MANAGING CYBERSECURITY – AWARENESS BY EXPERIENCE

Kaspersky Interactive Protection Simulation –
security awareness training for top managers and decision makers

KASPERSKY lab

CYBERSECURITY TODAY – LOST IN A ‘CORPORATE BERMUDA TRIANGLE’

CEO

Does not see how cybersecurity spendings relate to Revenues

SECURITY

Focus on protecting the confidential information

Many security controls are under IT management

IT & BUSINESS MANAGERS

Focused on business efficiency, automation, new technologies

Mutual understanding and daily attention to cyberthreats between these 3 are crucial to successful cybersecurity in the modern business

CYBERSECURITY TODAY – LOST IN A ‘CORPORATE BERMUDA TRIANGLE’

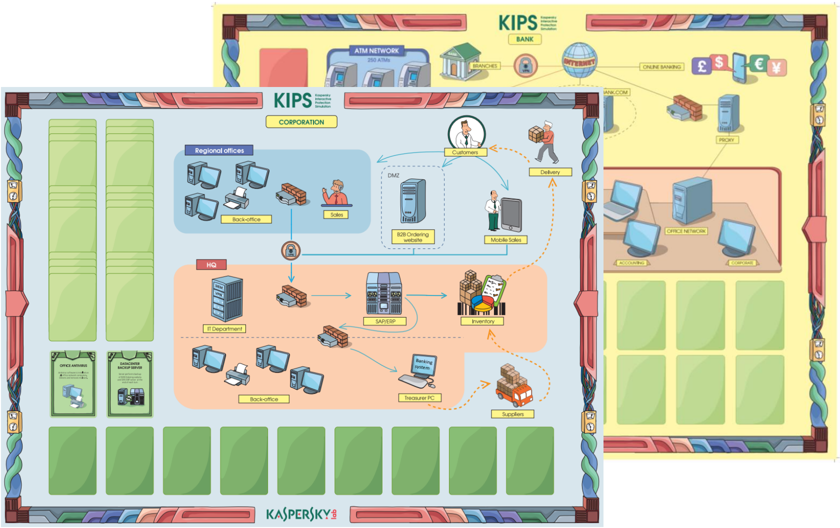
Lectures and technical red/blue exercises are flawed:

- 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 INTERACTIVE PROTECTION SIMULATION (KIPS)

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



PREPARE PR STATEMENT

Notify authorities about the security breach. Prepare and issue a PR statement disclosing the breach, explaining actions taken and giving recommendations to customers on how to avoid it.

PERFORM PENETRATION TEST

Hire security professionals to perform a penetration test at your company. This identifies vulnerabilities and security issues and provides recommendations on fixing them. May affect the business performance if security holes are discovered.

