STORMSHIELD

OPINION ARTICLE

CYBERATTACK: WHEN COMMUNICATION BECOMES A TACTICAL CRISIS MANAGEMENT TOOL

Julien Paffumi
Senior Product
Manager, Stormshield

When hit by a cyberattack, some companies opt to issue few or no public statements on the subject. Yet national security agencies and CERTs (Computer Emergency Response Teams) recommend communicating as transparently as possible. Why? To improve general cooperation in response to cybercrime and reassure the business community. So why is communication sometimes seen as a taboo? Should we communicate or not? And to whom?

In terms of communication by victims of cyberattacks, the example of Norsk Hydro is striking. In 2019, this Norwegian industrial company fell victim to a ransomware attack that paralysed several production plants and some of its communication services. Nevertheless, the company opted for transparency and created a public crisis communication page on its website the day after the attack. This was regularly updated. In the months following the crisis, the media cited Norsk Hydro as a case study in how to communicate following a cyberattack.

WHY DO SOME COMPANIES PREFER THE LOW-KEY APPROACH?

This case study is still cited today as an example of how to manage a crisis. So how can we explain the fact that some victims prefer to keep a lower profile?

“*For a company, it’s naturally hard to admit to having fallen victim to a cyberattack,*” explains Yannick Duvergé, the CEO and founder of Exemplary a company specialising in crisis communication. “*It’s an admission of weakness that can have serious consequences for the business.*” For reasons of brand image and business imperatives, strategies aimed at hiding or minimising the consequences of an attack are common. Another argument against publicising the attack is the fear of creating a windfall effect: other malicious individuals could take advantage of the delay between the discovery of the cyberattack and the release of a patch for the exploited software flaw to commit a number of misdeeds themselves. It is therefore essential to ration the technical details shared publicly, in the interests of conveying an intelligible message and protecting the company in question, explains Stéphanie Ledoux, founder and CEO of Alcyconie, a cyber crisis management and communication firm. “*If the attack is the result of an exploited software vulnerability, communicating with other parties in the same sector can also prevent the attack from affecting other organisations that use the same software.*”

> *“For a company, it’s naturally hard to admit to having fallen victim to a cyberattack. It’s an admission of weakness that can have serious consequences for the business.”*
>
> **Yannick Duvergé,** CEO and founder of Exemplary

At the same time, **legislation provides a framework for a number of corporate statements** - which in some cases involve an obligation not to publicise such issues. In cases where there are legal implications, “*companies often find that they cannot implement their crisis communication plans at the pace they want while the investigators are doing their work*,” says **Pierre-Yves Hentzen**, CEO of Stormshield. Companies with critical status – whether *Opérateurs d’importance vitale* (OIVs) in France or Operators of Essential Services (OESs) at European level – are subject to **a strict communication protocol**. On the other hand, other laws require companies to issue some kind of notification – not in this case to the general public, but to inform the competent authorities of the cyberattack. For example, Article 33 of the General Data Protection Regulation (GDPR)) obliges companies handling the personal data of European citizens to follow the whistleblowing protocols in force in the countries where they operate, starting with “*notifying the personal data breach to the supervisory authority*”. Companies that have fallen victim to a cyber-attack must alert the authorities no later than 72 hours after discovering the data exfiltration. In addition, Article 34 of the GDPR obliges these companies to inform parties affected by a leak of information. However, the time limit for communication is imprecise, and remains at the discretion of the company that has fallen victim to the cyberattack, and/or the judicial authorities in the event of an investigation. Personal, sensitive, critical and even vital data; the very vocabulary used can lead to a degree of confusion. In any case, Ledoux points out that "*such companies are often contractually obliged to inform their stakeholders or customers. That's why it's important to have the support of a competent legal department providing information about exactly what to do or say, depending on the situation*".

> *"Such companies are often contractually obliged to inform their stakeholders or customers. That's why it's important to have the support of a competent legal department providing information about exactly what to do or say, depending on the situation."*
>
> **Stéphanie Ledoux,** founder and CEO of Alcyconie

But while this may explain the silence of some companies, experts agree that communication in the event of a cyberattack is a necessity.

WHY DO EXPERTS RECOMMEND TRANSPARENT CRISIS COMMUNICATION?

Ledoux presents communication as "a tactical tool for crisis management." If done effectively, it plays a key role in facilitating a positive resolution, as the case of Anthem illustrates. On 27 January 2015, this American health insurance company (one of the largest in the US) fell victim to a cyberattack. On 4 February, the company issued its first public statements, admitting that it had been the victim of a "*very sophisticated attack*". And worse: the data of tens of millions of customers ended up falling into the hands of cybercriminals. In the days that followed, Anthem sent personalised messages to all customers concerned, advising them on what action to take. While the situation could have been catastrophic for the company's image, Anthem's strategy – like that of Norsk Hydro – is regularly held up as an example of professionalism and transparency.

Many of the positive, lasting effects of a transparent approach to crisis communication can be explained by improved awareness on the part of the general public. While there may previously have been public censure of companies targeted by cyber-attacks, this is perhaps no longer the case, because the public "*is aware that cyber-attacks are increasingly common and can affect all companies, even the most prepared,*" explains Sébastien Viou, Director of Product Cybersecurity & Cyber-Evangelist at Stormshield When presented with media coverage of a cyberattack, the public's first response is to "*find out more about how the company is managing the crisis and coping with its problems,*" Ledoux maintains. "*They are no longer naïve about such matters. When a company tries to conceal the effects of a cyberattack, it has the effect of ringing alarm bells.*" That would make it illogical to avoid communicating for fear of incurring the wrath of public opinion.

"The general public is aware that cyber-attacks are increasingly common and can affect all companies, even the most prepared."

