kaspersky BRING ON THE FUTURE

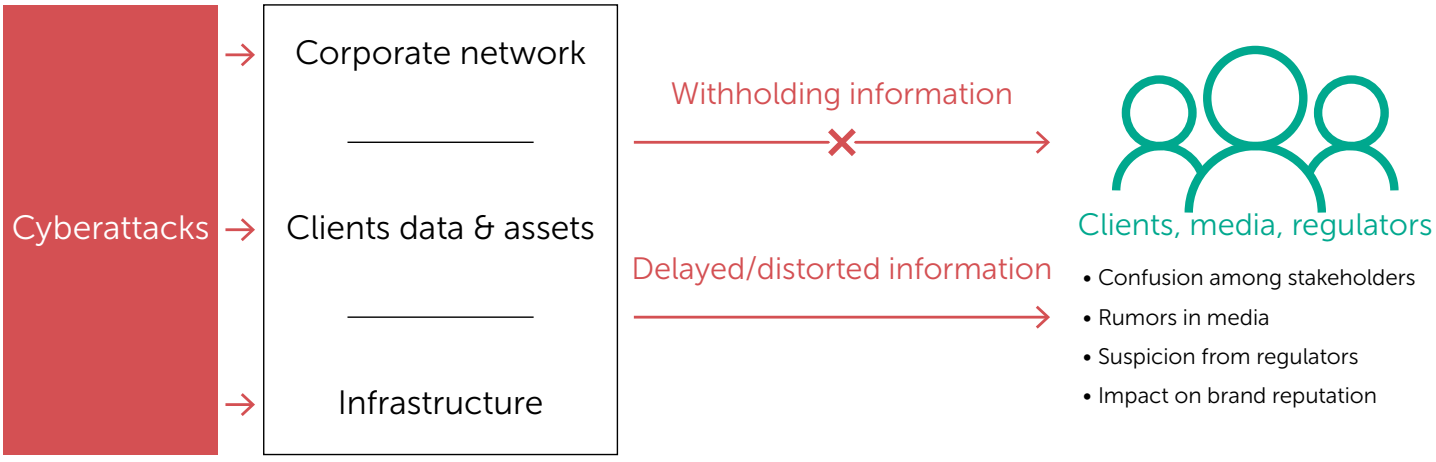
Kaspersky® Incident Communications

Incident communication techniques for financial institutions

The financial sector is one of the most innovative sectors of the economy, serving governments, corporate customers and individual consumers. Often it is an example of cutting-edge digital technologies and security mechanisms at work. However, this sector inevitably remains the most affected by cyberthreats and fraud, since it attracts large concentrations of assets and wealth. Moreover, financial organizations traditionally suffer from higher cybercrime costs than those in other industries.

This means financial institutions are constantly on the lookout for more sophisticated means of protection, from heavy-duty vault doors to cybersecurity incident response.

But it's not only technological remedies that are capable of protecting client assets and reputations; effective interaction between departments within a company as well as external communications are extremely important factors. Clients, media and regulators want to see a willingness to fulfil commitments and make every effort to ensure the safety of client assets.



The risks of miscommunication in the event of a cyberattack

The consequences of cyberattacks can be disastrous for financial institutions

Because it is directly related to money and valuable assets, disruption of the financial services industry usually entails huge losses for the individuals and institutions involved. When there is an interruption to banking or trading platform operations, customers immediately start losing money.

Due to mistakes in cyber-incident communications, companies face serious repercussions such as problems with the law, compensation payments, and a lack of trust among customers and partners.

Equifax: fatal miscommunication

The US credit rating firm Equifax compromised the personal records of over 145 million customers, including Social Security numbers, addresses, full names and other sensitive information.

The breach reportedly happened in March 2017, but wasn't reported until May and didn't become public until September. It was one of the biggest data breaches in history.

- Senior executives at Equifax sold shares worth a combined $1.8 million days after the company discovered the hack.
- Equifax has since lost a reported $439 million.
- The reputation of the company is in tatters.
- It is being sued by a number of private litigants and regulators.

TalkTalk: steps to failure

Telecom company TalkTalk fell victim to several data breaches. One incident in 2015 cost the company dearly.

More than 150,000 personal records were stolen. When TalkTalk realized what had happened, the company took down its webpage and concealed the hack for the next 24 hours.

