimizing risks and impact).

The scenarios, events and incidents in the game are based upon the most common sets identified in security trend reports and findings to ensure that the learning is both realistic and relevant.



Reflection and improvement
After this first game round the team will capture lessons learned. We will reflect on the 4 P's. An example of reflection items:

- PEOPLE: awareness & understanding of policy & procedures and the impact of not following; communication; feedback on confronting each other on behavior; knowledge and skills to perform security related activities
- PROCESS: Were the security policy, processes and procedures fit-for-use and fit-for-purpose; were the procedures being adhered to;
- PRODUCT: Were security events and incidents detected and recorded, were products used for detection, prevention and recovery;
- PARTNER: Were all partner and supplier capabilities in the end-to-end chain aligned;

The actual reflection items and themes can be customized to meet your organization's specific challenges and learning objectives.

Following reflection the team will agree and implement improvements to their Cyber Security and Cyber Resilience capabilities.

Moving the objects from Tokyo Airport to the Tokyo Museum
This is the final round. Again the team will receive a series of events and incidents based on the current security level after having made their improvements and investments in new countermeasures. Then we will hopefully celebrate the opening of the exhibition.

Closure and Lessons Learned
The simulation will finish with lessons learned and actions for day to day work.

> *This simulation confronts you how working with unreliable information (hacked by OCEAN´s 99) can dramatically harm your business* - CISO

Why a simulation?

Most of the elements that are trained are theory and knowledge. But PEOPLE are the most important reason why security fails. It is about attitudes, behaviors, communication, interaction as well as procedures and processes. You can have the best policy and procedures in the world but a user ignoring these and taking home a USB stick with sensitive data poses a risk.

Simulations are ideal instruments for helping translate theory into practice and at the same time address 'attitude' (creating understanding, buy-in and insight) and 'behavior' (recognizing and avoiding undesirable behavior and testing and experimenting with new 'desirable behavior') as they combine theory and 'learning-by-doing' in an interactive session. Teams of 10-12 participants, often representing different departments, must organize their work. They must design, plan, execute, reflect and improve their way of working in a simulated environment. In the simulation the teas see and experience the complete end-to-end delivery chain and the interdependencies.

Each of the participants can bring in their own knowledge and experience. Students will receive direct feedback from the game environment, the facilitator and each other on their decisions. The game is played in a number of rounds allowing delegates to learn 'continual improvement'. At the end of the simulation concrete improvement actions can be captured and taken away. This way the learning process will move much faster.

Target Audience

This simulation is targeted for the following groups of 8-12 participants:

BOARDROOM

With this audience we will run the Security Policy and Risk Assessment exercise. This will create an understanding about the current Cyber Security status in the organization.

1½ hours

IT GROUPS

We will run the full day simulation to give the teams a clear picture of all the Cyber Security aspects related to IT Services and processes.

1 full day

END USERS

We will execute the two final rounds of the simulation. This audience will experience the consequences of Cyber Security attacks, threats and activities and the need for disciplined, desirable behaviors.

2½ hours

Learning objectives

- You will be aware of the importance of a Cyber Security and Cyber Resilience for your organization.
- You will have a better understanding and insight into the threats, risks and weaknesses in your own organization.
- You will understand the essence, definitions, roles and responsibilities and terminology of Cyber Security and Cyber Resilience.
- You will be able to apply your knowledge and understanding to assess the current maturity or status of Cyber Security and Cyber Resilience of you own organization.
- You will have gained practical insights and tips on how to initiate and implement effective Cyber Security and Cyber Resilience initiatives in your own organization.
- You and your colleagues will have seen, felt and experienced the impact of 'attitude' and 'behavior' as critical success or fail factors in Cyber Security.

Do you recognize these issues or would you like more information?
Please contact our partner:

Martin Andenmatten
General Manager, Trainer & Coach
Glenfis AG | Badenerstrasse 623 | CH-8048 Zürich
T +41 848 889 089 | www.glenfis.ch
M +41 79 476 0888 | Martin.Andenmatten@glenfis.ch

glenfis

www.gamingworks.nl

version 3