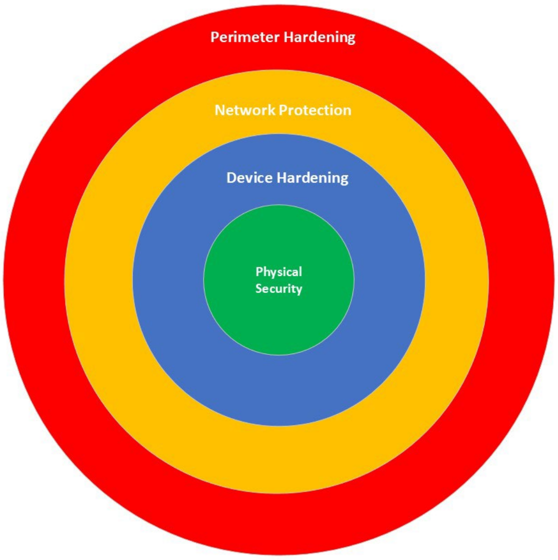
RECOMMENDED CYBERSECURITY BEST PRACTICES

We Value and Prioritise Cybersecurity

We recommend that you follow the cybersecurity best practices outlined in this document to minimise the risk of successful cybersecurity attacks.

1 Defence In Depth



We consider security during the design, development and manufacture of our products. Our products are thoroughly tested for security vulnerabilities, and we provide updates, as needed. This ensures that our products are kept current and reduces exploitable weaknesses.

Our products are designed to be incorporated into networks protected by defence in depth mechanisms. Within these mechanisms are multiple layers of protection (as displayed in image above), used to reduce the risk and impact of security events. This document provides general guidance on best practices to ensure that our products remain secure once installed in your organisation.

We recommend the following best practices:

2 Physical Security

It is important to implement physical controls that prevent and/or monitor physical access to the device, including:

- Controlling access to the device location
- Physically locked cabinets
- Physical protection of cabling and power supply to the device
- Physical protection of any remote controller or device that connect to the device
- Security monitoring of physical access either by security cameras or door access logs.

3 Device Hardening

Device hardening is the process of reducing the attack surface of the device and any devices used to connect to the device and involves:

Controlling Authentication and Authorisation

Utilise a Role Based Access Control (RBAC) mechanism that uses security identifiers uniquely assigned to individuals, provides the least privilege required by the role and that enforces strong password policy with Multi-Factor Authentication (MFA) where possible. Often this is achieved by federation of access with directory services such as LDAP or Active Directory.

If it is impossible to remove or disable unnecessary default user accounts, firstly ensure that default passwords are changed. Secondly, tightly control access to the credentials of any built-in accounts, for example, use Password Manager to store passwords.

Minimise Exposed Functionality

Disable or remove unused and unnecessary functionality on both the device and any devices connecting to it. This includes disabling or removing unused services and software. Limit software installation to safe, whitelisted software.

Implement device level security protections.

Install and maintain anti-virus and anti-malware products where appropriate. Implement local firewalls and limit access to required additional devices and protocols.

Scan devices such as USB devices to confirm they are malware free before using them on the device or any devices used to connect to it.

Read user manuals, product notes, and our website (softstarterhub.com/cybersecurity) to be aware of specific information about the security features for your device.

Encourage secure device operation

Educate staff so that they are aware of secure operation practice. Ensure they do not disclose passwords and when leaving them, they log out or lock workstations.

Ensure Recovery

Complete regular data and configuration backups of all components required to operate the device. Securely store your backups and test recovery procedures periodically.

4 Network Protection

Segment your networks

Use network segmentation to separate Industrial Control Systems (ICS) from business networks and to separate devices that are un-related within networks. This will reduce the ability of a cyber attacker who compromises one part of the network to transition to another.

Use secure remote access

Strictly control and secure mechanisms used for remote network access. Limit the number of remote access points and mechanisms. Authenticate users using strong techniques such as IP whitelisting, Public Key Infrastructure and Mult-Factor Authentication.

Limit Network Protocols.

Allow only those network protocols and ports required within the network. Drop traffic that is unnecessary or unexpected.

Maintain an Asset Inventory and Network Documentation.

Increase the likelihood that patching is kept current, and backups are complete by implementing an inventory and map of assets (including software and hardware). Automated inventory tools can assist and inventory can include:

- All devices connected to the network, including IP addresses, protocols and connection locations
- All software and firmware versions
- Any spares
- Any network-to-network connections

Monitor your Network

Set up network monitoring to minimise the chance of compromise. This can include all or a selection of these items:

- Intrusion detection and prevention systems (IDS/IPS)
- Traffic volume and flow monitoring
- Time synchronized log collection and analysis
- Anti-Virus and Anti Malware software and alerting

5 Perimeter Protection

Protect outside access to your network by:

- Disabling direct access to other networks, and in particular, the internet
- Using Firewalls with Deny-all firewall rules that allow only specific and expected traffic to enter or exit the network.
- Implement Denial of Service protection
- Monitor and alert for events that might indicate attempts at Unauthorized access

Be Prepared

Keep all devices and software patched and updated. Companies issue fixes for security vulnerabilities regularly. By keeping your software, networking equipment and devices patched you minimise the likelihood of compromise.

Legacy devices and software also pose a risk. This is software or a device that is unsupported by the vendor, including old networking equipment and operating systems. In general, these should be retired. In these cases, the vendor will no longer support the device or software and may no longer be examining or patching it for security vulnerabilities. Consequently, if you do have a security issue you may be unable to get support.

Implement an Incident Management Plan

The reality is that even with the best protection, you cannot eliminate the risk of security incidents. You can however reduce the time and impact of any incident by implementing and testing an incident management plan. In your plan identify roles, responsibilities, possible compromise scenarios and impact mitigations.