Company representatives then decided to blame their suppliers instead of pleading guilty. The CEO Dido Harding came across as incredibly naive and uninformed in the interviews and public appearances that followed.

- TalkTalk was fined a record £400,000.
- The company's reputation was severely damaged.
- The CEO stood down in early 2017.
- The share price halved.
- Subsequent losses totaled £42 million.

Misinformation (accidental or deliberate) of clients, stakeholders and the media is one of the biggest risks for financial institutions

Kaspersky research shows that the majority of employees are not even aware their company is subject to cybersecurity regulation. That could well be the case in your company too.

While this confusion exists, millions of dollars are being stolen from customer accounts or data is being leaked.

The research included interviews with approximately 2,000 businesses that suffered data breaches:

- The most widespread risk is that of losses from **penalties and fines**, which affected 31% of respondents. Almost half of them (47%) were forced to pay **compensation** to clients and customers. Another consequence of data breaches is the risk of **legal fees**.
- **Breach of trust** among existing and potential customers and partners is another threat. 38% of enterprises had problems attracting new clients.
- **Tangible assets may be unsafe** when a data breach occurs.

To ensure an adequate response, it is crucial to allocate roles and responsibilities. There must be a chief information security officer (CISO) responsible for preventing threats and operational measures to eliminate them.

All business units must speak in the language of business and compliance. The CISO must be able to communicate clearly to the corporate communications officer (CCO), who in turn must be able to understand the issue and make competent public statements.

Company departments often have trouble understanding what's going on in the event of an attack. When the CISO and CCO do not understand each other, there is a danger the company representative will provide inaccurate information to journalists. Even worse, inaccurate information can be sent out to clients and stakeholders.

Poorly prepared reports and erroneous information can cause more damage to an organization than technical issues.

But it is even worse when miscommunication is intentional!

According to research by Business Insider, most banks hide the lion's share of cyberattacks. In the case of Equifax, the concealment and delay resulted in discontent and falling ratings. The company has forever left a stain on its reputation. Nearly 145.5 million personal records were stolen, the company has lost a reported $439 million and is being sued.

Transparency is not an option but an integral part of compliance. There are regulations that stipulate financial institutions must be transparent. One prime example is GDPR regulation. In certain cases, it obliges an organization to report breaches to the competent supervisory authority within 72 hours. If companies cannot comply appropriately, fines can reach up to 20 million euros or 4% of global annual turnover.

Ashley Madison: passivity and negligence

In 2015, dating service Ashley Madison was attacked by hacktivists. About 37 million personal records were stolen.

The hackers threatened to disclose the users personal information if the service wasn't immediately shut down.

The CEO tried to distance himself from the hack, but a second data dump brought him right back into it, as details of his own affairs came to light.

Adding to the impact of the breach was that they'd lost the trust of their customers, who had previously counted on them to safeguard their secrets.

- Personal toll of victims (30 million people in more than 40 countries affected – varying degrees of panic and marital stress, even suicides reported).
- Paid $1.66 million to settle charges with authorities.
- Payout of $11.2 million to victims.
- Forced to spend millions of dollars to boost security and user privacy.
- Lost over a quarter of revenue.

Transparency is not an option but an inherent part of compliance

The US, inter alia, has the SEC 2018 – guidance on the disclosure of cyber-risks for public companies.

In the European Union, the General Data Protection Regulation (GDPR), which entered into force in May 2018, requires companies to report a data leak to the government within 72 hours of it being identified. If companies cannot comply appropriately, fines can reach up to 20 million euros or 4% of global annual turnover.

However, banks are in no hurry to disclose their troubles

Bankers and experts in cybersecurity say many more attacks are taking place than reported. In fact, banks are under almost constant attack.

Ensuring incident management

- Executives and all responsible employees should be primarily guided by the interests of the business, focusing on reputation and financial sustainability.
- All units must be aware of the cybersecurity tools the company has. This is necessary to effectively coordinate incident response.
- Information should circulate freely in an accessible form. Do not abuse the narrow terminology and do not neglect the meaning. Use intelligible frameworks and graphics.
- Talk about your successes. Staff must be aware of the current state of security systems and their capabilities in order to take advantage of them at a critical moment.
- IT professionals must turn technical details of security risks into information that can be easily comprehended and digested by upper management.
- Finally, it is the responsibility of the CIO or top IT executive to address these issues directly with the CEO and executive team. This way, the issues are brought directly to their attention, and facts are not filtered out by intermediate players.

