

The Impact of Cyber Attacks on Reputation: Insights from Andrea Baggio, CEO of Help Ransomware

[Multimedia](#)

Online security and reputation expert Andrea Baggio, CEO of Help Ransomware, discusses the impact of cyberattacks on reputation

In the past year, 66% of organizations have been hit by ransomware.

These figures threaten the stability, economy and reputation of businesses large and small around the world, affecting both public and private organizations and causing damage at all levels.

In light of this reality, Andrea Baggio, CEO and co-founder of [Help Ransomware](#), a global leader in cybersecurity and corporate reputation, sets out some advice. The project was born out of a desire to provide a solution for those who fall victim to these unexpected situations, offering unique and effective tools.

What is Help Ransomware?

Help Ransomware is a cybersecurity company that is part of the [ReputationUP Group](#), a multinational company that provides IT and online reputation services.

Services provided by Help Ransomware include:

- 24/7 ransomware decryption;
- Guaranteed recovery of ransomware-encrypted data;
- Ransomware protection and prevention consulting;
- Incident response planning;
- Training;
- Data breach and leak protection;
- Monitoring and remediation of data leaked by ransomware;
- Crisis Management and Reputation Protection;
- Cyber insurance.

The Reality for Organizations that Suffer a Cyber Attack

The first thing to know is that when an organization suffers a cyberattack, the company's entire system grinds to a halt.

“When a company is attacked, it cannot access its information, and we as a group are the first to offer a comprehensive 360-degree service. We reach the attacked company and recover the stolen data, and we also tell them how and why the attack occurred: only by finding the source of the problem can we restore the company's operations,” explains Andrea Baggio.

“We also take care of all the legal aspects. Beyond the technical part, when a company is attacked, it has to issue a statement explaining whether sensitive data of third parties has been affected or justifying any delays or disruptions in services: we provide them with the tools to communicate this to suppliers, customers and their collaborators, which is an essential part of crisis reputation management,” continues the CEO of Help Ransomware.

Why Companies Should Invest in Protection Against Online Attacks

Today, there is an alarming reality: cyber-attacks and those causing reputational crises are increasing at a rate of 3,000% per month, according to public data.

Many of the affected companies face a range of issues, including reputational damage, economic damage from data recovery, and financial damage from the disruption of daily business operations.

“2021 was the year with the highest number of ransomware attacks: there were 623 million attacks worldwide, a 105% increase from 2020, according to the 2022 IDC and Statista report.

It's important to note that the average cost of repairing the damage from a ransomware attack is \$1.85 million, and critically, 43% of organizations that paid the ransom were still unable to recover their data, resulting in further loss,” Baggio explains.

Advice for Protecting Businesses and their Online Reputation

According to Andrea Baggio, CEO of Help Ransomware, there are two main things to do.

The first is to constantly monitor everything that happens around the company: in this type of attack, there is not a second to lose, because the hackers will use this time to cause greater damage to the company.

In fact, the second thing you need to do is to invest in training people in cybersecurity: not just the technical people, but everyone needs to know what to do, so that when an attack spreads via email, such as a typical phishing attack, everyone can act. [How to Mitigate the Impact on the Company's Reputation after a Ransomware Attack](#)

The first step is to avoid misrepresentation: 90% of companies that have been

attacked or are in a reputational crisis spread false information.

The second thing is to report what happened correctly: you need to communicate clearly and concisely what happened to customers, suppliers, the press and the entire internal and external communications team.

That is why the ReputationUP Group, together with Help Ransomware, decided to act in both directions, offering a unique service for IT and online reputation protection, with 25 years of experience in Europe and America.

“We work 24/7 to make a company's reputation its most valuable asset”, finalizes Baggio.
