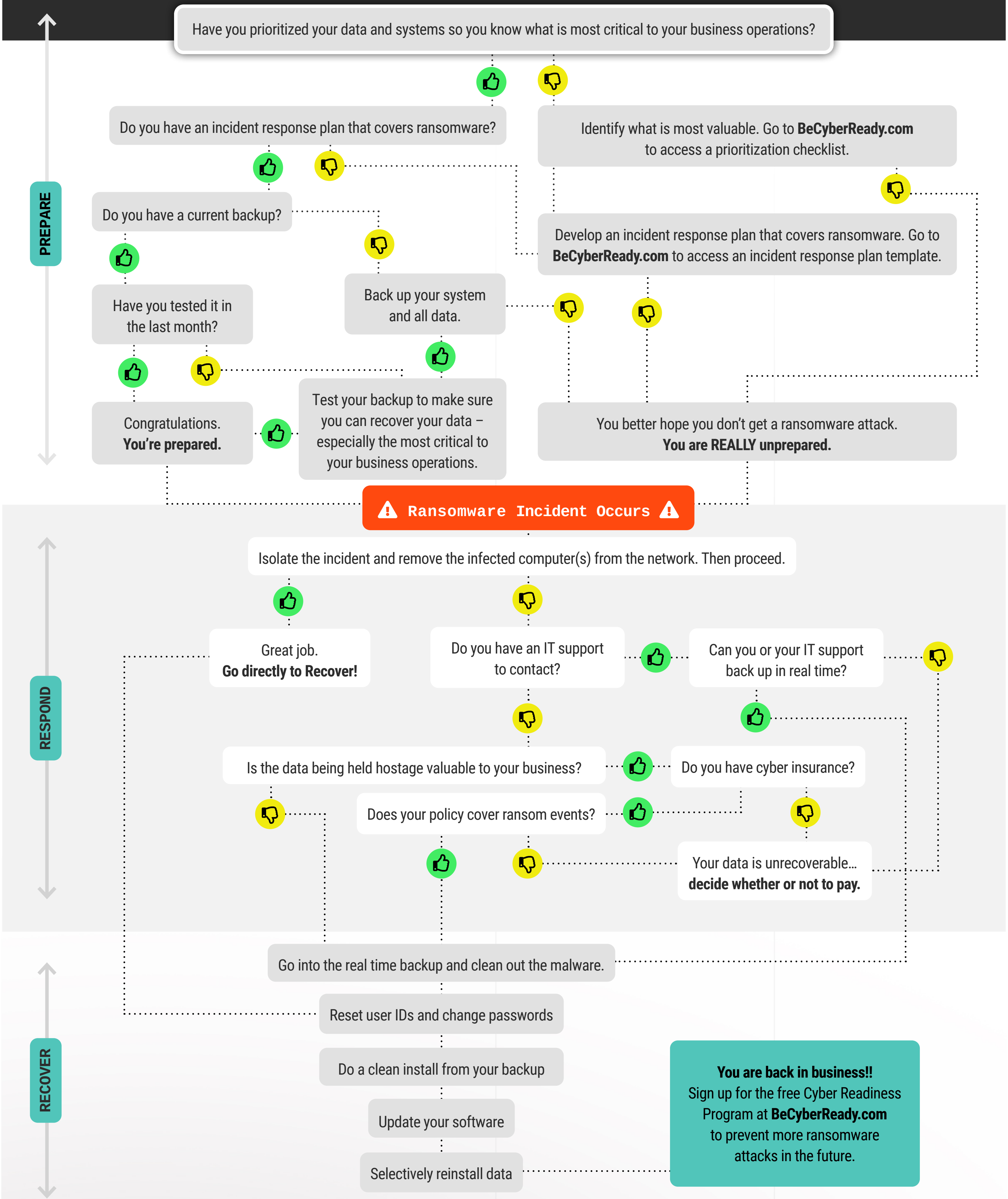
Ransomware Decision Guide



PREPARE

Have you prioritized your data and systems so you know what is most critical to your business operations?

Do you have an incident response plan that covers ransomware?

Identify what is most valuable. Go to **BeCyberReady.com** to access a prioritization checklist.

Do you have a current backup?

Develop an incident response plan that covers ransomware. Go to **BeCyberReady.com** to access an incident response plan template.

Have you tested it in the last month?

Back up your system and all data.

Congratulations. **You're prepared.**

Test your backup to make sure you can recover your data – especially the most critical to your business operations.

You better hope you don't get a ransomware attack. **You are REALLY unprepared.**

Ransomware Incident Occurs

RESPOND

Isolate the incident and remove the infected computer(s) from the network. Then proceed.

Great job. **Go directly to Recover!**

Do you have an IT support to contact?

Can you or your IT support back up in real time?

Is the data being held hostage valuable to your business?

Do you have cyber insurance?

Does your policy cover ransom events?

Your data is unrecoverable… **decide whether or not to pay.**

RECOVER

Go into the real time backup and clean out the malware.

Reset user IDs and change passwords

Do a clean install from your backup

Update your software

Selectively reinstall data

You are back in business!! Sign up for the free Cyber Readiness Program at **BeCyberReady.com** to prevent more ransomware attacks in the future.

CYBERREADINESSINSTITUTE.ORG

guide@cyberreadinessinstitute.org