



# Cybersecurity for Executives Training

Digital technologies have a profound impact on every part of life, bringing greater opportunities, cost efficiencies, the ability to scale globally, and numerous other enriching benefits. But in order to fully benefit from them, security awareness and the proper use of cybersecurity skills is more important than ever.

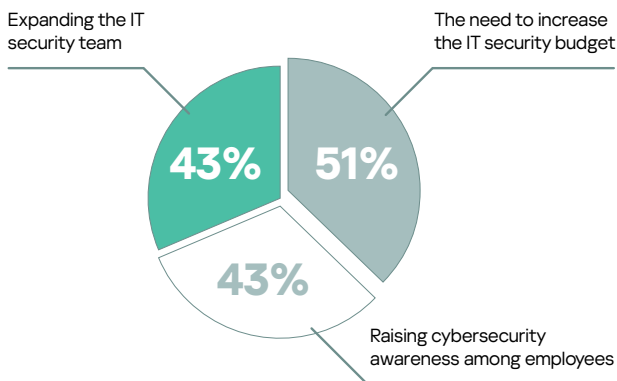
Successful cyberattacks and breaches lead, at best, to headaches for a company's IT, with minor disruptions to internal systems. At worst, they can devastate your organization. Staying ahead of security threats requires the active involvement not only of CISOs and IT, but of non-technical leadership as well, with a shared commitment to building a culture of cybersafety throughout your organization.

Having access to the highest level of security and confidential information, top managers are sought-after targets for cybercriminals. A lack of cybersecurity knowledge, gaps in essential cybersafety skills, and even honest mistakes by these executives can cost your business dearly.

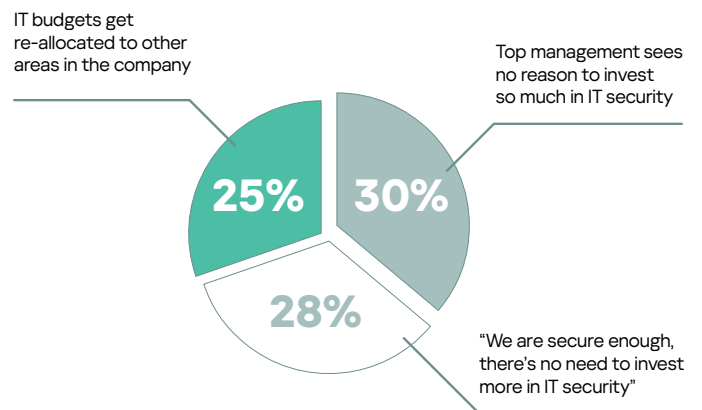
## Are C-level executives and IT security managers on the same page?

While cooperation between IT security teams and the board is beneficial for all businesses, only 50% of IT leaders believe that senior management fully understands cyber risks. In fact, 90% of IT decision-makers claim their business leaders would be willing to compromise on cybersecurity in favor of digital transformation, productivity, or other goals\*. This mindset makes discussing the importance of IT security budgets one of the top 3 most difficult conversations for IT staff to have C-level execs.

The three most difficult discussions include\*\*:



Top 3 reasons that IT security budgets for enterprises get reduced\*\*\*:



62% of managers admit that this disconnect between IT security and C-level executives has led to at least one cybersecurity incident\*\*

## C-suite engagement in cybersecurity – a challenge for educators

Enterprises where managers actively contribute to discussions and decisions about protecting their business from cyberthreats are better prepared for cyberattacks, and better equipped to quickly recover from them. The involvement of the CEO as a key influencer is vital to ensure consistent, effective security awareness throughout the organization. But they're busy people, with other priorities and packed schedules. How can they be encouraged to make the time for training?

The answer lies in training specifically tailored to their C-suite needs. A specially designed program that helps them understand the cybersecurity landscape, and the key connection between that landscape and business efficiency, while providing insights into the operational realities of building and applying cybersecurity strategies that benefit the entire organization.

\* A global study "Business friction is exposing organizations to cyber threats", Trend micro

\*\* "Fluent in Infosec", Kaspersky 2023

\*\*\* "Managing the trend of growing IT complexity", Kaspersky



# Kaspersky Executive Training & Cybersecurity for Executives

## Online Training: building cybersecurity awareness among top managers and decision-makers

Cybersecurity is an important aspect of revenue generation along with project management, financial instruments, and business efficiency. This is the focus of Kaspersky's course for executives. Business leaders and top managers learn the basics of cybersecurity through a tutor-led course which gives them a better understanding of cyberthreats and how to protect against them.

### What the training delivers

The course covers the critical and business-related aspects of cybersecurity, in accessible, non-technical language. It focuses on cybersecurity's ROI, and promotes mutual understanding and cooperation between departments when it comes to cybersecurity.

Executive Training is available in two formats: an interactive offline workshop, which is **Executive Training** led by a Kaspersky expert, and an online course – **Cybersecurity for Executives Online Training**.

**Cybersecurity for Executives Online Training consists of 6 topics:**

#### 1. Introduction to cybersecurity

- a. What cybersecurity is
- b. Why managers should be involved in cybersecurity
- c. Address by Eugene Kaspersky: from cyber defence to cyber immunity

#### 2. Cyber risks for businesses

- a. Business losses as a result of a cyberattack
- b. Measures and approaches to cyber risk management
- c. Case studies of successful and unsuccessful cyber risk management

#### 3. Cyberattacks and attackers' tools

- a. Attackers' tools: social engineering, malware, exploits, dark market
- b. Cyberattacks: types, success factors, targeted attacks, mass attacks, data leaks, how to protect yourself

#### 4. Protecting yourself and your company from cyberattacks

- a. Managers' cyber hygiene
- b. Staff cybersecurity training and awareness
- c. Cybersecurity at different levels of a company's maturity
- d. Cybersecurity audit and cybersecurity services

#### 5. Managing the consequences of cyberattacks

- a. How to react and respond to a cyberattack
- b. Cyber crisis management plan
- c. Incident communication

#### 6. The future of cybersecurity

- a. Cyberthreats: statistics and attack vectors
- b. Industry 4.0. and the Internet of Things
- c. Cyber immunity

The course was created by Kaspersky's top managers and leading cybersecurity experts. In total, it contains 50 lessons of 3-6 minutes each. It can be provided via access to a cloud platform or in SCORM to be integrated into your LMS.

These programs are part of Kaspersky's Security Awareness portfolio, which offers a range of engaging training options to boost your employees' cybersecurity awareness and empower them to play their part in the overall cybersafety of your organization.

There's a practical task and 5-10 questions for self-assessment and reinforcement of your new knowledge at the end of each topic. When you've completed all the tasks and lessons, you have to pass the final test.

Once you've done so, you'll receive your certificate of completion.

### Main benefits:

- **Easy to master:** microlearning + practical tasks + tests = knowledge consolidation and retention
- **Convenient format:** the online course is adapted for mobile and desktop
- **Based on deep knowledge of top management needs:** Kaspersky's top managers created this course
- **Practical guidelines and checklists:** contains ready-to-use materials

### Training outcomes

After completing the course, managers will be able to:

- Speak the same language as IT and information security specialists
- Develop a cyber crisis management plan together with their IT and IT security teams
- Plan effective incident communications
- Make strategic decisions based on cyber risk assessments
- Apply the rules of cyber hygiene
- Protect themselves from cyberthreats

To learn more please visit  
[kaspersky.com/awareness](https://kaspersky.com/awareness)

[www.kaspersky.com](https://www.kaspersky.com)