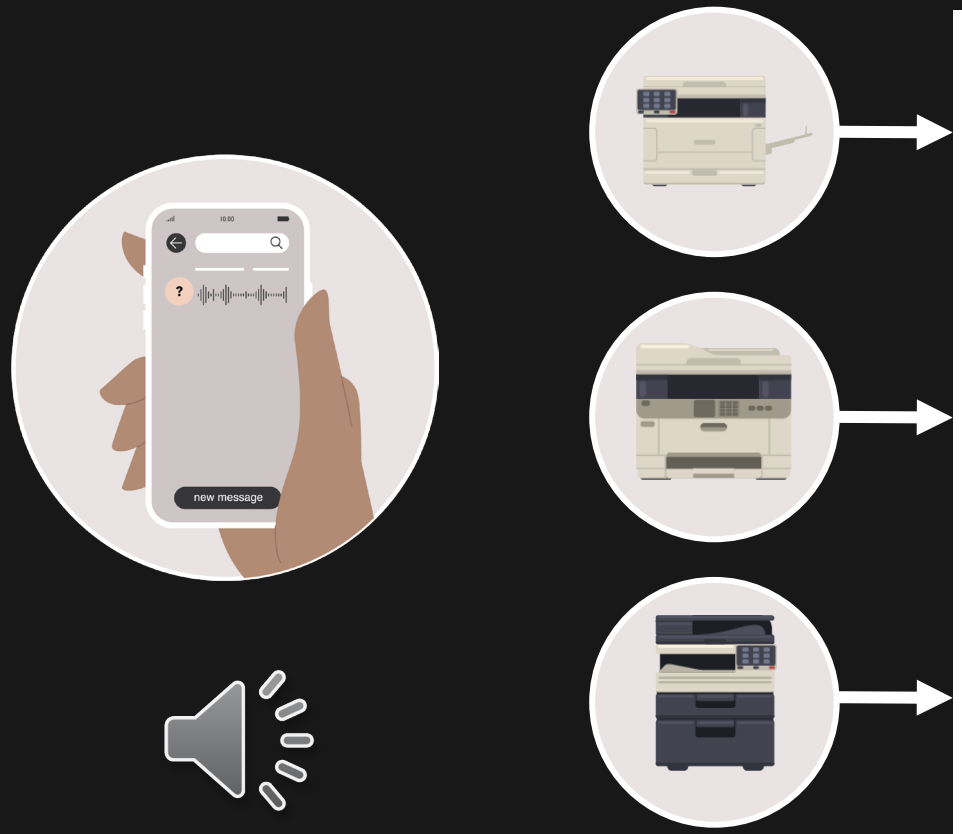
The Ransomware Stages of Grief

Tony Kirtley
FIRSTCON 2022
July 1, 2022

The Ransomware Nightmare



May 09, 2022

RECOVER-[redacted]-FILES.txt - Notepad

File Edit Format View Help

```
>> What happened?

Important files on your network was ENCRYPTED and now they have "[redacted]" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- Manufacturing documents including: datagrams, schemas, drawings in solidworks format
- And more...

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://[redacted].onion/?access-
[redacted]
```

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

Secureworks

Kubler-Ross Model

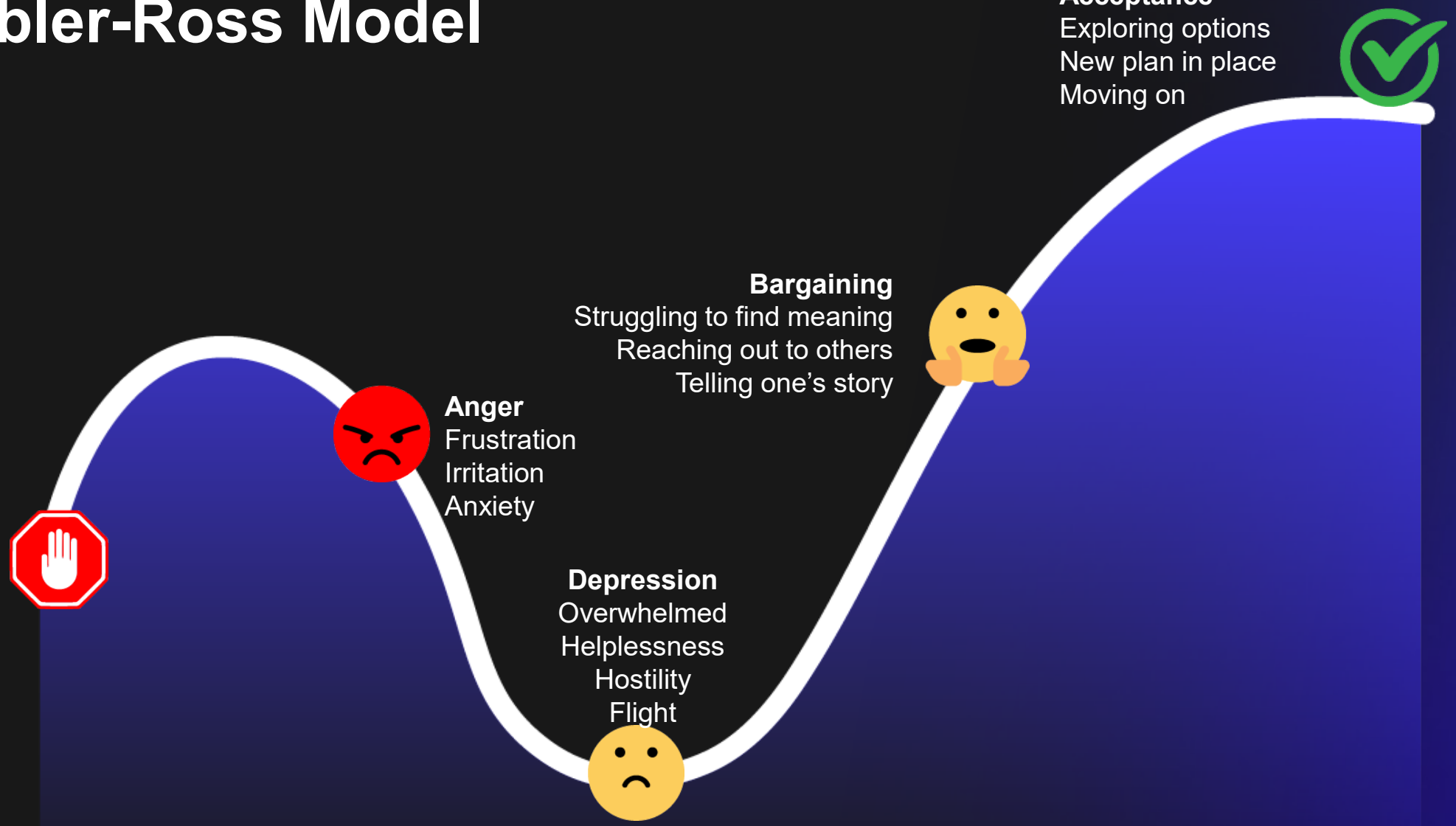
Denial
Avoidance
Confusion
Elation
Shock
Fear