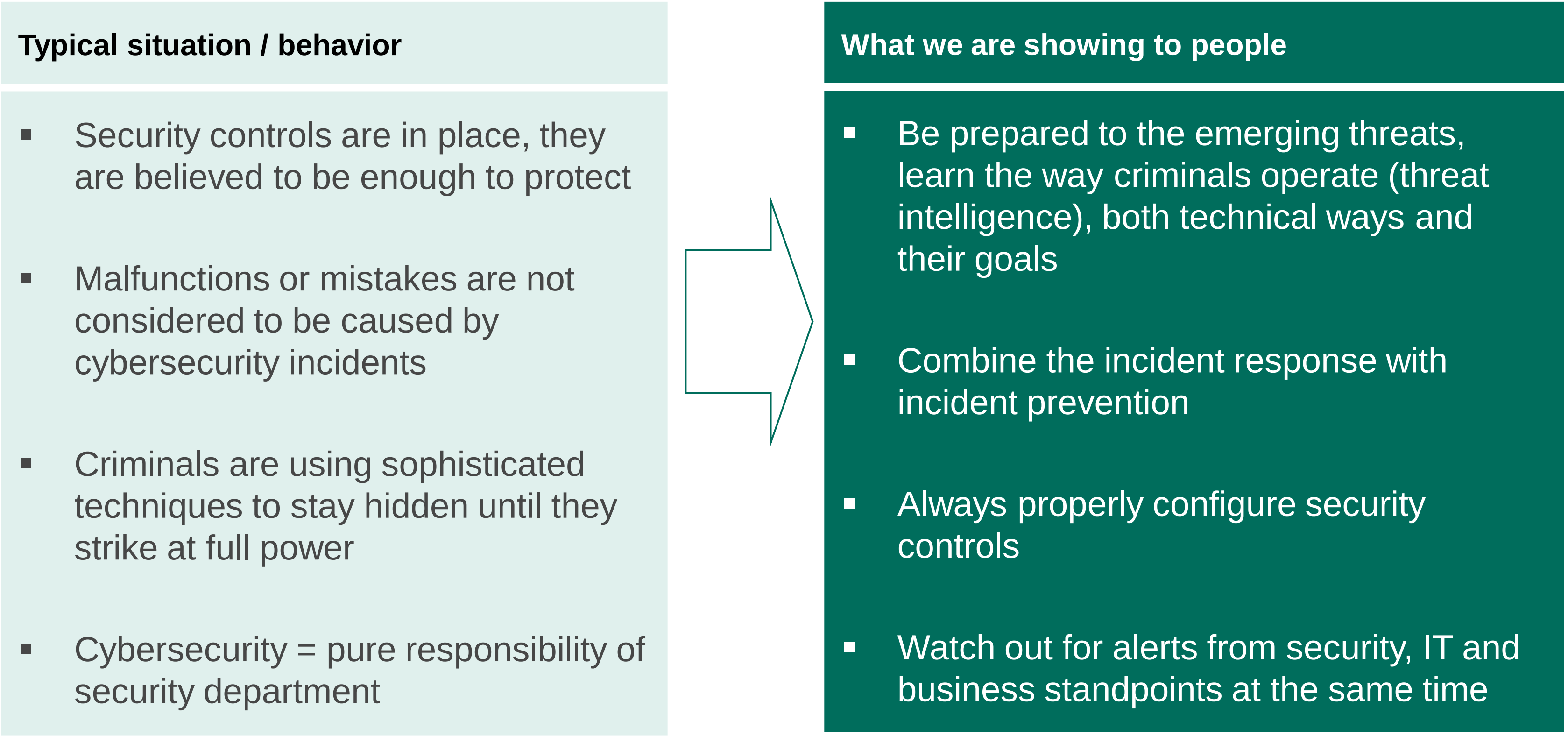
INSTALL SHELLSHOCK PATCH

Patch the web server vulnerability that allows remote attackers to take full control of web servers exposed to the Internet. The patch is applied to all corporate web servers.

CONDUCT CYBERSECURITY TRAINING

Perform cybersecurity training for all of the corporation's employees.

SIMULATION IS CHANGING THE ATTITUDE



Typical situation / behavior

- Security controls are in place, they are believed to be enough to protect
- Malfunctions or mistakes are not considered to be caused by cybersecurity incidents
- Criminals are using sophisticated techniques to stay hidden until they strike at full power
- Cybersecurity = pure responsibility of security department

What we are showing to people

- Be prepared to the emerging threats, learn the way criminals operate (threat intelligence), both technical ways and their goals
- Combine the incident response with incident prevention
- Always properly configure security controls
- Watch out for alerts from security, IT and business standpoints at the same time

FOUR KIPS SCENARIOS AVAILABLE

Corporation

Manufacturing and sales with B2B ordering portal, regional sales and delivery

Bank

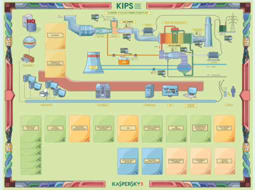
Bank with own ATM network; with retail and corporate business

