# BUSINESS SIMULATION ON CYBERSECURITY

*Kaspersky CyberSafety training for senior managers*

# KASPERSKY INTERACTIVE PROTECTION SIMULATION

*An effective way of building cybersecurity awareness among top managers and decision makers*

## THE "PEOPLE PROBLEM"

One of the biggest security challenges is that different senior management roles view cybersecurity from different perspectives, and have different priorities. This can result in a sort of decision-making "Security Bermuda Triangle":

- Business see security measures as a contradiction to their business goals (cheaper/faster/better),
- IT Security Managers may feel that cybersecurity as an infrastructure and investment issue moves outside their remit,
- Managers tasked with cost control may not see how cybersecurity spending relates to revenues and saves rather than generates cost.

Mutual understanding and partnership between these 3 are crucial to successful cybersecurity. However, traditional awareness formats, like lectures and red/blue exercises, are flawed: lengthy, over-technical, and unsuited to busy managers, and they fail to build "common language" at the common sense level.

## WHAT IS KIPS?

Kaspersky Interactive Protection Simulation (KIPS) is an exercise that places IT security teams from corporations and government departments into a simulated business environment facing a series of unexpected cyber threats, while trying to maximize profit and maintain confidence.

The idea is to build a cyber defense strategy by making choices from amongst the best pro-active and re-active controls available. Every reaction made by the teams to the unfolding events changes the way the scenario plays out, and ultimately how much profit the company makes... or fails to make.

Balancing engineering, business, and security priorities against the cost of a realistic cyber attack, the teams analyze data and make strategic decisions based on uncertain information and limited resources. If that sounds realistic, it should do, because each of the scenarios is based on real-life events.

### WHY KIPS IS AN EFFECTIVE EXERCISE?

KIPS training is targeted at business system experts, IT people and line managers, and should increase their awareness of the risks and security problems of running modern computerized systems.

Each of the competing teams of 4-6 people is tasked with running a business (water purification plant, bank, etc.) in the most efficient way. This enterprise consists of some production facilities and computers controlling it. During the rounds of the game, production facilities generate revenues / public welfare / business results. However, the teams also have to face cyberattacks potentially impacting enterprise performance.

In order to defend their enterprise, each team has to take strategic, managerial and technical decisions while taking operational constraints into account and maintaining a high level of revenue.

KIPS Game is a dynamic awareness program based on “learning by doing”:

- Fun, engaging and fast (2 hours)
- Team-work builds cooperation
- Competition fosters initiative & analysis skills
- Gameplay develops understanding of cybersecurity measures

After the KIPS Game, players come to the important and actionable conclusions for their everyday job:

- Cyberattacks hurt revenues, and need to be addressed from top-management level,
- Cooperation between IT and Business people is essential for cybersecurity success,
- Effective security budget is much smaller than revenue you risk losing, and does not require millions,
- People get used to particular security controls and its importance (audit, training, anti-virus, etc).

*“What does emerge from the exercise, though, is that some of the first and most basic strategic decisions you take, such as security audits and training, password changes and patch management, will help enormously with the incident responses you may have to make later on.”*

*Mark Jenkins · December 16, 2015 ICT Qatar*
*www.digitalqatar.qa/en/2015/12/16/let-the- cyber-games-commence*

# ENTERPRISE KIPS SCENARIOS FOR ALL INDUSTRY SECTORS

KIPS training shows to participants:

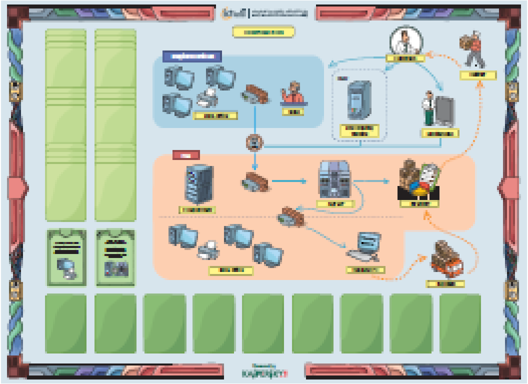
- A real role of the cybersecurity in business continuity and profitability,
- Highlights the emerging challenges and threats that are coming in nowadays,
- What are the typical mistakes companies are doing when building the cybersecurity,
- What kind of cooperation between business and security teams can help to maintain the stable operations of the enterprise and sustainability to the cyber threats.

As the enterprise experiences a cyberattack, the players experience the impact on production and revenues, and learn to adopt different business and IT strategies and solutions in order to minimize the impact of the attack and to earn more money.

Each of the scenarios focuses on the respectful thereat vectors, allows discovering and analyzing the typical mistakes in building the cybersecurity and incident response procedures in the corresponding industry.

