



The Ransomware Stages of Grief

Tony Kirtley
FIRSTCON 2022
July 1, 2022

The Ransomware Nightmare

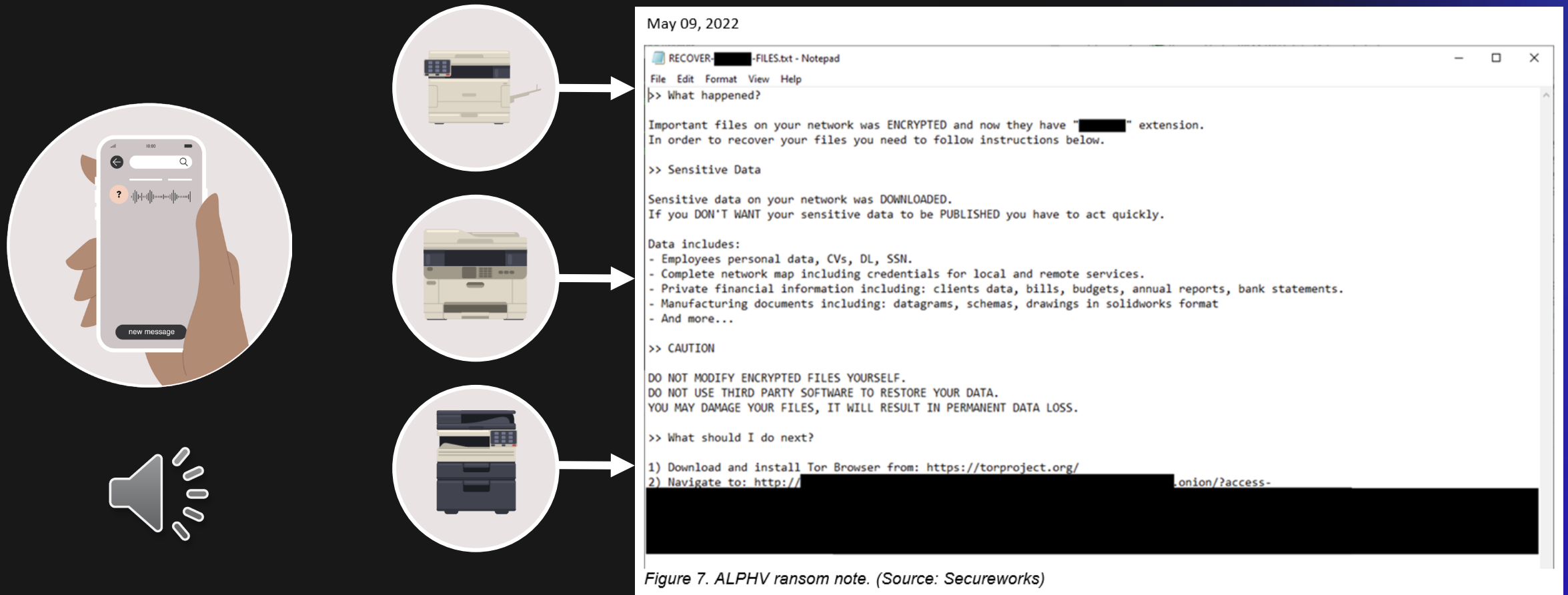
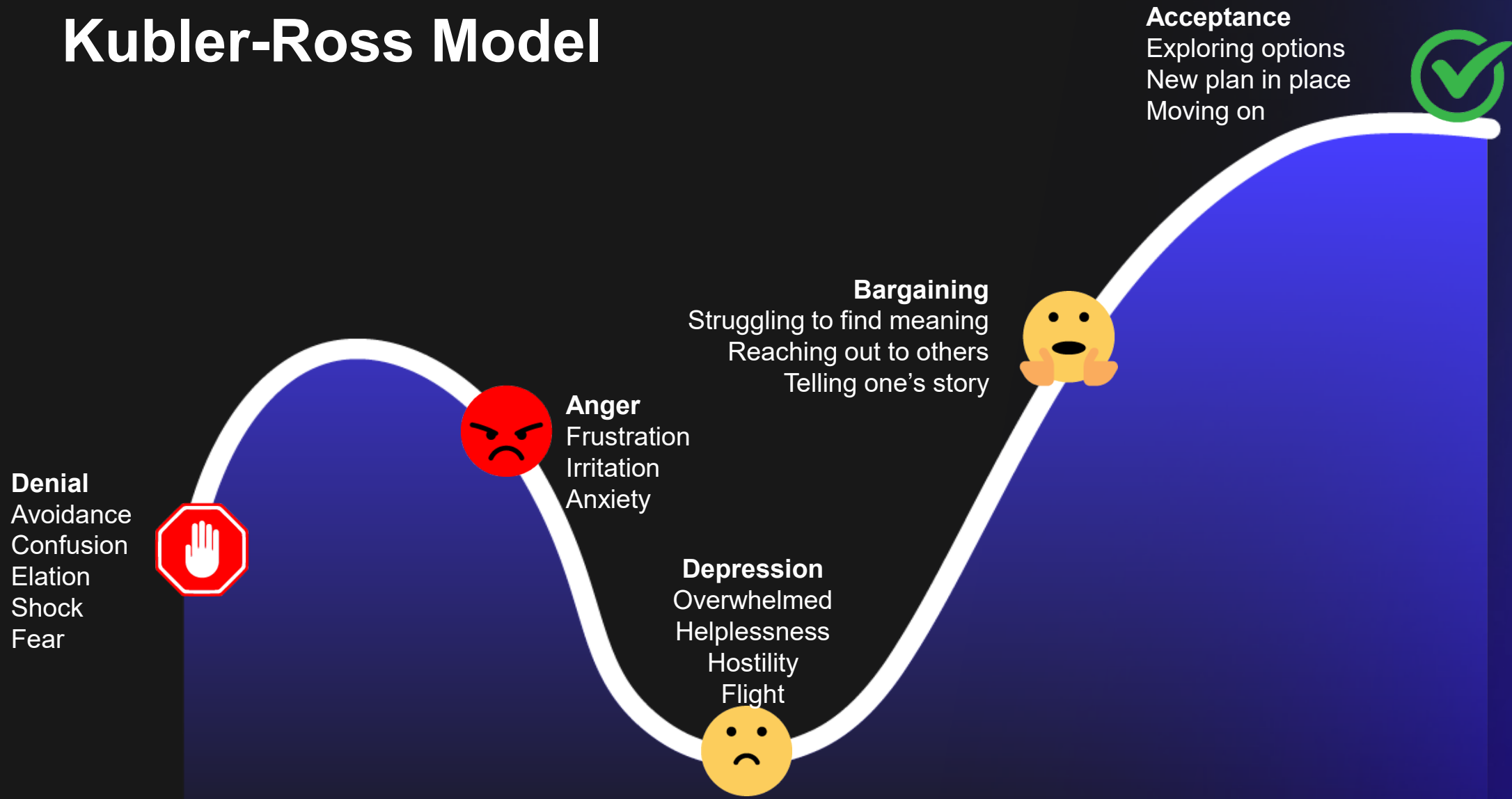
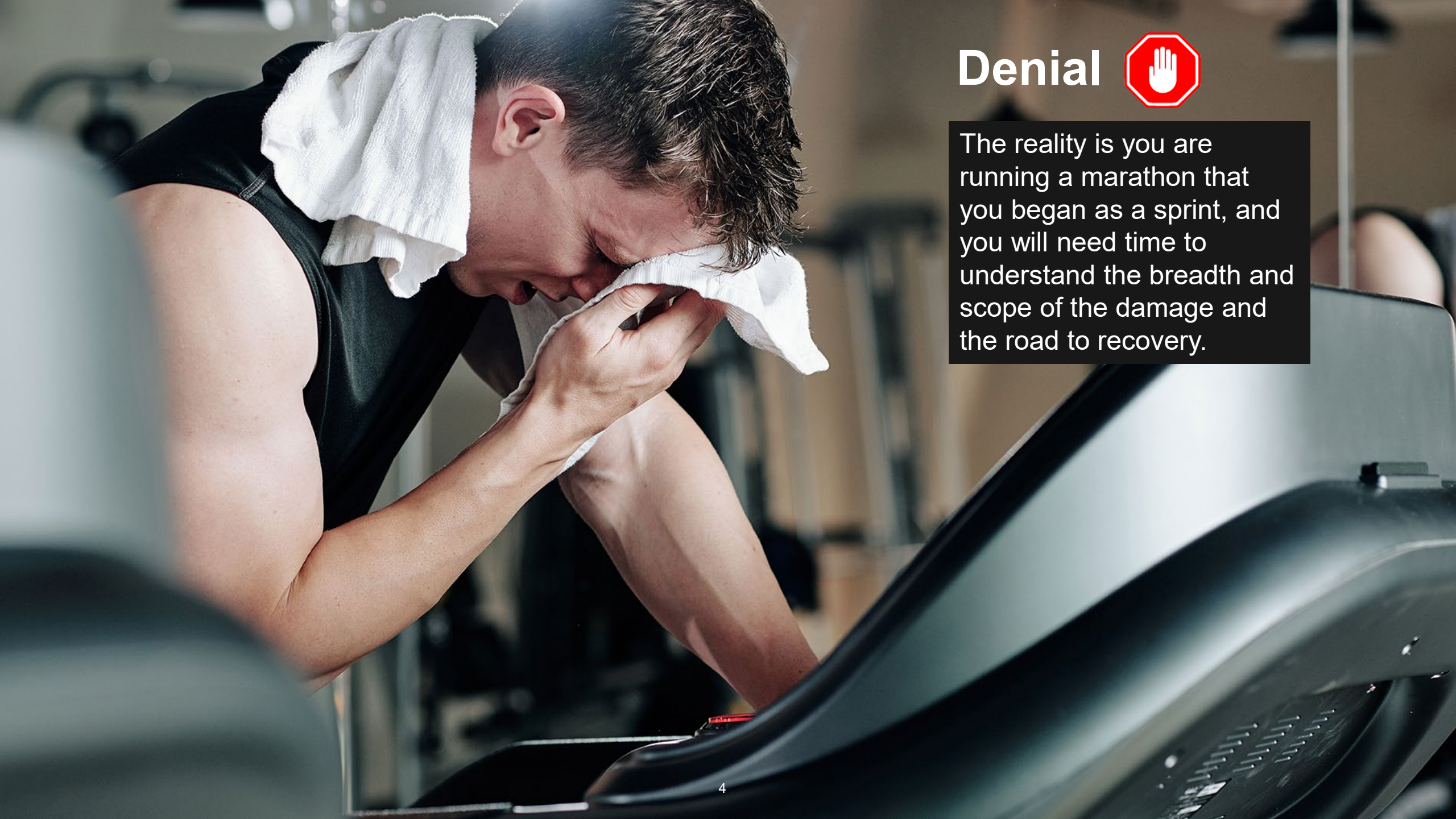


