Kaspersky Interactive Protection Simulation

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

kaspersky.com/awareness
#truecybersecurity
Kaspersky Interactive Protection Simulation

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, overtechnical, 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 business decision makers 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 cyberattack, 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 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).
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 cyberthreats.

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 threat vectors, allows discovering and analyzing the typical mistakes in building the cybersecurity and incident response procedures in the corresponding industry.

Enterprise KIPS Scenarios for All Vertical Sectors

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

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

**Oil & Gas**
Exploring influence of variety of threats – from website deface to a highly actual ransomware and a sophisticated APT.

**e-Goverment**
Protecting the public web servers from attacks and exploits

**Power station or Water plant**
Protecting industrial control systems and critical infrastructure from Stuxnet-style cyberattack.

**Transportation**
References and Case Studies

KIPS Game was played by industrial security professionals from 50+ countries.

- KIPS has been translated to English, Russian, German, French, Japanese, Spanish EU, Spanish LA, Portuguese, Turkish, Italian.
- KIPS was used by government agencies such as 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.

Two forms of KIPS training

KIPS Live

More limitations, but stronger engagement due to on-site presence and face-to-face competition. Plays as a team-building event as well.

- up to 80 trainees in the same room
- the same language for all participants
- a trainer and an assistant on site
- printed materials are essential

KIPS Online

Perfect for global organizations or public activities. Can be combined with KIPS Live to add some remote teams to the on-site event.

- up to 300 teams (= 1000 trainees) simultaneously, from any location
- different teams can choose a game interface in different languages
- a trainer leads a session via WebEx

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 Lab has launched a family of computer-based gamified training products that utilize modern learning techniques and address all levels of organizational structure. This approach helps create a collaborative cybersafety culture which engenders a self-sustaining level of cybersecurity throughout the organization.

- **Senior Managers**: Strategy and corporate support
- **Line Managers**: Cybersafe business decisions
- **All Employees**: Individual cyber-hygiene skills
- **CISO**: analyze & improve attitudes
- **KIPS**
- **CyberSafety Management Games**
- **Kaspersky Security Awareness Platform**
- **CyberSafety Culture Assessment**
- **CyberSecurity for IT Online**
- **General IT**: First line of incident response

### Key Statistics
- **Reduction in the total number of incidents**: up to 90%
- **Reduction in the financial impact of incidents**: not less than 50%
- **Probability that knowledge will be applied in everyday work**: up to 93%
- **ROI from investment in security awareness**: more than 30x
- **Of participants willing to recommend the experience**: amazing 86%

**Setting objectives & choosing a program**
- Setting goals based on global data
- Benchmarking against world/industry averages

**Learning management**
- Learning automation
- Self-adjusting learning path
- Calculation on time spent

**Reporting & analytics**
- Actionable reports anytime
- On-the-fly analysis of potential for improvement

**Program efficiency & appreciation**
- True gamification
- Competition & challenge
- Overload prevention