E-Government

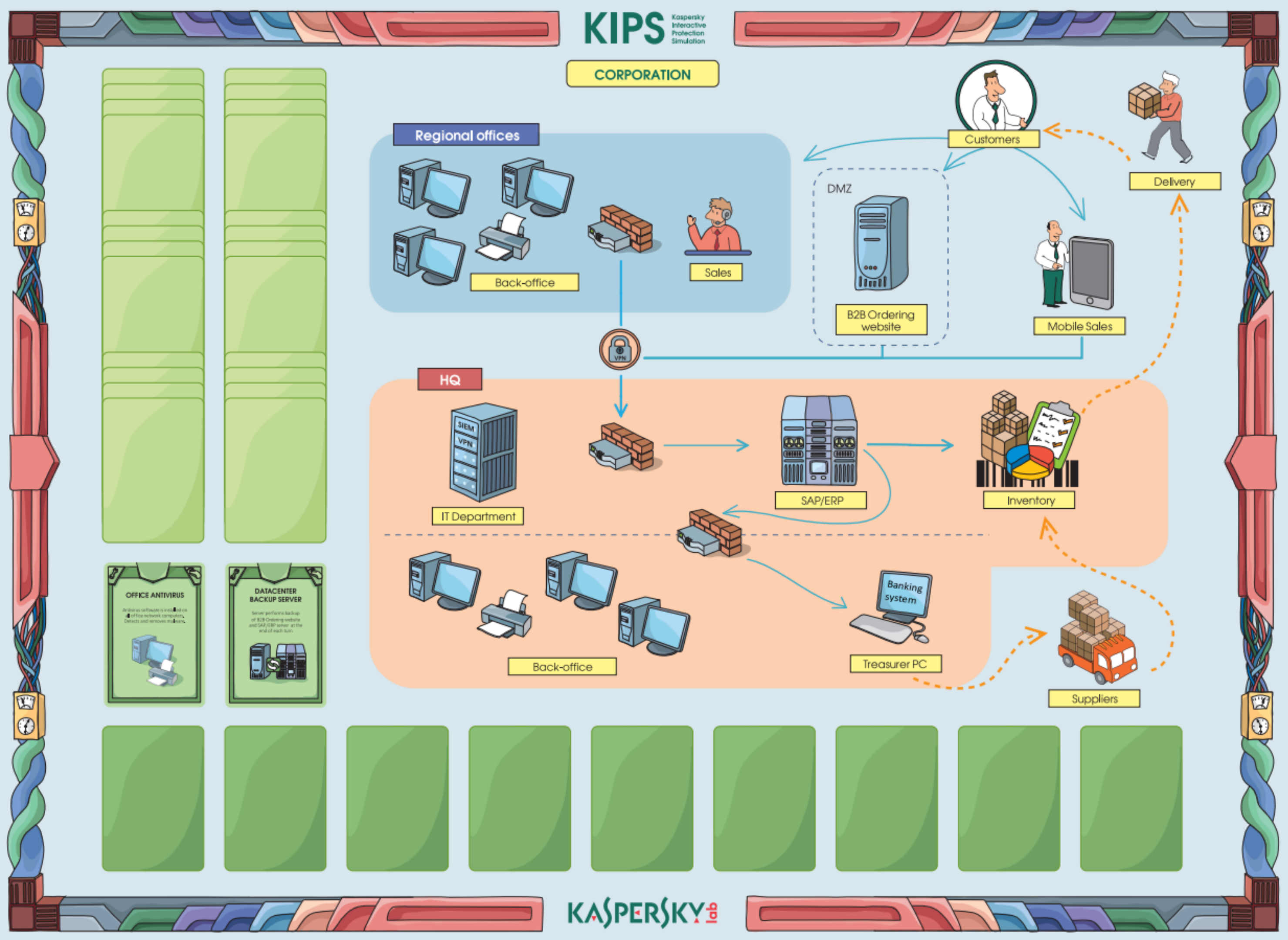
Web servers and portals to run government online services

Industrial

Industrial control systems and critical infrastructure (power station or water plant)



