GCA Cybersecurity Toolkit Backgrounder: Know What You Have Toolbox

GCA Cybersecurity Toolkit For Small Business

It is really important to understand what you have because you cannot protect what you do not know you have. By knowing what you have, you will:

- Understand the potential risks, allowing you to do something about them
- Know that you will never remove all the risks, but you can reduce them
- Have better cyber hygiene and awareness, which can limit your exposure to up to 80% of common threats

Cybersecurity is a journey, not a destination, so start building it into your daily routine.

Know What You Have Checklist

<u>Create an inventory:</u>

- What's in your IT environment?
  - ○ *Your devices - desktops, servers, laptops, smart phones, tablets, POS, IoT, CCTV…*
  - ○ *Your applications - Microsoft Office, Adobe, POS applications, Chrome…*
  - ○ *Your online accounts - email, Amazon, iCloud, Facebook, banking, credit cards…*

- What is accessible from the Internet or on your internal network?
  - ○ *An IoT device that shares your internal network but can be controlled over the Internet could pose a risk*
  - ○ *An old device no longer in use and unpatched, but still switched on, may be vulnerable to an attack*
  - ○ *Any device that still uses a default password you have not changed is a common way in (a CCTV system with a simple admin/admin password or older router for example)*
  - ○ *An old online account you don't use but still holds your data may suffer a breach and leave you (and other connected devices) at risk*
  - ○ *Software on your computer you no longer use or maintain but have not removed may be targeted*
- What level of access is needed to ensure 'business as usual' functionality?
  - ○ Has access been removed for those that no longer need access?
    - *Relationships ended with third-party contractors?*
    - *Supply chain companies that no longer exist?*
    - *Employees that left the organization, changed roles, or are on extended leave?*

- ○ Have systems and applications been removed that are no longer relevant or in use?
- ○ Limit the number of users with admin privileges. Admin level access should only be for administrators and not daily users of the systems or applications.

- Restrict access to systems and applications to potentially reduce the damage from:
    - Intentional and accidental insider threats caused by:
        - *Deliberate action by a disgruntled employee*
        - *An employee blackmailed to access confidential information*
        - *The impact and consequence of opening a phishing email*
        - *Accidental deletion or corruption of data*

While doing the inventory, also consider whether strong password requirements are enforceable and Two-Factor Authentication (2FA) is enabled. (2FA is an additional layer of protection for your passwords.)

- Create separate networks and restricting access rights (admin/user/none) so that sensitive information is harder to get to and key systems do not sit on the same network as less secure devices, potentially reducing the impact of an attack because:
    - Many consumer IoT devices have no, or very minimal, built in security
    - Older equipment may be out of warranty and no longer protected against new vulnerabilities
    - Third parties with network access rights offer a route in for attackers
        - *If third parties do have access to your network, do they have a policy in place to enforce password changes when key personnel leave?*

- Make sure you keep your inventory updated on a regular basis, including whenever you add or delete new equipment, accounts, or critical data.

Use the tools in the 'Know What you Have' Toolbox to help you or to develop an alternate system that works for you.

https://gcatoolkit.org/smallbusiness/know-what-you-have/