THALES
CASE STUDY

How to preserve your reputation during a cyberattack with a prepared crisis communication

When the topic of cybersecurity comes up, we frequently think of technology. But, let's not forget that people use technology, whether they are employees, customers, suppliers, partners, and so on.
Without communication. no sales, no purchases, no partnerships, etc. Thus, during a cyberattack, protecting communication is crucial, all the more in the age of AI.
Preparing the communication is as important as preparing IT processes/tools.

Thales is a perfect example that illustrates this truth.

Context

Two significant cyberattacks against Thales were reported in 2022 by the Russian-speaking organisation Lockbit 3.0. (also named BlackCat)
Thales handled the problem with a clear and efficient internal and external communication strategy and plan in spite of the severity of the ransomware attacks.
The company opted not to comply with demands for ransomware (a French custom) right from the beginning of the crisis, demonstrating not just a wish to discourage attackers but also its resilience, its coherence to the company values and the unwillingness to compromise.

Benefit 1 - Cohesion & Pride

Having been prepared and briefed, the employees reacted as One, following instructions scrupulously. By being kept regularly informed of developments, they felt valued and protected by their employer. All the reasons to be proud of working for Thales!

Benefit 2 - Reputation & Loyalty

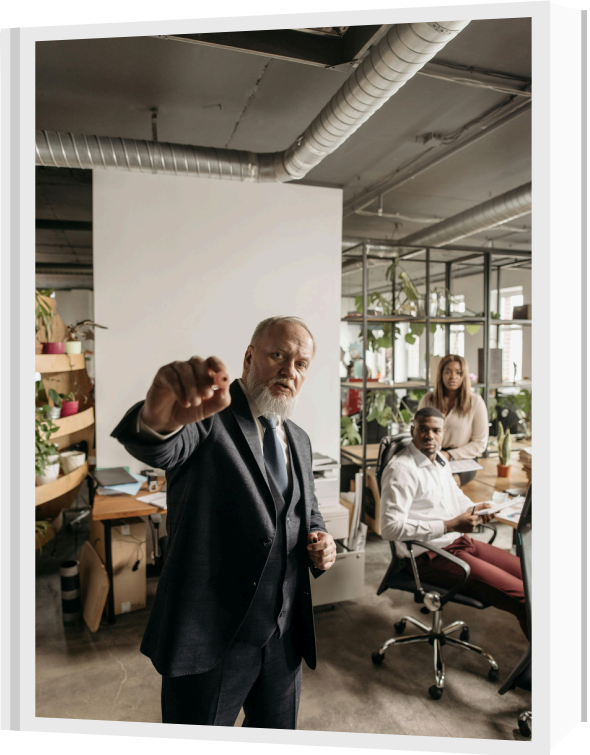
Thanks to regular, transparent communication, customers, suppliers and partners have never lost trust in Thales, despite their fear that their data might be published. This trust increased their loyalty to Thales.

Benefit 3 - Act as a Leader

Thales has clearly demonstrated the power of well-prepared communications to overcome a cyber attack with moderate impact, and binds together the company, making the strategy become practice. This is true leadership.

A prepared communication mitigates the damage that could prove very costly over several years.

Meticulous preparation internally, on several levels



PROACTIVELY

A dedicated Crisis Management team (CMT)

as OZ'N'GO teaches and recommends, Thales set up a crisis communication team made up of members of the company's crucial departments, who worked with in-house cybersecurity experts.

Objectives & Responsibilities

- Increase the security of systems in the face of the threat
- Organise appropriate and secure communication channels
- Prepare internal and external communication messages and tools
- Improve internal information and communication flows with all stakeholders

Employees cyber-training

Raising awareness

In other words, training on the cyber-security principles. Types of cyberattacks. Best practices. Advice on security protocols. Internal rules. Information on laws, etc.

Simulations

Don't we hold fire drills at least once a year? The same goes for cyber security in an advanced way with simulations based on clearly identified and defined crisis scenarios. That is what Thales did for the CMT and key critical roles within the organisation.

DURING THE CYBERATTACK

Thales CMT notified the staff right away, being cautious not to inspire fear, while keeping the attack's nature and origins clear.

The group leaders were routinely updated on any development of the situation, along with a kind reminder of proper conduct.

All the communications were done through secure internal routes, like the Cybels suite, specifically Cryptosmart, a secure mobile communications solution created in collaboration with Samsung. This solution offers military-grade message encryption to safeguard internal data transfers throughout the crisis.

Thales also implemented CipherTrust, a data security platform that encrypts critical data while it's in transit and at rest.

Solid preparation for external Stakeholders

External communication covers a large set of audiences: clients, suppliers, partners, authorities, investors, share-holders journalists, etc. The crisis communica-tion strategy and plan must strongly address the needs of information of each audience to **maintain trust in the whole company ecosystem**.

PROACTIVELY

As OZ'N'GO advises its clients, Thales CMT prepared specific messages and communication materials, aligned with the incident response plan and the escalation framework. .

As much as possible, were crafted and produced the following:

- Press releases
- Emails
- Presentations
- Mobile text-messages.
- FAQ
- Etc

Lists of key contacts were elaborated and saved in a secured place.

Secured communication

Again, OZ'N'GO recommends it, Thales did it. Secured communication channels were set up and shared with the different audiences.

- Secure portals for partners and suppliers with access to exchange information and documents.
- Secure video conferencing platforms
- Encrypted emails/messages using Cybels solutions for personalised communications.
- a secured Hotline to answer urgent questions.

