Involving Law Enforcement in Ransomware Response Improves Security for All

The number and cost of ransomware attacks continues to rise. And yet, many organizations resist involving law enforcement in ransomware response. Some fear that involving law enforcement will highlight the attack and negatively affect business reputation. Others worry that investigator demands will distract from recovery efforts.

However, reporting ransomware attacks can prove beneficial both for the reporting organization and for the general fight against cybercrime. Additionally, in some cases regulatory compliance and insurance mandates may require that organizations alert law enforcement.

Unique Challenges of Ransomware

When thieves steal money from the cash register or vandals destroy company property, business representatives contact the police as a matter of course. With ransomware, the choice of whether to report and whom to call is more complex.

To begin with, since ransomware often involves state-backed cyber-attacks, local authorities may have no jurisdiction. In addition, investigating cyber attacks requires specialized technology and skills that many agencies do not possess. And it can prove difficult to immediately determine whether an actual data security breach has occurred.

The ransom demand itself adds further wrinkles. While the FBI and other agencies strongly discourage paying ransoms, sometimes businesses feel they have no choice. But ransom payments do not guarantee data recovery and may actually increase the chance the organization will suffer another attack.

Benefits of Involving Law Enforcement in Ransomware Response

While some organizations may hesitate to report a ransomware attack to authorities, involving law enforcement brings several key benefits, including:

- Sophisticated cyber investigation tools – Because agencies like the FBI have devoted teams specifically to fighting cybercrime, they have access to innovative resources unavailable to many organizations.
- Ability to leverage inter-agency relationships – In addition to investigative tools, law enforcement agencies can coordinate with their partners internationally. These relationships aid both in locating stolen data and in identifying and apprehending cyber criminals.
- Authority to issue subpoenas – Ransomware often travels through the supply chain. The FBI can issue warrants to gather critical data from third parties that may also be affected by the attack. Linking related attacks and developing a more complete picture increases the odds of finding the perpetrator.
- Wealth of information about bad actors and current threats – Over years of cyber investigations, law enforcement has gathered deep knowledge of threat actors and ransomware variants. They may even have a decrypter on hand to help victims recover their data without contacting the attacker.

- Improving security for all – As ransomware victims report attacks, the information helps law enforcement develop a clear picture of current threats and how to approach them. Typically, a single ransomware attack represents part of a much bigger picture. Putting the puzzle pieces together helps everyone.

How to Report a Ransomware Incident

In the event of a ransomware attack, organizations must act quickly. Know ahead of time which agencies to contact and how to reach them. In most cases, the local FBI field office represents a good place to start. Additionally, report the incident to the FBI's Internet Crime Complaint Center. The agency does not release that information to the public.

Local authorities will typically offer only limited investigative resources. But in some cases, your state's data breach notification laws may require that victims notify a state agency or a consumer protection agency.

Law Enforcement Just One Part of Overall Incident Response Plan

While ransomware victims should report incidents immediately to law enforcement, this forms just one piece of a comprehensive response. Take time before an incident occurs to create an incident response plan. This plan will include steps to identify, contain and eradicate the threat. It will also involve communication plans and recovery procedures.

The cybersecurity experts at eMazzanti stand ready to assist organizations in identifying security risks and implementing strategies to prevent ransomware. They will help you build an incident response plan to address threats proactively, minimizing the possible damage.