Kaspersky®
Incident
Communications

Upskilling Your Corporate Communications Team to Operate Optimally during a Cyber-attack

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 CorpComms 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 practical exercises
- Use appropriate comms tools
- Know what is essential, and safe, to say
- Update and implement your Cyber-Crisis Communications Plan
- Stay informed and up-to-date

When your organization comes under attack, your Corporate Communications Team must be ready to minimize the damage caused, through authoritative, appropriate, accurate and timely actions:

Authoritative – Reassuring customers, stakeholders and the press 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 unintentionally making potentially misleading statements or claims while under attack.
Timely – Ensuring that all your legal and regulatory obligations, relating to the public disclosure of specific information regarding any data, are fully met within the timeframes stipulated.

Kaspersky Lab has developed best-of-breed training that empowers 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).

Through a choice of short, intensive workshops, we will arm your CorpComms Team with:

- The ability to appreciate what's happening, why and what the results could be.
- And understanding of how such incidents can and should be handled, and how this is done.
- An established communications gateway between the CorpComms and IT Security Teams.
- Hands-on experience of similar incidents gained through practical exercises.
- The appropriate tools to cope and to communicate safely and effectively.
- The knowledge to create or refine an efficient, practical cyber-crisis communications plan that reflects your current threat landscape.
- The confidence and expertise to act calmly, smoothly and professionally in a time of corporate crisis.
- An online service keeping you informed on emerging threats and their potential impact to your company's brand.

CISO (Chief Information Security Officer)	Two-way communication	CCO (Corporate Communications Officer)
• Highly technical jargon, details and accuracy • Audience is relatively 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 continuously and pragmatically work closely together	• Would prefer to call everything anti-virus • Media audiences would prefer that it was all 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 We Offer and How It Works

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 which has also, ourselves, dealt successfully with an advanced cyberattack, we are better placed than most to vouch for the importance of an informed and effective cyber-crisis management plan.

Keynote Presentation

What happens when a global enterprise, itself leading the fight against cybercrime and staffed by world-leading cybersecurity experts, is attacked? The presentation is based on Kaspersky Lab’s own first-hand experience at the battlefront. Our story of the successful handling of a major cyber-attack offers a blueprint for effective cyber-crisis communications management.

This absorbing and revealing presentation, from one of our leading experts and keynote speakers, serves as an introduction to each of our two training packages.

The quality and content of our Keynote Presentation is such that you may want to use this opportunity to reach an wider audience, as part of your customer event or as a conference keynote.

Our training complements your cyber-incident reputation solution

New industry standard	Current industry solution	
Kaspersky Lab Training • Technical Training/Workshop • Insert for CrisisComms Manual • Real-time cyber-advice for communicators	In-house Corporate Communications • Generic CrisisComms Manual • Crisis Communications Strategy • Top level execution	External Consultant • PR/Communications Agency • Crisis Communications Training • Mid/low level execution

Standard Training

An information-packed, lively, half-day session suitable for communications professionals at all levels.

How can you be sure you’re communicating the right information, and doing it securely, in the event of an advanced or unknown cyber-incident? Our standard training package pairs historical insights with an understanding of the broader cyber-incident landscape, while our database of recent case studies is used to explore best (and worst) practices.

Outcome – Participants emerge armed with the knowledge, the tools and the confidence needed to perform effectively during, and in the aftermath of, a cyber-crisis.

Tailored Workshop

The highly customized nature of this training means that we can add further modules, exploring related topics, as required. For example – has your organization come under attack recently? How would your CorpComms Team have acted differently, based on what they know now?

A professional skills training workshop, custom-built for your organization on the basis of:

- Your key objectives in building and maintaining your business continuity program.
- Our knowledge of the specific threats currently targeting your industry and organizations like your own.
- The outcomes of our pre-workshop audits of your incident protocols and reporting lines, and of a simulated 'phishing attack' conducted (with your knowledge and approval) by us on your organization.

The result is a full-day customized workshop, preparing your Corporate Communications Team to manage communications effectively in the event of an advanced or unknown cyber-incident.

Threats and scenarios specific to your organization and its environment are explored in depth, best practices and appropriate tools and responses are analyzed, and recommendations made.

These recommendations feed into your CorpComms Team's Cyber-Crisis Communications Plan, which is developed and 'live tested' during the workshop in a specially-crafted 'war room' experience based on a fictitious scenario.

Outcome – your CorpComms Teams will emerge from this experience with the precise knowledge, skills, tools, and hands-on experience required to mitigate the damage to your organization from whatever's about to come your way.

The Training Packages

Kaspersky Incident Communications is available in different packages, depending on your crisis communications management maturity and cyber-threat awareness.

- The Standard Package combines our Keynote Presentation with a half-day training program, offering a good grounding in cyber-incidents and how to handle them.
- Our Premium Package features a full-day tailored workshop that's highly customized to the needs of your organization, based on our preliminary work with you, and resulting in the development and adoption of your own communications plan for use during a cyber-attack.

Which Package to Choose?

Services provided	Standard	Premium
An engaging 60 minute Keynote Presentation, followed by a Q&A session, delivered by a spokesperson from Kaspersky Lab	✓	✓
A Generic overview of the current global cyberthreat landscape – its history and evolution, and how corporate brands and reputations can be (and are) impacted.	✓	✓
Threats types - malware, ransomware, APTs, or unknown cyber-attacks – and how they differ from a CorpComms perpective.	✓	✓
A deep dive into how Kaspersky Lab's own CorpComms Team managed the situation after discovering Duqu 2 - one of the most advanced APTs in the World	✓	✓
Education session on OpSec (Operational Security) for CorpComms professionals – including technical toolkits and their use, best practice implementation, and effective liaison with the IT Security, Incident Response and other corporate teams.	✓	✓
Pre-workshop audit, conducted in conjunction with your CISO (Chief Information Security Officer), on incident management protocols and threat vectors.	–	✓
Pre-workshop audit conducted in conjunction with your CCO (Chief Communications Officer) on the organizational structure, escalation, de-escalation, and reporting lines.	–	✓
Expert-led deep dive into cyberthreats specifically relevant to your industry and environment, and those particularly likely to target your organization.	–	✓
Tailored OpSec best practice recommendations for your organization, based on our preliminary researches and audits.	–	✓
New or updated cyber-crisis handling section for your corporate Incident Communications Manual or Plan.	–	✓
Practical 'war room' exercise based on implementing your Incident Communications Plan.	–	✓

Which Package is right for your corporate communications professionals?

To find out more about Kaspersky Incident Communications, and to see which workshop would best meet your needs, visit https://kas.pr/kacic

www.kaspersky.com

Enterprise Cybersecurity:
www.kaspersky.com/enterprise
Cyber Threats News:
www.securelist.com

#truecybersecurity

Kaspersky Incident Communications:
https://kas.pr/kacic