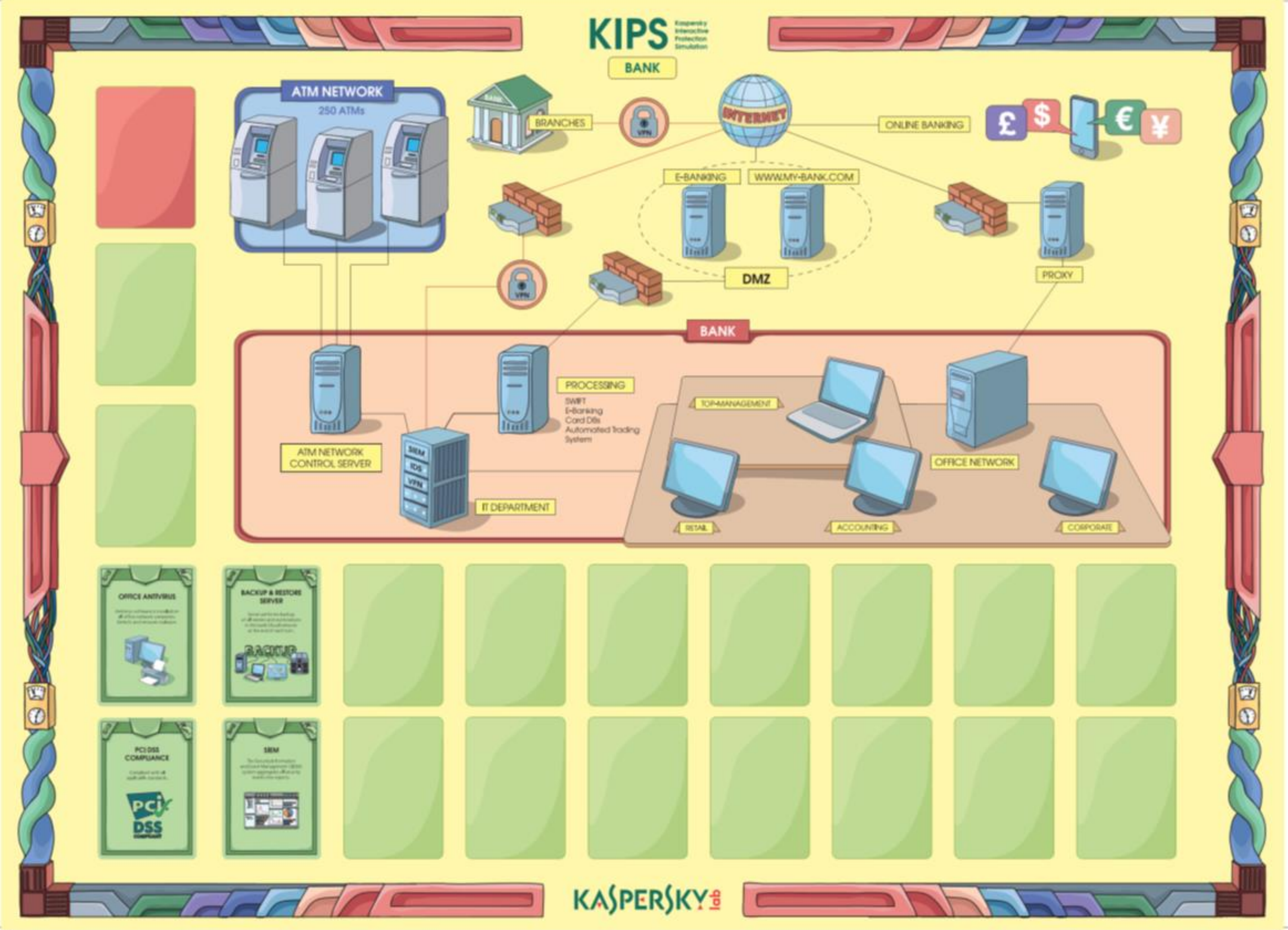
- Each of the scenarios focuses on the respectful threat vectors, allows to discover and analyze the typical mistakes in building the cybersecurity and incident response procedures in the corresponding industry
- KIPS training shows to participants the real role of the cybersecurity in business continuity and profitability; highlights the emerging challenges and threats which are coming in nowadays; describes typical mistakes companies are doing when building the cybersecurity; and encourages a cooperation between business and security teams – a cooperation which helps to maintain the stable operations and sustainability to the cyberthreats



CORPORATION

Teams compete running a simulated company manufacturing goods, with B2B customers buying directly and via online channels, suppliers shipping spare parts. Some security controls are in place, and company is earning decent profit.

