kaspersky BRING ON THE FUTURE

Kaspersky® Incident Communications

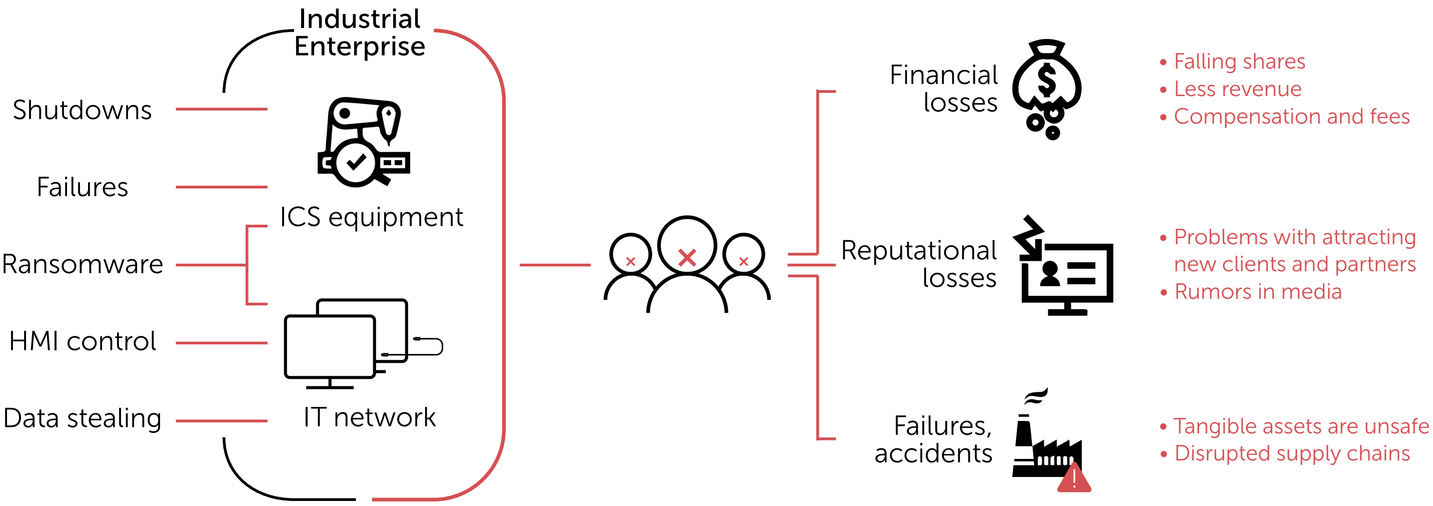
Incident communication techniques for the industrial sector

Digitalization is a growing trend in all areas, and the industrial sector is no exception. With the introduction of digital technologies, smart measuring, connectivity, and data transmission, many machines and devices can no longer work without being integrated into a network. However, manufacturing optimization processes based on data flows now mean there are lots of possible entry points for cyberattacks.

As well as internet access, which is used for business purposes or other forms of communication, there are numerous connections between industrial tools, data centers, measuring equipment, etc. The industrial internet of things (IIoT) has brought a whole new level of interaction, as well as huge challenges. Supply chains, industrial facilities, equipment, manufacturers and consumers are all now closely interrelated and any one of the many units providing external access could be susceptible to hackers.

Cyberattacks in the industrial sector can affect a wide range of systems and cause serious damage to companies and their customers, from industrial espionage and data theft to disruptions to production processes and power supplies.

Highly specialized professionals need to be involved in the process of preventing and eliminating threats in the industrial sector. Your corporate communications team must be well trained to interpret any available information on cyberattacks. Their goal is to formulate a clear and detailed message for media, partners and clients.



Dozens of cyberattacks are known to have hit the industrial sector. Here are some examples from the Top 20 by Waterfall Security Solutions Ltd.
Source: The Top 20 Cyber Attacks Against Industrial Control Systems, NCCIC

ICS Insider
A disgruntled insider with access to ICS equipment uses social engineering to steal passwords able to trigger a partial plant shutdown.

IT Insider
A disgruntled insider with access to an IT network uses social engineering to steal passwords able to give them remote control of a copy of the HMI system on an engineering workstation.

Common Ransomware
Accidentally downloaded to an engineering workstation and spreads to rest of ICS.

Targeted Ransomware
Spear phishing seeds a Remote Access Trojan (RAT) on an IT network, which is used to deliberately spread ransomware through an ICS.

Zero-Day Ransomware
Ransomware incorporating a zero-day Windows exploit spreads through IT/OT firewalls.

Market Manipulation
An organized-crime syndicate uses known vulnerabilities in internet-facing systems to seed RATs that are ultimately used to simulate random equipment failures, triggering commodities markets fluctuations.

Sophisticated Market Manipulation
A similar attack targeting an ICS site's services suppliers as a means of seeding peer-to-peer RAT malware into an ICS and simulating random failures.

Cell-phone WIFI
A combination of spear phishing and a Trojan cell phone app provides attackers with access to ICS WIFI networks.

Hijacked Two-Factor
Sophisticated malware allows attackers to hijack remote desktop/VPN sessions after a remote user logs in with two-factor authentication.

IIoT Pivot
Hacktivists pivot into an ICS via a poorly defended cloud vendor.

Poor cyber-incident communication management threatens your business and your counterparties

Industrial cyberattacks can have a significant effect on a wide range of individuals and organizations. Due to industry specifics, many parties can end up being affected.