Figure 7. ALPHV ransom note. (Source: Secureworks)

Kubler-Ross Model



A man in a black tank top is running on a treadmill in a gym. He is looking down, sweating, and has a white towel draped over his head. He is using the towel to wipe sweat from his face. The background shows other gym equipment and a blurred figure of another person.

Denial



The reality is you are running a marathon that you began as a sprint, and you will need time to understand the breadth and scope of the damage and the road to recovery.



Anger

Be aware, that your anger may start to migrate to your team members and partners, affecting their performance.

Depression



The situation hit you unexpectedly. Your business is down for the count, and for every step forward you take two steps backward.





Bargaining



When faced with near or complete business failure, it is natural to want to rally your team for an epic response push.



Acceptance

The sooner you can come to terms with the situation at hand and the enormity of the challenges ahead, the sooner you will start to make rational and informed decisions that will expedite your recovery rather than hinder it.

Conclusion

1

While experiencing the shock of the situation, lean on the experts to give you perspective, and don't be afraid to ask for more help.

2

If you experience anger, ensure that it is not directed at your team. Create a no-blame environment for your staff.

3

Establish and enforce a manageable response tempo to allow your team to get enough rest to be at their best.

4

Stay positive in light of a gloomy situation. Your attitude in the face of adversity is contagious and could greatly affect the timeframe of recovery

5

The best way to avoid the pitfalls of ransomware is to prepare and trust the recovery process.

Secureworks Incident Response Hotline



If your organization needs immediate assistance for a potential incident or security breach, please contact Secureworks directly on the Global Incident Response Hotline. Our globally accredited Incident Response team is ready to assist 24x7x365.

Global Emergency IR Hotline

+1 770-870-6343

<https://www.secureworks.com/contact/emergency-response>

Secureworks®