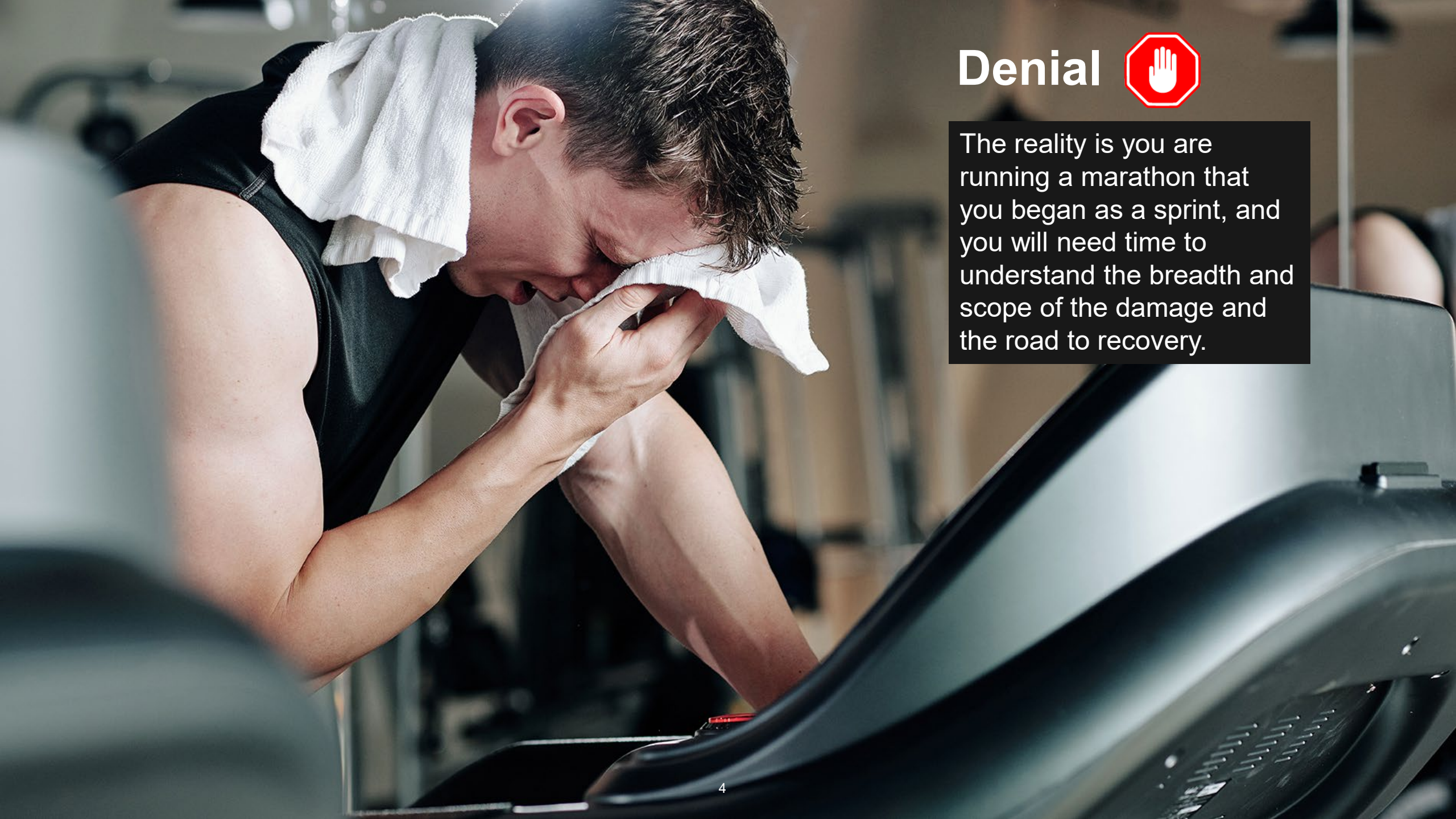
Anger
Frustration
Irritation
Anxiety

Depression
Overwhelmed
Helplessness
Hostility
Flight

Bargaining
Struggling to find meaning
Reaching out to others
Telling one's story

Acceptance
Exploring options
New plan in place
Moving on





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 in 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®