Cybersecurity Improvement Plan

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.*

Identify Assets

People: What cybersecurity knowledge and skills do your people have?
Process: What cybersecurity processes, practices and frameworks does your business have?
Technology: What cybersecurity technology is being used today?

Create Your Profile

What…
- Are your business assets?
- What might a hacker have to gain from your business?
- What keeps you up at night?

How Do You…
- Detect potential theft?
- Manage access control?

Conduct a Risk Assessment

- Where are the risks and vulnerability in your technology systems?
- What risky behaviors are your people engaging in?
- How secure is your data?
- How often are external audits/reviews conducted?

Create a Target Profile

- Where do you need to be?
- Where do you want to be?
- What policies or regulations does your business need to comply with?

Determine, Analyze and Prioritize Gaps

- What are the gaps?
- Which gaps are priorities for your business?
- Which gaps are priorities for compliance?
- What gaps are "low hanging fruit" that you can tackle easily and quickly?

Implement Action Plan

- How will you fill the gaps?
- What will you change?
- Who will you work with?
- How will you continue to improve?

What would an ideal future state look like?

People

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.

Process

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.

Tech

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.

Technology is always changing. You should be too.

Cybersecurity assessments should be a regular part of your annual business planning.