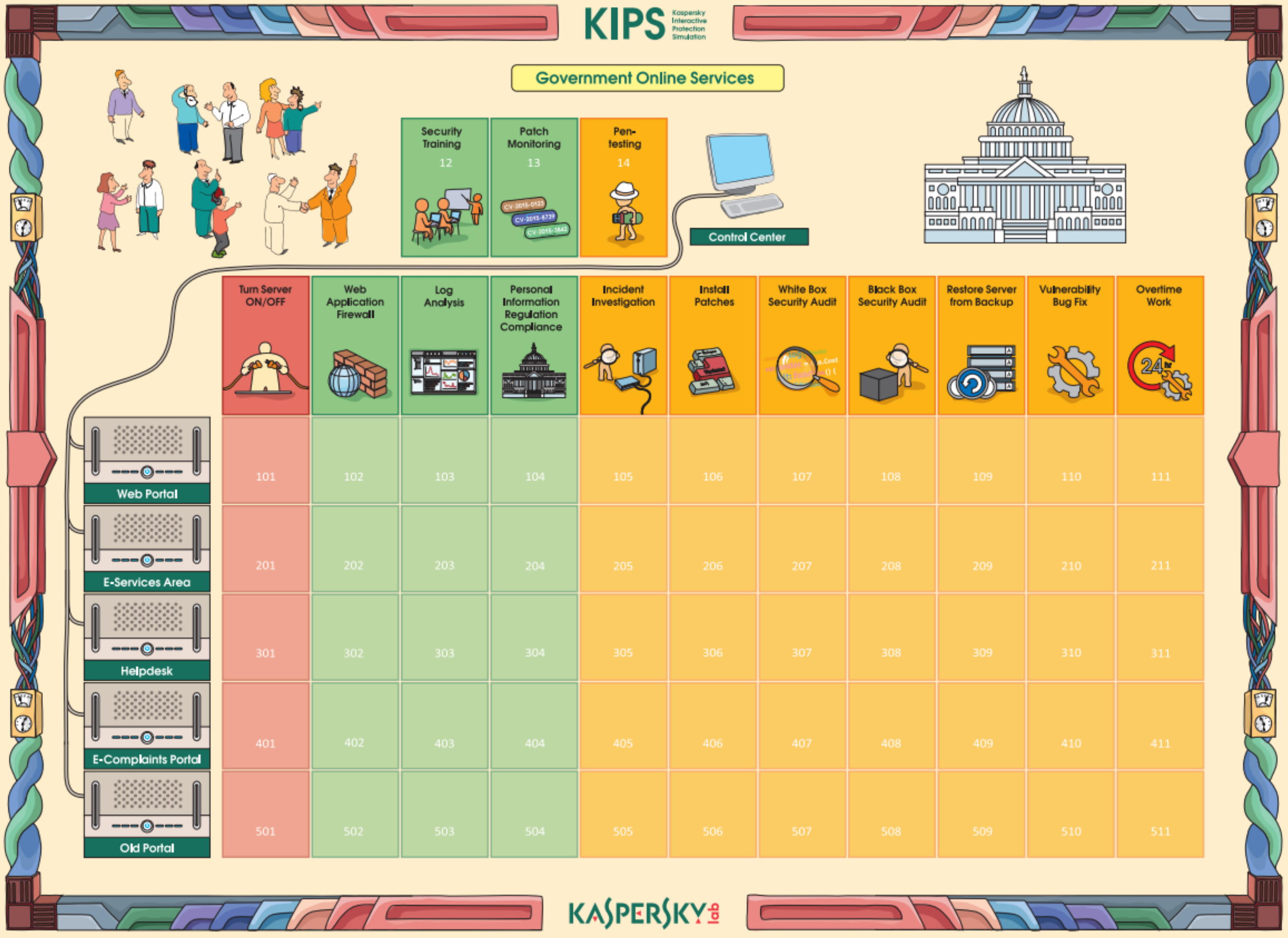
However, as the company experiences a series of attacks – **Heartbleed**, **APT**, **B2B Ransomware**, **Insider** – they see the unexpected impact on profits, and have to adopt financial, IT or Security strategies and solutions to minimize the impact of the attack and keep their profits.



BANK

Teams compete running a simulated regional bank with ATM network, trade business, online banking, a lot of security controls in place, compliant to security standards, predictable fraud level, and earning profit.

However, as the bank experiences a series of attacks – **Carbanak, Tyupkin, Cryptor, Black Energy** – they see the exponentially growing impact on profits, and have to adopt different financial, IT or Security strategies and solutions to minimize the impact of the attack and keep their profits.