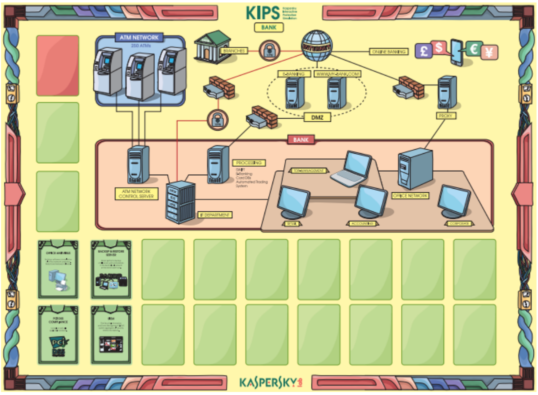
## SCENARIOS AVAILABLE

### CORPORATION



Protecting the enterprise from ransomware, APTs, automation security flaws.

### BANK

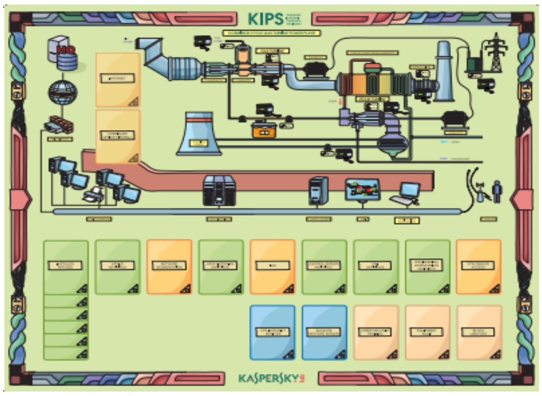


Protecting the financial institutions from high-level emerging APTs, like Tyukpin, Carbanak

### GOVERNMENT ONLINE SERVICES

Protecting the public web servers from attacks and exploits

### POWER STATION



Protecting industrial control systems and critical infrastructure

## REFERENCES AND CASE STUDIE

Since its inception in 2013, KIPS Game was played by 5000 industrial security professionals from 20 countries.

- KIPS has been translated to English, Russian, German, French, Japanese, Spanish, Portuguese,
- KIPS was used by government agencies such as ICTQatar, CyberSecurity Malaysia, Czech's NSA, Netherlands Cyber Security Centrum, to boost the awareness in the Critical Infrastructures, training hundreds of experts from national critical infrastructure companies,
- KIPS is used in enterprises like BASF (world top chemical manufacturer), CERN (Large Hadron Collider), Mitsubishi, Yokogawa, RusHydro, Panasonic, ISA (International Society of Automation), to train their own engineers, developers, customer-facing personal to note and take care about cybersecurity in the industrial automation environments,
- KIPS is licensed by leading education authorities like SANS Institute, used in the cybersecurity training programs delivered to SANS students worldwide,
- KIPS has been licensed by Security service providers and vendors, including Mitsubishi-Hitachi Power Systems, to be used as the training course for the end-customers from the Critical Infrastructure sectors.

### QUOTES AND REFERENCES ON KIPS GAME

*The Kaspersky Industrial Protection Simulation was a real eye-opener and should be made mandatory for all security professionals.*

Warwick Ashford, Computer Weekly

*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

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

Joe Weiss PE, CISM, CRISC, ISA Fellow

*We have to built a network of people based on affiliation and cooperation and the KIPS is a perfect way how to kick it off.*

Daniel P. Bagge, Národní centrum kybernetické bezpečnosti, Chezh Republic

## DELIVERABLES

Each KIPS training consists of:

- 2 hours KIPS Game (briefing, play, debriefing and discussion), 1 scenario,
- Up to 100 participants,
- Run by professional certified KIPS trainer from Kaspersky Lab or authorized training partners.

**Kaspersky Lab will provide:**

- The KIPS description for invitations
- KIPS materials (Game Fields, Cards) used during the KIPS session, and KIPS software
- Facilitator team to run the game

**Customer is responsible for:**

- Room, iPads[1], AV Equipment, Internet access
- Invitations and registration of the players.

### RECOMMENDATIONS ON HOW TO PREPARE FOR KIPS SESSION

**Schedule**: Plan KIPS as separate event, or session inside existing event/ conference/ seminar (in this case the optimum time for KIPS is the evening of the first day)

**Group**: 20-100 people, split into teams of 3-4 people, ideally each team is a mix of people from Management, Engineers, CISO/IT Security:

- it is better to have at least 1 member from each role/function,
- teams may consist of people from different or the same company/ department,
- people may know each other, or may not.

