INDUSTRIAL CYBER SECURITY - AWARENESS BY EXPERIENCE

INDUSTRIAL SECURITY TODAY – LOW AWARENESS

CEO

Doesn't see how Cyber Security spending relates to Revenues

IT Security

Is not allowed to go into Industrial sites

Engineers

Are more concerned about security measures than malware

Mutual understanding and partnership between these 3 are crucial to successful cyber security and Critical Infrastructure Protection.

Lectures and technical red/blue exercises are flawed:

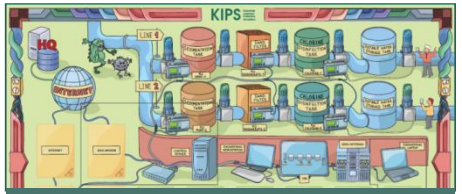
- ✖ Long, too-technical, boring, not for managers
- ✖ Fail to build "common language" at the "common sense" level

We need a fresh and workable approach

KASPERSKY lab

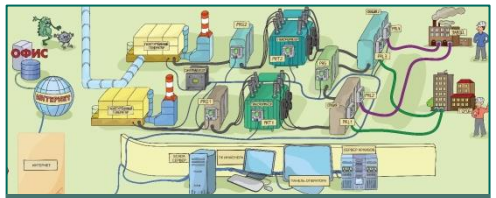
KASPERSKY INDUSTRIAL PROTECTION SIMULATION (KIPS)

- Fun, engaging and fast (2 hours)
- Team-work builds co-operation
- Competition fosters initiative & analysis skills
- Gameplay develops understanding of cyber security measures
- No deep expertise necessary



Water supply plant scenario

Teams compete running a simulated industrial object
and earning money.
As the plant experiences a Stuxnet-style cyberattack they see the impact on production and revenues, and have to adopt different engineering or IT strategies and solutions to minimize the impact of the attack and earn more money.


Power substation scenario

KIPS PLAYED BY ~2000 SECURITY PROFESSIONALS FROM 17 COUNTRIES

Atlanta,
USA

”The Kaspersky Industrial Protection Simulation was a real eye-opener and should be made mandatory for all security professionals, especially those working for suppliers of national infrastructure.”
http://www.computerweekly.com/feature/Industrial-cyber-attack-a-dangerous-game

ComputerWeekly.com

Kuala-Lumpur,
Malaysia

SANS ISA TOSHIBA CERN

«It was truly eye-opening and a number of the participants asked about using this game at their companies».

RusHydro MITSUBISHI HITACHI POWER SYSTEMS YOKOGAWA

KASPERSKY lab

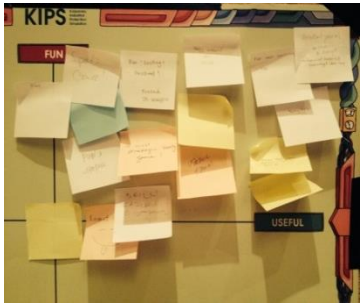
KIPS GAME OUTCOME IS PRACTICAL AND VALUABLE

Players by themselves come to the conclusions, important and actionable for their everyday job on CyberSecurity:

- Cyber attacks hurt revenues,
  need to be addressed from top-management level,
- Cooperation between IT and OT people is essential for ICS cybersecurity success,
- Effective security budget is much smaller than revenue you risk losing, and don't require Millions,
- People get used to particular security controls and its importance (audit, trainings, anti-virus, etc).

"Attendees not only realize the cost of cyber attacks but more amazingly, how important it is to spend cyber security funding wisely"

We at CERN have a huge number of IT and engineering systems, with thousands of people working on them. Thus, from a cybersecurity perspective, increasing awareness and engaging people to take care about cybersecurity is as crucial as the technical controls. Kaspersky Lab's training proved to be engaging, bright and efficient.
- Stefan Luders, CERN CISO



KIPS SCENARIOS – FROM BEGINNER TO ADVANCED

Level 1: Understanding the cyber security importance, building the cross-domain team

- Scenario: Playing water plant or power generation station
- Threats: Facing generic and ICS-specific threats
- Goals: Maintain the revenues, solve the incident, build cyber security system

Level 2: Understanding the sophisticated incidents, think out-of-the-box

- Scenario: Combined Circle Gas Turbine power generation station
- Threats: Facing advanced ICS-specific threats
- Goals: Maintain the revenues, identify the root-cause of the incident, build cyber security

APPENDIX: LOGISTICAL REQUIREMENTS FOR KIPS

Facilities, Setup, Announcements

KIPS SETUP

- Group: 20-200 people, split into teams comprised of:
- A mix of 3-4 people from Manager, Engineer, CISO/IT Security
  - Its better to have at least 1 member from each role/function
  - Teams may consist of people from different or the same company
  - People may know each other prior to the game, or may not
- Time: 2 hours (briefing, play, debriefing and discussion)
- Separate event, or session inside existing event/conference/seminar

KIPS PREPARATIONS AND WORK SPLIT

Kaspersky Lab will provide:

- Advertising and details for game invitations
- Printed game materials (fields, cards)
- Facilitator team to run the game
- Optional presentations (Threat Intelligence, technology approaches for Industrial Cyber Security)

Requirements for the hosting partner:

- ❑ Facility (room, equipment)
- ❑ Invitations and registration of the players

KASPERSKY lab

TECHNICAL REQUIREMENTS

- **Room**: ~3m^2/person, no columns, regular form
- **Time**: The game takes 2 hours, and the room must be available for 2 hours prior to the game for preparation and setup
- **Equipment**: Projector (6 - 8 lumens), Screen, Sound system (speakers, remote control, microphones)
  - 1 iPad per team + Wi-Fi and internet access (for KIPS game server access)
- **Furniture**: Tables of participants for 4 people (rectangular size not less than 75 * 180 cm, or round with no more than 1.5 m diameter), Participants should sit in groups of 4 at the tables. Tables for co-host, Chairs on the number of participants at the tables

KIPS ANNOUNCEMENT EXAMPLE

Attendees will play **KIPS, the Kaspersky Infrastructure Protection Simulation,** a role playing game developed by **Kaspersky Lab,** a global leader in cyber security.

It features a simulated water utility trying to accomplish its mission to produce and sell water to the community, while dealing with and resolving a number of unexpected IT events. Every response the team makes will have a knock-on effect on the running of their plant. Each utility is staffed by four participants in different roles who have to analyze data and make decisions despite uncertain information and limited resources! Sounds like real life? That's the point, and this is your chance to convince your team to test your strategy in a competitive environment!

Players will thrive on basic OT and IT knowledge, and lessons learned from the other primers on ICS and IT security will certainly not be wasted.