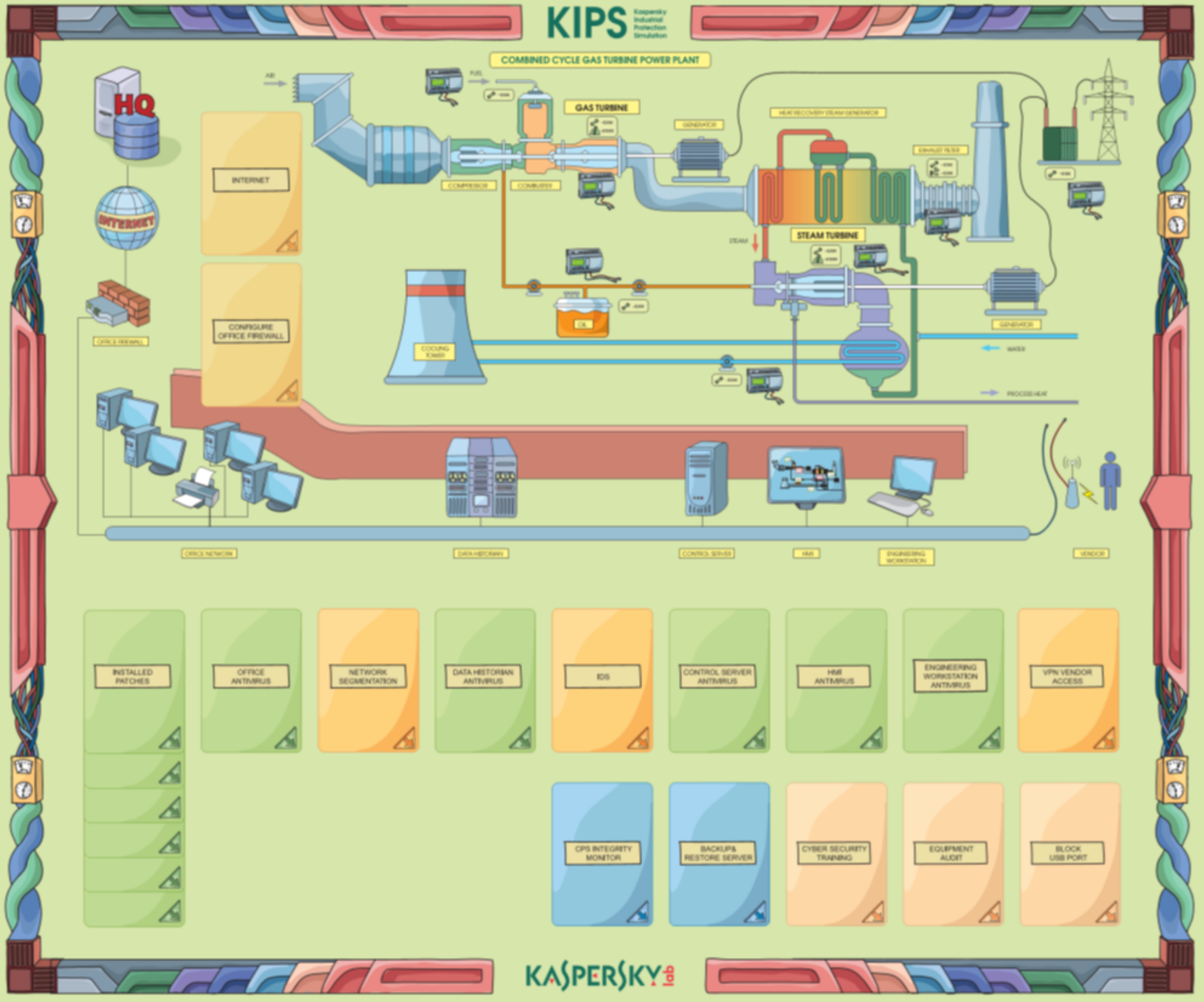


	Turn Server ON/OFF	Web Application Firewall	Log Analysis	Personal Information Regulation Compliance	Incident Investigation	Install Patches	White Box Security Audit	Black Box Security Audit	Restore Server from Backup	Vulnerability Bug Fix	Overtime Work
Web Portal	101	102	103	104	105	106	107	108	109	110	111
E-Services Area	201	202	203	204	205	206	207	208	209	210	211
Helpdesk	301	302	303	304	305	306	307	308	309	310	311
E-Complaints Portal	401	402	403	404	405	406	407	408	409	410	411
Old Portal	501	502	503	504	505	506	507	508	509	510	511

eGOVERNMENT

Teams compete running a set of public web services for the citizens in the Agency’s data center, with the goal of providing services in a timely manner, and protecting sensitive personal information of citizens.

