KASPERSKY lab

CYBERSAFETY MANAGEMENT GAMES

IMMERSIVE LEARNING AND MOTIVATIONAL EXPERIENCE TO PROMOTE CYBER-SECURE DECISION-MAKING BY LINE MANAGERS

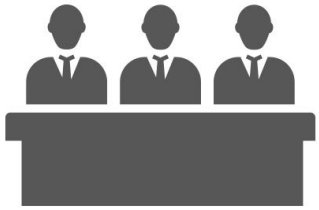
WHOM TO TRAIN

LINE MANAGERS AS A FORCE TO ENSURE CYBER-SAFE WORKING ENVIRONMENT FOR THE ENTIRE COMPANY

Typical state of cybersecurity in Enterprises (not-that-bad scenario):

Organizational level

Dedicated IT Security department.
Overall problem recognition.
High-level cybersecurity strategy in place.



Employee level

Once-a-year compliance training on cybersecurity.
Cybersecurity tip sheets in some office spaces.

All organizations are taking steps to address cyberthreats by setting up IT security structures and training compliance. But is this enough?

- Does knowledge gained at training really drive employees' behavior? Or is it something else?
- Does business efficiency have to be sacrificed to achieve security?
- Do security officers feel that there are too few of them to reach every ear in their fight for cyber safety?

These challenges can only be addressed by engaging **line managers in making organizations cyber secure, without sacrificing efficiency. Only they** interact with employees on a daily basis and make business decisions. The answer lies in making cyber-safety the mandatory ingredient of everyday decision-making.

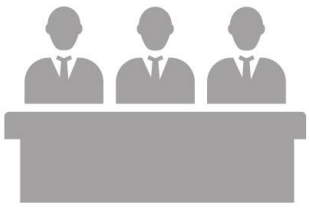
Normally, this is the biggest challenge for the Security team – how to engage management.

That's why Kaspersky Lab developed a special training program aimed at converting line/ middle managers into cybersecurity supporters and advocates.

Role of middle managers in a well-tuned cybersecurity environment:

Organizational level

Dedicated and well-communicating
IT Security department.
Actionable cybersecurity strategy.
Business process aligned
with cybersecurity principles.



Line managers level

Ensuring an effective use of cybersecurity principles in everyday work.
Support, surveilance and guidance for employees.

Employee level

Continuous cybersecurity education.
Regular and time-efficient assessments
with auto-adjustment of a learning path.

TRAINING OUTCOME

WHAT LINE MANAGERS WILL GAIN TO BECOME A PRIMARY INFLUENCE FORCE IN INCREASING CYBER HYGIENE

Kaspersky CyberSafety Management Games provide managers with **competence, knowledge and attitudes** essential to maintain secure working environment in their divisions.

✓ UNDERSTANDING
Inner adoption of cybersecurity measures as an important yet uncomplicated set of actions

Managers obtain:

- a sense of "why they **should care about security**",
- insights on how they look from **the perspective of cybercriminals**,
- a reframed **understanding of cyberthreats** and **possibilities to successfully avoid/ prevent them**.

✓ MONITORING
Seeing everyday working process through the cybersafety lens

Managers learn to:

- distinguish between **safe and unsafe behavior**,
- "Scan" daily events in typical workplaces to **pay attention to potentially threatening situations and direct employees toward safety**.

✓ CYBER-SAFE DECISION MAKING

Cybersecurity considerations as an integral part of business processes

Managers get the experience of:

- choosing an **optimal balance** between security precautions and business efficiency,
- planning and implementing business projects, while **estimating level of cyber-risks** at every stage and for every team involved,
- estimating how much time and money needs to be allocated to ensure cyber-safe decisions at every step of every project,
- Cooperating efficiently with the security team.

Managers become convinced that security measures **do not have to be complex and time-consuming,** while helping to avoid potentially enormous corporate and personal losses.

