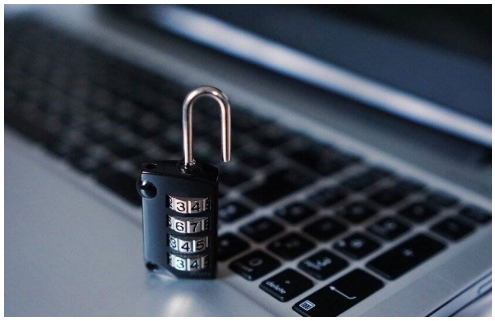
Risk for companies of cyberattacks: the necessity of forward planning for increased protection

The current uncertain geopolitical situation could also have dangerous digital implications for companies. In fact, the ANSSI (National Agency for Information System Security) has identified the use of cyberattacks as part of this conflict and calls on French entities to be especially vigilant due to the risk of increasing threats. The challenge in these unprecedented times is to plan ahead and implement protection without giving in to panic.

Adista is a Hosted Services operator that specialises in IT and Telecom services for companies and communities and helps organisations construct a cybersecurity policy that provides maximum protection for their data, information systems, and activities.

The government website cybermalveillance.gouv.fr specifies that as yet no *"direct cyberattack with a potentially significant impact on the French population has been identified"* within its scope. It does specify, however, that this situation is likely to change over time and that even if the risk is low at the moment, it has the potential to disrupt French digital services.

Above and beyond the ongoing exceptional circumstances, the number of cyberattacks have sharply increased in recent years. As a consequence, the ANSSI has identified a **65% increase** in cybercrime throughout the country compared to 2020, which generated **more than 173,000 requests** for online assistance on the **cybermalveillance.govt.fr** website. Its latest annual activity report also reveals that the threats encountered by the French population particularly concern three types of malicious cyber activity: **phishing, ransomware, and account hacking (email, banking, etc.)**



Increased vigilance is therefore required, as the consequences of cyberattacks on organisations are often significant: information systems that are partially or even completely paralysed, sensitive data stolen or lost, blackmail related to releasing data, etc...
In the majority of cases it is small and medium-sized businesses who are the victims of these malicious cyber activities, notably because they lack the dedicated resources to effectively secure their digital environment. But the largest groups are equally concerned. In any case, *IS Directors* are faced with multiple challenges.

Key actions and forward planning for maintaining activity in the event of an emergency

Nearly one in two companies state that they have concerns about their ability to effectively deal with cyber risks. For these companies, it is essential that the level of cybersecurity guarantees that a trusted digital environment remains available for their relationship with partners, customers, but also with their employees.

Organisations are often hyper-dependent on their information systems, and inevitably have weaknesses that must be known and understand so that their cyber-resilience can be improved when confronted by a crisis. The capacity of a system or network to maintain operation, despite an incident, is essential for limiting the downtime of services.
Adista has established five main recommendations so that companies can ensure continuous operation in the event of an emergency and are able limit the impact of a major incident to the greatest extent possible:

1. **Reducing vulnerability to hackers** by implementing effective systems for controlling and filtering access, but also by regularly applying and enforcing security updates.

2. **Prioritising dynamic protection** by using advanced technologies such as EDR or IDS/IS to significantly reduce risks.

3. **Engaging employees** by developing a cyber-culture within the organisation and by promoting good behaviours for combating threats and reactions when an event is detected.

4. **Preparing for the worst** by backing up and verifying recovery capabilities, identifying reliable partners in the case of an incident, and transferring residual risks to an insurer when this is possible.

In order to outperform the cybersecurity and achieve cyber-resilience, there must be a focus on the behaviours of all internal participants and not just the security teams. A more global approach **placing individuals at the heart of cybersecurity.**

With this in mind, Adista has launched **an unprecedented and innovative employee awareness campaign** that comprises a photo-story, web and printed posters. The photo-story is an initiative that is unparalleled in the sector, and presents three everyday incidents of cyberattack and the best ways of responding to them. The quirky posters remind us of the importance of day-to-day vigilance when the danger exists of attacks that are increasingly sophisticated.

Adista: more than 30 years of expertise helping organisations become cyber-resilient

In its role as a Telecom operator and provider of information management services such as computer hosting, Adista has a long history of integrating the essential component of cybersecurity into the construction of resilient information systems.

Adista's Cybersecurity and Cyber Resilience offer is supported by a dedicated centre of expertise with adequate training to ensure the security of the IS of several hundred customers, local authorities, SMEs, intermediate-sized or large companies. Irrespective of the size or activity segment of the organisations that it works with, Adista operates and advises across a very broad spectrum. Its IT security experts define the security strategies, the business continuity and recovery plans. This strategy is personalised based on the context and the requirement defined by the organisations' leaders. Even more that simply protecting networks, infrastructures, and terminals, Adista has chosen a position that includes organisational aspects and the human factor.

"We assist organisations to develop a genuine cybersecurity culture, by training employees to adopt the best practices when confronted by IT risks. An efficient way to anticipate threats more effectively and reduce risks. "

David Boucher, Manager of the Adista Cybersecurity Expertise Centre

Adista is currently involved in the security of several hundred organisations, **in particular by protecting more than 17,000 workstations and several tens of thousands of inboxes.**

About Adista

A Hosted Services operator, Adista is positioned as the number one alternative B2B cloud and telecoms operator in France and the specialist in IT and voice services. Adista's strength lies in its capacity to combine expertise as a host, a telecommunications operator and a specialist in business IT and the security of information systems. End to end control over the quality of services, a hybrid vision of the Cloud and the capacity to deliver IT services and THD technologies all over France have made the company's success. With the acquisition of Fingerprint in 2020 and Waycom in 2021, Adista has this year joined forces with unyc, a major player in indirect sales of telecom services. The company achieved sales revenue of 222 million euros in 2021 and counts 900 employees working in forty agencies. Its ambition is to generate sales revenue of 500 million euros in 2026 and become the number 3 B2B telecoms operator in France in ten years.
www.adista.fr

PRESS CONTACT - WORDCOM Consulting
Tel. 01 45 44 82 65
Eglantine de Cossé Brissac eglantine@wordcom.fr
Ellora Possenti rp@wordcom.fr