However, as the hackers are seeking the way to harm Agency reputation and they experience a series of attacks using the vulnerabilities in their systems, the customer satisfaction drops dramatically and they have to adopt different strategies and solutions to minimize the impact of the attack and keep their reputation high.



INDUSTRIAL

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.

We also have an easier version of industrial scenario – Water Plant.

KIPS PLAYED BY 10,000 SECURITY PROFESSIONALS FROM 40+ COUNTRIES

Atlanta, USA

ComputerWeekly.com

"The Kaspersky Interactive Protection Simulation was a real eyeopener and should be made mandatory for all security professionals."

www.computerweekly.com/feature/Interactive-cyber-attack-a-dangerous-game

Kuala-Lumpur, Malaysia

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

SANS CERN ISA TOSHIBA

ROSATOM RusHydro YOKOGAWA MITSUBISHI HITACHI POWER SYSTEMS

CASE STUDY. STAR-3 – NATIONAL CYBER DRILL OF QATAR. 2015

National Cyber Drill was based on Kaspersky Interactive Protection Simulation

Games were held for 4 different economy sectors:

- Financial
- Industrial
- Corporate
- Government

KIPS OUTCOME IS PRACTICAL AND VALUABLE

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

- Cyber incident is not a virus, it is a damage to the business
- More automation brings more “patchwork”, so it is crucial to fix the security holes they bring
- It is not enough only for IT Security to take care about cyberrisks, business must participate

CERN

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, CISO, CERN

KASPERSKY lab

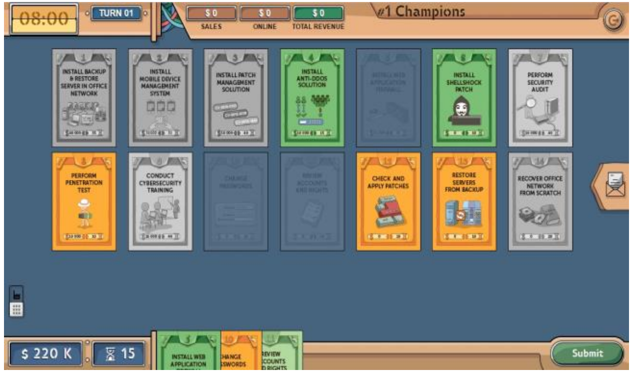
TWO FORMS OF KIPS TRAINING

KIPS Live

- 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

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

KIPS Online


08:00
TURN 01
$ 0
SALES
$ 0
ONLINE
$ 0
TOTAL REVENUE
#1 Champions
INSTALL BACKUP & RESTORE SERVER IN OFFICE NETWORK
INSTALL MOBILE DEVICE MANAGEMENT SYSTEM
INSTALL PATCH MANAGEMENT SOLUTION
INSTALL ANTI-DDOS SOLUTION
INSTALL SHELLSHOCK PATCH
PERFORM SECURITY AUDIT
PERFORM PENETRATION TEST
CONDUCT CYBERSECURITY TRAINING
CHECK AND APPLY PATCHES
RESTORE SERVERS FROM BACKUP
RECOVER OFFICE NETWORK FROM SCRATCH
$ 220 K
15
INSTALL WEB APPLICATION
HANGE SSWORDS
REVIEW CCOUNTS D RIGHTS
Submit

- 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

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

TRAINING PROCESS OVERVIEW

Game rules and housekeeping explained

Trainer tells about the game and its rules, trainees listen and follow slides on a big screen or via WebEx.

25 minutes

KIPS is played by teams

Players read news and decide on actions by choosing cards according to their strategy and budget and time limitations.

After each turn a rating is updated.