**Setup**: The game takes 2 hours, but the room must be available to Kaspersky Lab facilitator team for 2 hours prior to the game for preparation and setup

**Room**: Plan ~3m$^2$/person, no columns, regular form

**AV Equipment**: Projector (6 - 8 lumens), Screen, Sound system (speakers, remote control, microphones)

**Wi-Fi** with internet access (for KIPS game server access), from 4Mbps

**1 iPad per each team** (4 persons) with Wi-Fi support (iPad with Retina is better), or other tablets

**Furniture**: Tables of participants for 4 people (rectangular size not less than 75x180 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

[1] Kaspersky Lab can provide iPads at extra charge, approx. $100 per iPad.

# TRAIN-THE-TRAINER AVAILABLE

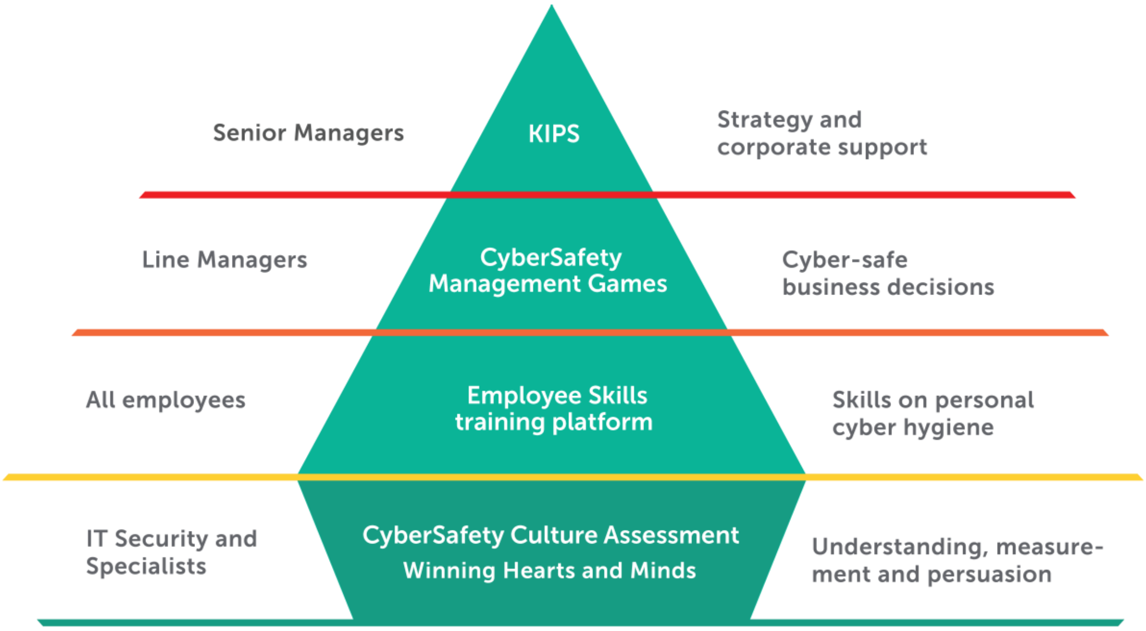
For the cases when the customer want to use KIPS to train a wider number of employees, managers and experts from multiple departments or sites, it may be useful to purchase the license to KIPS training, educate internal trainers and run KIPS sessions at the customer own pace and convenience.

Such license is available from Kaspersky Lab and includes:

- The right to use the KIPS training program internally,
- The set of training materials and the right to use/reproduce it,
- Login/password for the KIPS software server,
- Trainer’s guide, education and training for program leaders o/n how to run KIPS training,
- Maintenance and support (updates and support for KIPS software and training content),
- Optional customization of the KIPS Scenario (extra fee applies).

# KASPERSKY SECURITY AWARENESS TRAINING PRODUCTS

Interactive Protection Simulation training is a part of Kaspersky Security Awareness portfolio, based on CyberSafety Culture methodology. Cyber Safety Culture development by set of awareness trainings with gamification, for all levels of the organization structure, managed by Security and HR teams.


Senior Managers
KIPS
Strategy and corporate support
Line Managers
CyberSafety Management Games
Cyber-safe business decisions
All employees
Employee Skills training platform
Skills on personal cyber hygiene
IT Security and Specialists
CyberSafety Culture Assessment
Winning Hearts and Minds
Understanding, measurement and persuasion

## COMPREHENSIVE BUT SIMPLE AND STRAIGHTFORWARD

- Wide range of security issues
- Familiar environments
- Engaging training process
- Practical exercises
- Language suitable for non-IT people

## BUSINESS BENEFITS

- As much as 93% probability of using the knowledge in the daily work
- Decrease the number of incidents by up to 90%
- Reduce the cyber risk monetary volume by 50-60%
- Translate the cybersecurity from IT-jargon to business language, and get business management involvement
- Get measurable cybersecurity awareness program results
- Provide ROI from investment into the Security Awareness more than 30x times