Sébastien Viou, Director of Product Cybersecurity & Cyber-Evangelist at Stormshield

Meanwhile, Hentzen points out that **most of the arguments against transparent communication feature fear as a common denominator** – and specifically, the fear of damaging existing business relationships. However, "*this is precisely what crisis communication is for: to provide reassurance. Depending on the situation, the company may not be obliged to alert the public immediately, but it does need to reassure its employees, stakeholders and customers! The consequences of the crisis may be just as significant for them, and denying that fact is likely to be more damaging to the reputation of the company that has suffered the attack.*"

Bear in mind that France's ANSSI cybersecurity agency lists damage to the brand image of a company as one of the four main motivations for cyberattacks. The ANSSI confirms that the most common cyberattacks "*are basically aimed at harming the image of their target*." Moreover, Viou reminds us that following their attacks, "*it is not uncommon for cybercriminals to carry out communication campaigns on social networks to promote the data assets they wish to sell on the darknet and/or damage the victim's brand image*." No matter how hard the company tries to hide or minimise the impact of the cyber-attack, it is **likely that some other party will take it upon themselves to leak the information**. "*It's better to go for a transparent approach immediately, to show that you're facing up to it and not running away*," concludes Ledoux.

HOW SHOULD YOU COMMUNICATE DURING THE CYBERATTACK?

For companies wishing to communicate, the question is how to go about it. The first piece of advice "*is to act quickly*," says Duvergé. As previously mentioned, the company should assume that the information will be leaked sooner or later. However, **if a company's own statement is preceded by a number of more or less credible rumours, the impact on public trust in the brand can be devastating**. Between November and December 2013, the American company Target was the victim of a cyberattack that resulted in the circulation of bank details for around ten million customers across the web. The company opted not to make a statement. Unfortunately, that meant an outside source was the first to inform the public. As a result of this strategy, Target was accused of concealing the attack and its potential impact on the public. The effects on brand image were disastrous, and consumer perception hit an all-time low. According to Viou, information communicated by sources "external" to the company is increasingly being used by cybercriminals. "*They see it as a way of forcing corporate victims to pay ransoms (for example, in the case of ransomware attacks), or of publicising the stolen data to potential buyers.*" To avoid suffering the same fate as Target, companies are therefore recommended to get their communications in first. This approach is often referred to as “*stealing thunder*”:**corporate communication should seek to take the wind out of cybercriminals’ sails.**

But who should the first messages be directed at? Speaking from experience, Hentzen believes that it is imperative to start the crisis communication phase with the company’s employees. They should be informed wherever possible; but above all, they should be reassured about the “*state of the company and their own personal future*.” This is also the ideal time to impress upon them the conduct that is expected of them throughout the crisis, particularly with regard to confidentiality. “*They will be approached by the press or third parties, and must adhere to the established communication plan. Involving them therefore helps greatly to bring the crisis to a positive resolution*.” And Ledoux stresses the importance of “*not adopting an approach that is cold, technical or even designed to induce guilt*”, which could heighten the shame that may be felt by employees who have unwillingly contributed to the propagation of the cyberattack. “*They are the first victims of the cyber-criminal; and as long as there is no evidence of a* ***breach of security rules****, they should be treated as such*,” Viou adds. Expert opinions are in line with the recommendations of the European Network and Information Security Agency (ENISA) and the various European CERTs. Both institutions advise communicating with the various targets in this order: employees, stakeholders (or shareholders), business partners (and service providers), customers, and finally the press.

> *“Employees will be approached by the press or third parties, and must adhere to the established communication plan. Involving them therefore helps greatly to bring the crisis to a positive resolution.”*

Pierre-Yves Hentzen, CEO of Stormshield

However, **the quality of the supplied information** must be **maintained.** Yet it is very difficult in the hours following the discovery of a cyber-attack to ascertain precisely what has happened, and therefore to plan a communication campaign on the subject. Depending on the specific case and the severity of the attack, the company can potentially obtain help from the competent authorities. In France, the ANSSI can carry out technical investigations to help corporate victims to identify key aspects of the attack. Does this mean that no statement can be made until the cybercriminal’s modus operandi is known? “*The company can start by acknowledging the attack, while avoiding any speculation. It can also explain how this affects its ability to operate normally. This has the merit of being transparent and showing that the company’s management is facing up to its responsibilities*,” Ledoux explains. This feeling can be increased if the company’s communication “comes from a senior manager, or even the company’s director,” adds Duvergé. “*This process lends a human face to communication, making it much easier to establish a relationship of trust with the public*. “Furthermore, if the company feels that it is not yet able to issue external statements, it can still make use of certain private entities and clubs such as the *Clubs de la sécurité de l’information en réseau* (Clusir). Its members are thus guaranteed **a relatively confidential interaction space in which the challenge is to share best practice and experiences in the field of cybersecurity**.

And after the cyberattack? Several months after a cyberattack, some companies produce a detailed report of their ordeals. This type of communication has the advantage of allowing others to benefit from this feedback. Viou explains that cybersecurity players such as Stormshield are particularly interested in reports that detail cyberattack processes and the indicators of compromise for the affected solutions: "*This allows us to stay constantly in touch with the reality on the ground*. On the other hand, "*if the company continues to communicate, but now with a focus on the actions it has carried out and the experience it has gained, it could very well emerge stronger*," explains Duvergé. A more transparent approach of this kind has helped Target out of its initial slump. In the year following the attack, the new management implemented a number of cyber-resilience projects to the value of almost $17 million. By constantly informing the public about these developments, it was able to restore its reputation, and ended the quarter at the same level as before the cyberattack.

Proof that the public understands – and can even forgive – a lack of security... provided that the communication focuses on the right arguments.