After Cyber Extortion.. What to do?

Here is an interesting article on how a Company should respond after a Cyber Extortion demand.

How to Deal With Cyber Extortion – Before and After It Occurs

Once a company or individual becomes a victim of cyber extortion, the number of good options dwindles quickly. Rather than react after the fact, corporate leaders need to have a response plan in place so mitigating the risk of cyber extortion schemes can be the main focus.

The author of this article suggests a comprehensive plan that should include

- A list of stakeholders to be informed.
- Predetermined and defined lines of communication that will speed information sharing.
- Appropriately trained and informed leaders empowered to make decisions during an incident.
- A process for the continuous updating of information technology systems and security policies (at least quarterly) to keep pace with changes in business and technology.
- Established relationships with law enforcement (local, state and/or federal) to reduce the chance of a slow, confused response.
- **Prevention**Companies can also take a number of steps to lessen the likelihood that they will fall victim to cyber extortion or extortion:
    - Identify all potential internal and external threats by:
        - Monitoring social media.
        - Staying on top of public forums related to

your business.
    - Identifying employees who may want to harm your company.
- Audit computer networks to identify and assess vulnerabilities. Questions include:
    - Are software patches being applied in a timely fashion?
    - Does the network have segmentation so that an attack in one area won't impact others?
    - Are there access controls in place for your data?
    - Are network logs collecting sufficient detail and maintained for a long enough period of time to allow for proper historical investigation?
    - Do you know where all your endpoints are and are network topology maps up to date? This especially is important because networks are dynamic, with companies continually adding and removing servers and distributing new devices to employees.

Refer here for the detailed article: Source Cyber Security Today