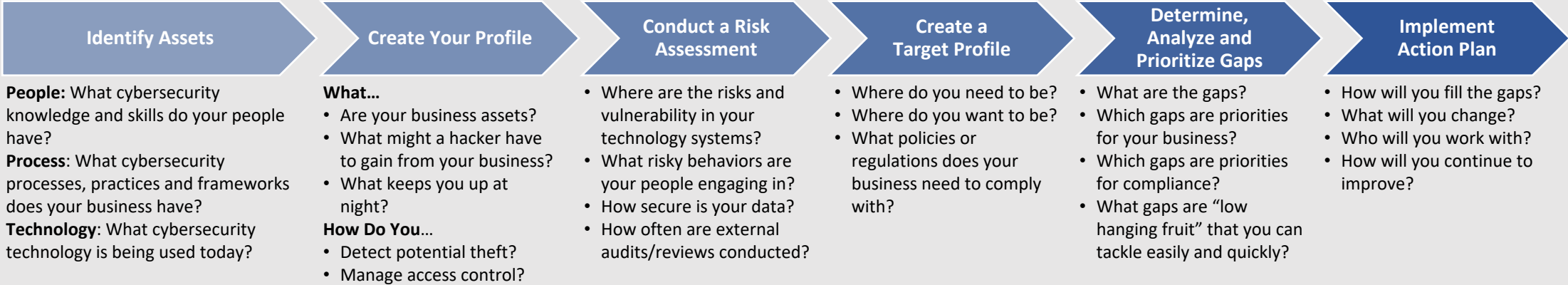




In today's connected world, cybersecurity cannot be ignored. For a small businesses, cybersecurity may seem like an intimidating endeavor. We're here to help!

We recommend beginning this journey by performing a **current state assessment**, creating a desired future state, and determining the gaps. To close the gaps, remember you have NCSS resources and support to help you get where you want to be.



What would an ideal future state look like?

People	Process	Tech
<p>The workforce is aware of how their behavior online affects their organization's cybersecurity. Everyone uses strong passwords and has good e-mail habits, and your champions have strong cybersecurity skills. Your organization has a regular cyber training regime, so the workforce can keep pace with the rapidly changing world of cyber and so they don't forget these practices.</p>	<p>The organization has plans and processes in place to secure data, networks and systems, and protect the organization in the event of a cybersecurity incident. Processes will make sure operating systems are regularly updated, devices configuration is actively managed, software is updated, patches are implemented quickly, hardware is replaced regularly, and updating IT is part of the process when people leave the organization. Plans to protect data "crown jewels" will protect customers and partners, and plans to respond in the event of a cyber incident will protect the organization's brand.</p>	<p>IT is modern and commercial, when possible. The organization outsources backend hardware, like routers and switches, and data storage solutions, like cloud, to third-party vendors when appropriate, and uses a commercial cybersecurity service. Hardware and software are up to date, and IT audits ensure the organization has an accurate understanding of their organization's IT and security posture.</p>