How attack reporting can improve credibility. The Kaspersky case.

In 2015, Kaspersky faced a very professional and meticulously planned targeted attack. This was the second wave of the Duqu attack (the first was discovered in 2011) that later became known as Duqu 2.

The attackers penetrated the corporate network. Their ultimate goal remained unclear, but an interest in the company's latest cybersecurity technologies was suspected.

In some ways, the intrusion was viewed more as an opportunity than a problem. Kaspersky experts took measures to protect information about the incident and started preparing a communication plan as well as eliminating the threat. As a result, when the incident was resolved, the company published a detailed press release and technical documents describing the attack. Source: Kaspersky

This level of transparency and incident management was possible due to close cooperation between the Information Security and Corporate Communications departments. Established procedures were key to achieving a positive result. Through Kaspersky Incident Communications we want to share our valuable experience with you.

We provided the public and our partners with an in-depth report on the incident and how we worked to eliminate the threat. This policy of openness strengthened customer confidence as well as our position as an industry expert.

It was, nevertheless, a resource-intensive task that was successful thanks to high-level communications and management. It also demonstrated that you need to be extremely focused and prepared to be able to meet regulatory requirements such as GDPR.

Kaspersky Incident Communications provides the key components of a proper instant response and communications

Many financial institutions tend to conceal the details of cyberattacks, which can cause financial and reputational damage.

To ensure customer trust, show your willingness to be open and to do everything to preserve their assets and loyalty.

- Appoint a crisis response team that includes information security and communication departments, stakeholders and spokespeople.
- Each department and employee must be competent and have clear responsibilities.
- Analyze the incident and provide partners and customers with the most complete, verified, reliable and constructive information. Your statements must contain not only the problem but recommendations on the solution as well.

Proven solutions from Kaspersky experts

As one of the world's most widely recognized and acclaimed experts on cyberthreats and how to handle them, Kaspersky is happy to share its knowledge and expertise. And as an organization that has also dealt successfully with an advanced cyberattack, we are better placed to vouch for the importance of an informed and effective cybercrisis 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 own first-hand experience. Our story of the successful handling of a major cyberattack offers a blueprint for effective cybercrisis communications management.

Keynote Presentation

The presentation serves as an introduction to each of our two training packages.

By one of our leading experts and keynote speakers.

The presentation is based on Kaspersky Lab's own experience of the successful handling of a major cyberattack.

Generic Training

Information-packed, half-day session for communications professionals at all levels.

Historical insights with an understanding of the broader cyber-incident landscape.

Participants gain the knowledge, the tools and the confidence to mitigate a cybercrisis.

Tailored Workshop

A full-day tailored workshop for your Corporate Communications Team.

Threats and scenarios specific to your organization and its environment are explored.

The precise knowledge, skills, tools and hands-on experience to mitigate the damage from attacks.

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 it to reach a wider audience, as part of a customer event or as a conference keynote.

Generic training

Kaspersky offers 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 generic 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 cybercrisis.

Tailored workshop

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 linesl.

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, and all under the guidance of Kaspersky cybersecurity and communication experts.

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 Cybercrisis 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.

Not sure which package to choose?

Services	Standard	Premium
An engaging 60-minute Keynote Presentation, followed by a Q&A session, delivered by a Kaspersky spokesperson.	✓	✓
A generic overview of the current global cyberthreat landscape – its history and evolution, and how corporate brands and reputations can be (and are) impacted.	✓	✓
Threat types – malware, ransomware, APTs, or unknown cyberattacks – and how they differ from a CorpComms perspective.	✓	✓
A deep dive into how Kaspersky 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 IT Security, Incident Response and other corporate teams.	✓	✓
Pre-workshop audit, conducted in conjunction with your chief information security officer (CISO), on incident management protocols and threat vectors.	✗	✓
Pre-workshop audit conducted in conjunction with your chief communications officer (CCO) 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 research and audits.	✗	✓
New or updated cybercrisis handling section for your corporate Cybercrisis Communications Manual or Plan.	✗	✓
Practical 'war room' exercise based on implementing your Cybercrisis Communication Plan.	✗	✓

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

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.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.