For a company operating in the industrial sector, it is crucial to implement a response management and communications plan. In urgent situations, this will help to quickly provide valuable information on threat mitigation to those affected by an incident where you are at fault.

Cyberattacks on industrial enterprises – unlike financial organizations, for instance – can pose a direct threat to people's health and even lives. If you are unable to alert everyone affected by an incident in time, the price of a delay could be human lives; financial and reputational losses pale into insignificance in comparison.

Learn from Kaspersky own experience of managing cyber-incident communications to mitigate the reputational and financial impact of cyberattacks.

It is necessary to ensure the maximum level of awareness and technical literacy among the specialists in your organization so they work quickly and efficiently to provide relevant, accurate data to those who need it.

Kaspersky Incident Communications (KIC) aims to ensure your company has an effective structure in place that can make immediate decisions and formulate clear reports and guidelines on how to mitigate risks for customers and partners.

The best guarantee that your systems are secure and your personnel competent is by having:

- **Specialists with interdisciplinary competences.** As cyberattacks become one of the greatest challenges of the modern economy, the need for professionals who work at the junction of corporate communications and cybersecurity increases.
- **Responsibilities and a clear plan.** When a competent team of top managers, CorpComms, threat analysts and other specialists are gathered to outline a cyberattack mitigation plan, it is important to ensure effective cooperation.

After completing training and receiving the work materials included in Kaspersky Incident Communications, you too can achieve these aims.

Who is at risk and how to build communications in the event of cyberattacks?

Partners and suppliers

Obviously, the databases of any company contain confidential and sensitive information not only about the company but also about the organizations it works with. By allowing intruders to infiltrate your corporate network, you are compromising your counterparties.

Once they gain access to internal databases, hackers can get information that will enable them to control processes in other companies. They can then sell this information or use it to blackmail the owners. Situations like this reflect very badly on you.

You need to inform your partners quickly and accurately about any threats that may affect them. By providing data at an early stage, you retain your credibility and can take joint protective measures in time.

Example of successful cyber-incident communication

In 2018, Cisco released a document dedicated to three vulnerabilities in many modern microprocessors that can lead to side-channel information disclosure attacks.

In order to prevent a further worsening of the situation and to secure its users, the company provided a detailed list of products that were exposed to the vulnerabilities. The owner of each model could use the list to find out if there was a threat to their safety.

The document then described in detail how the detected vulnerabilities manifest themselves. This made it easier to diagnose and take measures to mitigate or prevent the threats.

Cisco developed a special tool that documents any workarounds and fixed software to provide immediate solutions to customers.

The company also announced the release of articles and events dedicated to the problem of resolving emerging threats.

All these measures provided high-quality communication with customers and partners. Comprehensive support allowed users to feel as safe as possible.

Source: cisco.com

Example of unsuccessful cyber-incident communication

The threat

In early 2019, it was announced that Intel CPUs were afflicted with a simple data-spewing spec-exec vulnerability called Spoiler.

The flaw allows intruders to exploit in-browser JavaScript or malware on a system to steal sensitive information, user credentials and data from memory. The vulnerability can only be mitigated by a significant redesign of the CPUs.

The response

In a brief interview with an Intel spokesperson, it was revealed that the company was notified of the threat back in December 2018, but did not react.

Experts say that a vulnerability like this cannot be fixed in a short time and, most likely, it will take years of product redesign.

AMD stated that its processors are not affected by the vulnerability and communicated in detail with the media about the situation. Meanwhile, there was no response from Intel.

Source: https://www.theregister.co.uk/2019/03/05/spoiler_intel_processor_flaw/

Clients

Both large companies and individual consumers can be clients of industrial enterprises.

If your company supplies materials or equipment that are subject to time-bound processes, any failure of electronic systems or interrupted data flows can result in supply disruptions. In this case, you will not only have to spend money to remediate your own resources but also to offset the costs to your customers.

Consumers may receive your product in real time, as is the case with power plants, or they may purchase durable goods, for example, electronic devices equipped with microprocessors that you manufacture. In either case, cyberattacks can cause tangible problems in the short and long term.

Giving your employees advanced communication skills with Kaspersky Incident Communications will help you establish direct contact and a relationship of trust with your customers.

Your enterprise

- **Disclosure of sensitive information**

Damage is inflicted on the enterprise whose infrastructure is being attacked. For instance, financial statements or correspondence can be hacked. In this case, confidential information intended for internal use may become available to the attackers, competitors or even the public.

Due to data theft, your company may lose its unique technology, confidential correspondence, sensitive customer information or system credentials.

- **Financial losses**

Intruders may be able to hijack financial transactions or carry out their own fraudulent transfers. Indirect financial damage may lead to a fall in share price. This can occur if it becomes clear that a company doesn't provide the appropriate level of corporate network security or fails to deal with attacks properly. Customers may also opt out of your services.

- Technological threats

By gaining control over IIoT devices, attackers are able to manipulate the operation of equipment to interrupt production or power supplies. In the worst case scenario, this can lead to a man-made disaster that will directly affect the company, as well as all those associated with it, from customers to suppliers. Moreover, random individuals may be caught up in the events.

Kaspersky Incident Communications will help increase the technical literacy and efficiency of communications between your units so they can do their utmost to mitigate the effects of an attack.

Kaspersky offers a comprehensive advanced training program to provide you with high-level expertise in cyber-incident communications

As one of the world's most widely recognized and acclaimed experts on cyberthreats and how to handle them, Kaspersky is happy to shares 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 lines.

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.

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.

Proven.
Transparent.
Independent.

Known more at kaspersky.com/transparency