✓ REINFORCEMENT AND INSPIRATION

Influential leadership and helpful advice to employees

Managers are equipped to:

- correctly **answer employees' questions** on cybersecurity topics, or give adequate feedback on topics they are not sure about (e.g. redirecting the inquirer to IT security specialists or asking for more details by themselves),
- **maintain commitment** towards cybersecurity values and procedures, and **prevent skepticism** in regard to those values,
- motivate personnel to actively **learn and utilize cybersecurity techniques** every day
- finally, managers get their **own motivation towards cybersecurity** – while knowing that it won't hamper their business goals, personal priorities and time balance.

TRAINING FORMAT

ENGAGING COMPUTER-BASED PROGRAM WITH SHORT TRAINING MODULES

CyberSafety Management Games are specially designed to accommodate managers' focus and priorities as well as to challenge them with a scale, complexity and credibility of simulated work-related situations.

The training is powered by **purpose-built CyberSafety Management Games software**, combining gamification with comprehensive coverage of security topics. Examples, explanations and exercises are built into the software to support easy-to-manage training delivery process for the trainer.

This allows the training to be run by business trainer, not a security expert (all security-related content is included in the software).

***Threats from 10 Security domains**: AV/Apps, Data leak, Mobile, Web, Mail, Victim behavior, Social engineering, Security alerts, Vigilance skills, Policy breach*

It is presumed that participants have already had some level of cybersecurity "hard skills" – preferably have passed several modules of Kaspersky Employee Skills Training Platform. If they haven't, CyberSafety Management Games can be supplemented with a brief theoretical introduction.

TRAIN-THE-TRAINER AVAILABLE

For the cases when the customer want to use CyberSafety Management Games to train a wider number of employees, managers and experts from multiple departments or sites, it may be useful to purchase the license, educate internal trainers and run training sessions (on-site or online) at the customer own pace and convenience. Such license is available from Kaspersky Lab and includes:

- The right to use the CyberSafety Management Games training program internally,
- Training materials and the right to use/reproduce them,
- Login/password for the CyberSafety Management Games software server,
- Trainer's guide and facilitation training for program leaders,
- Maintenance and support (updates and support for software and training content),
- Optional customization of the Scenario (extra fee applies).

STANDARD TRAINING PROGRAM

Recommended training program consists of 3 modules, accompanied by short technical clarifications and reflections on errors made by students. Modules can be added or removed according to client's preference.

Program and setting can be adjusted or your particular needs (for a fee). But most of our customers are happy with a standard curriculum which embraces places and situations every company and every manager face.

Session 1. "Afraid of bad people, not computers broken by viruses"

2 hours

1. Identifying the cyber threats – "Open office"

2. Risk mitigation:
   - Suspicious vs. normal links
   - Weak password. *Exercise "Creating strong memorable passwords and password families"*
   - Suspicious vs. normal attachments
   - Non-authorized access to confidential information.
   - *Exercise "What can I do to mitigate the risk"*
   - Improper dissemination of the confidential information
   - Taking confidential data outside of the company. *Exercise "Assessing the business situation and risks involved"*
   - Unattended Flash-drive. *Exercise "What can I do to mitigate the risk"*
   - Installing unsigned-software
   - Phishing emails. *Exercise "How to spot fraudulent emails"*
3. *Exercise "Meet the criminals"*
4. Session conclusion
   - Remember: "Afraid of bad people, not computers broken by viruses"
   - Do: "Always think who can misuse what you do in the digital world"

Session 2. "You don't need to be a target to be a victim"

2 hours

1. Identifying the cyber threats – "On the move"
2. Risk mitigation Exercises
   - Disclosing emails – personal vs. corporate
   - Ignoring security updates
   - Posting in Social networks – neutral with information leak
   - Sharing a password. *Exercise "Assessing the business situation and risks involved"*
   - Installing app on corporate smartphone
   - Unlocked PC. *Exercise "What can I do to mitigate the risk"*
   - Suspicious link. *Exercise "Suspicious URL training"*
   - Using confidential information in a public place
   - Weak authentication via public Wi-Fi
3. Exercise "Victim's profile"
4. Session conclusion
   - Remember: "You don't need to be a target to be a victim"
   - Do: "Be harder target than the others"

Session 3. "CyberSafety is everyone's responsibility"