Trainer facilitates, encourages and controls timing.

50 minutes

Ideal scenario unveiled and lessons learned

Trainer tells about threats met by players, unveils the ideal scenario and draw participants to conclusions and practical takeaways.

25 minutes

Results announced – congratulations to winners!

Participants can be invited to share results and photos on social media.

10 minutes

DELIVERY OPTIONS AND LANGUAGES

Kaspersky Lab trainer

Our certified trainer (available in all regions)

Train-the-trainer

License to use the training **inside the enterprise** by internal trainers or as a **training center license**

Custom scenario

Based on the customer cybersecurity environment

KIPS software and printed materials are available in a number of languages*, and new localizations are being added regularly.

English

Russian

German

Japanese

French

Spanish EU

Spanish LA

Portuguese

Turkish

Italian

* Please check with Kaspersky Security Awareness team if a specific scenario is available in your language – there can be some exclusions.

KIPS LIVE REQUIREMENTS

Group

20-80 people, split into teams comprised of 3-4 people

Room

~ 3m^2/person, no columns, regular form

Time

The game takes 2 hours, and the room must be available 2 hours prior to the game for preparation and setup

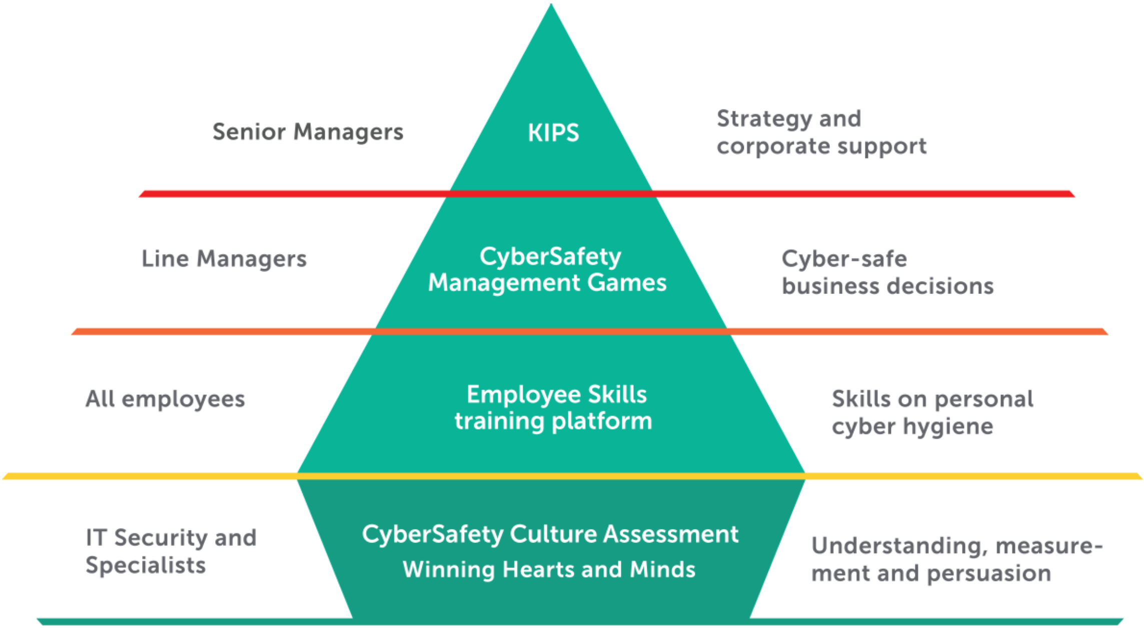
Equipment

Projector, Screen, 1 iPad per team + Wi-Fi, Sound system (speakers, microphones)

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

KASPERSKY SECURITY AWARENESS TRAINING PRODUCTS



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

- 93% likelihood to apply knowledge
- 90% decrease in the number of incidents
- 50-60% reduction* of the cyber risk monetary volume
- 30x ROI
- Measurable security awareness program results

* Aberdeen Group. Research as of 2014

Kaspersky Cybersecurity Awareness Training comprises of 5 elements which intermesh, but which are also fully effective if used separately.

WE PROTECT WHAT MATTERS MOST

KASPERSKY lab

www.kaspersky.com/awareness