DURING THE CYBERATTACK

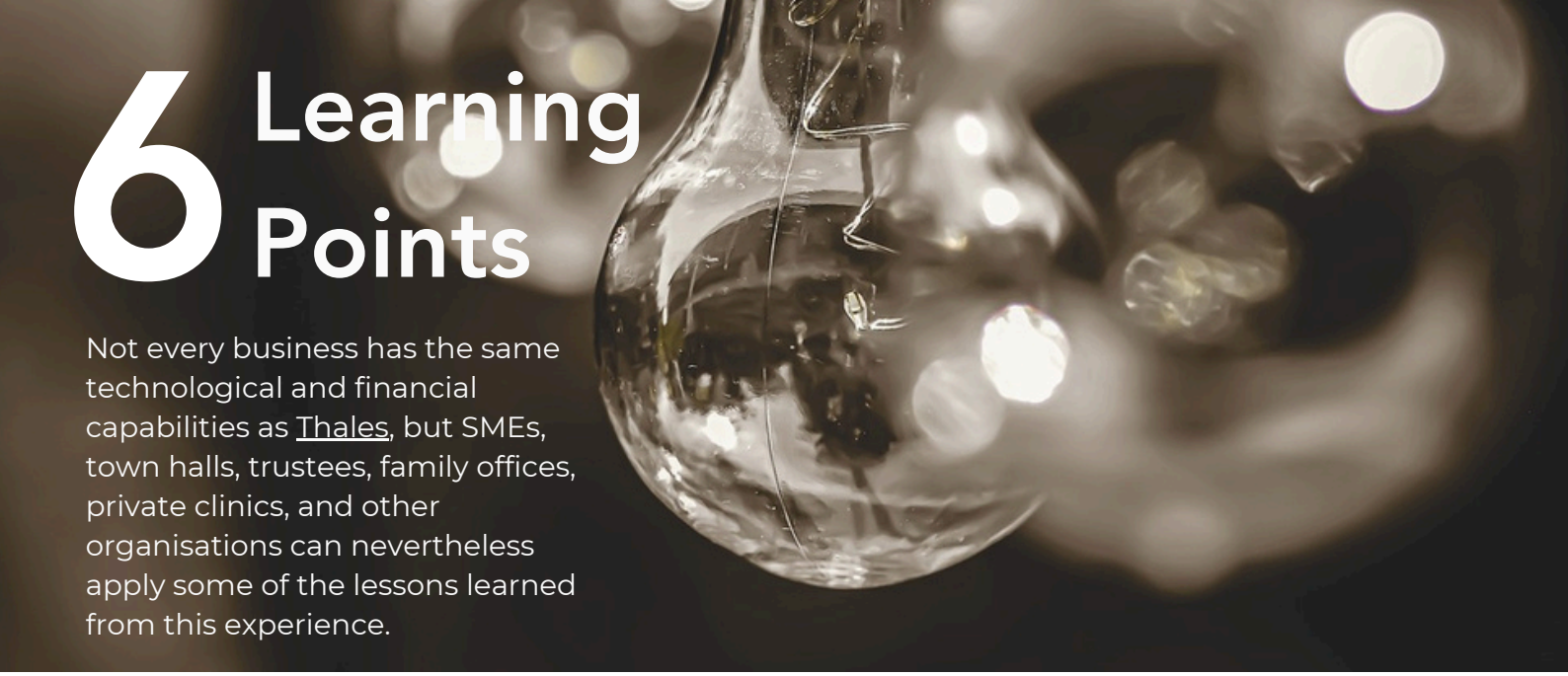
All parties involved were promptly informed about the attack on Thales thanks to the communication prepared in advance with chosen terms to lessen the financial and reputational damage.

Thales acknowledged the facts, stating that the integrity of its critical systems had not been compromised, that the attacks had minimal impact on their essential functions and that robust measures were being implemented to prevent future incidents.

They maintained regular and transparent communication on developments of the situation.

This honesty as well as advise on the security measures to be applied helped to defuse a trust feeling all along the crisis.

With media, they gave interviews with key press bodies like Reuters or Breaking Defense.



6 Learning Points

Not every business has the same technological and financial capabilities as Thales, but SMEs, town halls, trustees, family offices, private clinics, and other organisations can nevertheless apply some of the lessons learned from this experience.

Clarity builds Trust

Being clear and honest from the outset, even with bad news, helps to maintain trust. Organisations need to recognise the attack quickly and provide regular updates on their response efforts.

Messages prepared in advance = narrative under control

Ready-to-use communication templates and documents allow you to respond quickly to master the narrative, and avoid delays that could damage/kill credibility. Advance preparation enables to be one step ahead the domino events of a cyber-attack.

Your reputation is in the hands of all Stakeholders

Engaging both internal stakeholders (such as employees and management) and external stakeholders (clients, partners, suppliers, investors, etc.) is vital. It ensures better control of the reputational risk by coordinating the right messages sent to each audience, avoiding the spread of misinformation.

To replicate Thales case in a practical & personalised way, contact us

Simulating communication during crisis exercises

Organisations need to practise not only the technical response to a cyber attack, but also how their communications teams will react. By including communication in crisis simulation exercises, teams can be better prepared for real-life scenarios.

3rd Parties must be involved

suppliers, partners, and service providers often play key roles in the operations and can help contain the impact of a cyber incident. Establish clear protocols for updating third parties, outlining how and when they will receive information. By keeping them informed, you enhance transparency, reduce the risk of misinf or-mation, and ensure they're aligned with your recovery efforts.

A post-crisis review is critical

Analysing what worked well and what didn't is essential for future resilience, whether it is to assess the effectiveness of the communication, response time, and the tools used. Any gaps in the plan must be documented to develop actionable steps to address them. Doing this job with all stakeholders helps to be better prepared for future incidents and build stronger trust in the ecosystem..