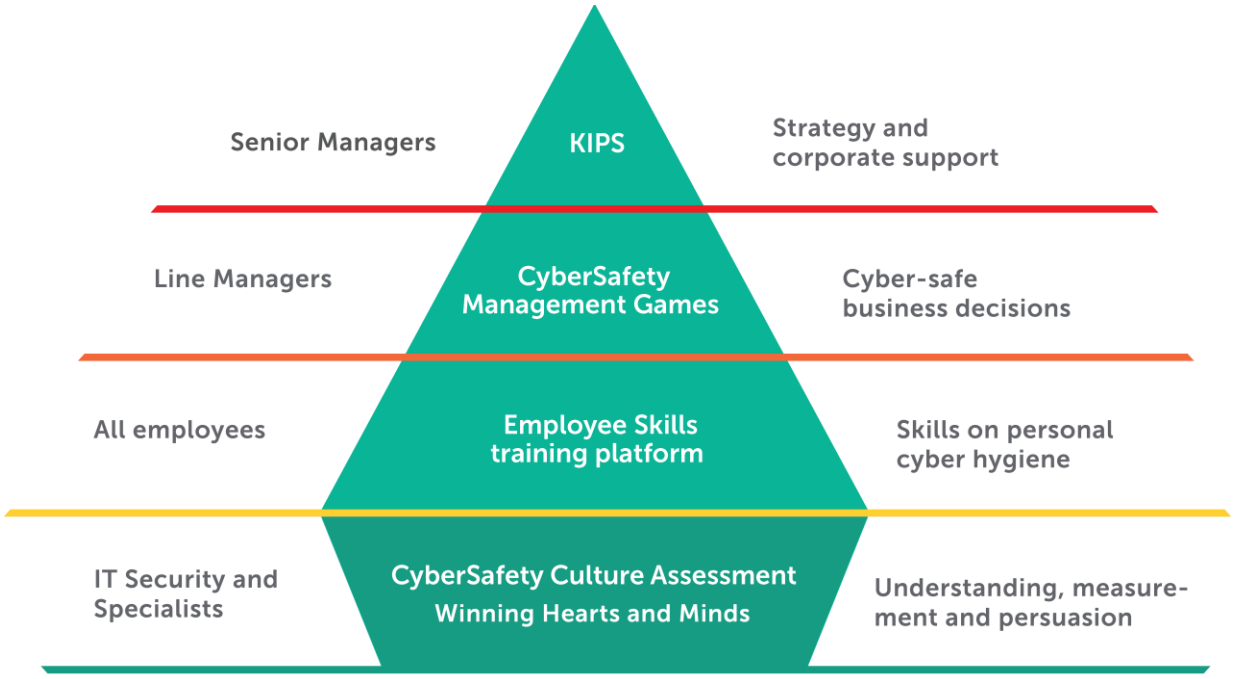
2 hours

1. Identifying the cyber threats – "Conference room"
2. Risk mitigation Exercises
   - Passwords reuse and storage
   - Accidental disclosure of confidential information. *Exercise "What can I do to mitigate the risk"*
   - DLP warnings
   - Social engineering attack. *Exercise "How to recognize social engineering"*
   - Ignoring IT Security
   - Sending confidential information outside the company. *Exercise "Assessing the business situation and risks involved"*
   - Malicious websites
   - Taking data outside of the company
   - Non-authorized access to confidential information
   - Outdated anti-virus
   - Solving business goal with security in place. *Exercise "Dialogue with the IT security department"*
3. *Exercise "Planning security as part of the business"*
4. Session conclusion
   - Remember: "CyberSafety is everyone's responsibility"
   - Do: "Cooperate with your IT Security team"

Kaspersky Security Awareness Training Products

CyberSafety Culture Assessment is a part of Kaspersky Security Awareness portfolio, based on CyberSafety Culture methodology. CyberSafety Culture is a set of values and attitudes that drives people's behavior, on an individual or corporate level.

We help customers develop a CyberSafety Culture, under the management of their security and HR teams, through a set of awareness training programs. The training programs utilize gamification and address all levels in the organization structure.



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