kaspersky BRING ON THE FUTURE

Kaspersky Incident Communications

Ensure your internal business processes are ready to disclose cyber-incidents

From the instant a cyber-incident is discovered, every action counts. How your communications are managed – externally and internally – is critical, particularly when dealing with unknown attack vectors and advanced persistent threats (APTs).

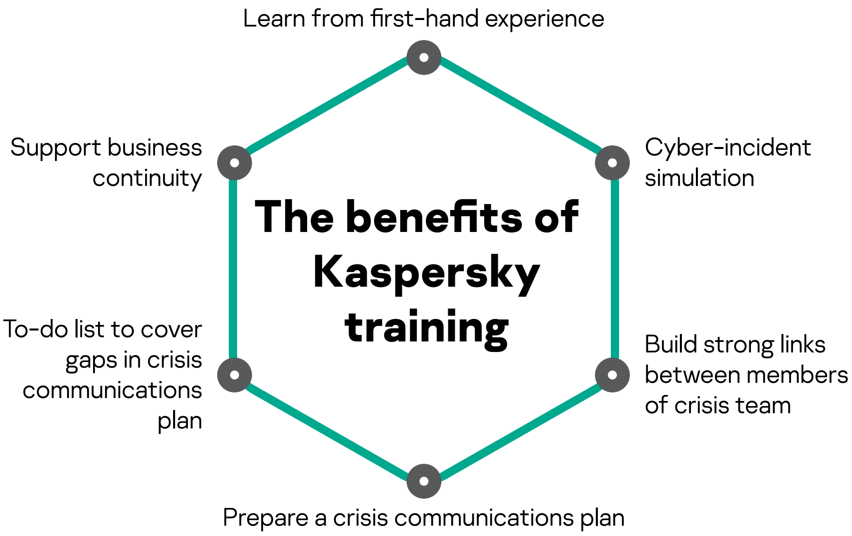
Upskilling your crisis team to:

- Understand the cyberthreats heading your way
- Recognize potential outcomes
- Know what should be done, and how
- Coordinate effectively with your IT security team
- Gain experience through cyber-incident simulation
- Prepare appropriate comms tools
- Know what is essential, and safe, to say
- Update and implement your cybercrisis communications plan
- Stay informed and up to date

Any enterprise can fall victim to a cyberattack, which is why there needs to be a crisis team – ideally made up of specialists from the information security department, the operations division, and corporate communications – ready to minimize the damage. This can be done through authoritative, appropriate, accurate and timely actions.

- **Authoritative** – Reassuring customers, stakeholders and the media that the organization is fully in control of the situation and is dealing with it calmly and effectively.
- **Appropriate** – Using the appropriate tools, channels and language to inform and reassure without causing panic or confusion, and without inadvertently assisting your attackers.
- **Accurate** – Avoiding the adverse consequences of making unintentionally misleading statements or claims while under attack.
- **Timely** – Ensuring that all your legal and regulatory obligations relating to the public disclosure of specific data-related information are fully met within the timeframes stipulated.

Kaspersky has developed best-of-breed training that empowers top management, information security and corporate communications professionals to handle crisis communications, including developing and applying appropriate assets, while under attack from an unknown cyber-incident or advanced persistent threat (APT).


Learn from first-hand experience
Cyber-incident simulation
Build strong links between members of crisis team
Prepare a crisis communications plan
To-do list to cover gaps in crisis communications plan
Support business continuity
The benefits of Kaspersky training

Building the links

IST **(Information Security Team)**	**Two-way communication**	**CCT** **(Corporate Communications Team)**
· Highly technical jargon, details and accuracy · Audience is relatively well educated, understands nuances · Why does the CCO think everything is "a virus"?	To manage your brand reputation the CISO and the CCO need to understand one another and to collaborate closely and pragmatically	· Would prefer to call everything a virus · Media audiences would prefer if everything was a virus · Why can't the CISO just call it a virus?

What is an advanced persistent threat (APT)?
An APT is a prolonged and targeted cyberattack in which the intruder gains access to the network of an organization and remains undetected for an extended period of time. The goal of an APT attack is usually to monitor network activity and steal data, rather than just to cause damage to the network or organization.

What you get

As one of the world's most widely recognized and acclaimed authorities on cyberthreats and how to handle them, we are happy to share our knowledge and expertise with others. And, as an organization that has also dealt successfully with an advanced cyberattack, we are better placed than most to vouch for the importance of an informed and effective cybercrisis management plan.

Packages available

	Standard	Workshop
Threat landscape and crisis incidents overview: the various types and how they differ	✓	
Deep dive into a hands-on experience. Kaspersky incident: from the first day to disclosure	✓	
Recommended operation security procedures and tools for communication encryption during a cyber-incident	✓	
Tailored workshop based on the specifics of the organization and worst-case scenario based on current cyber-incident preparation		✓
To-do list of tasks based on workshop to cover gaps in crisis communications plan		✓

Which package is right for you?

To find out more about Kaspersky Incident Communications and to see which workshop best suits your needs, visit https://kas.pr/kic or contact us at kic@kaspersky.com.

> "One particularly useful result of the training was the realization that we need to work on increasing awareness about cybersecurity inside the organization among the senior management. They, too, have to realize that the danger is significant, and measures need to be in place now, as the aftermath could be very serious."
> - Nebojsa Jokic, Head of CERT, Ministry of Internal Affairs, Serbia.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Proven.
Transparent.
Independent.

Known more at kaspersky.com/transparency