


SIA CYBERSECURITY ADVISORY BOARD

Beginners Guide to Product and System Hardening

The SIA Cybersecurity Advisory Board recommends a few basic safeguards to help protect security products, systems and services against failure from cyberattack. This is by no means an exhaustive list. Cybersecurity processes and technologies are constantly evolving along with the threats; the following can serve as the beginning for a larger cybersecurity plan.

These are the top 10 causes of cybersecurity failure in systems.

1. Inadequate security policy and process governance
 - Establish a department or a team that responds to reported threats.
 - Provide a way for end users and integrators to report found risks.
 - Develop a framework as to how reported threats are discovered, fixed and taken out of production.
2. Reliance on “Security through Obscurity”—assuming that nobody will ever test security
 - Assume that all of your security will be tested.
 - Use proven ports and protocols.
3. Inadequate software and firmware patching; inadequate testing of patches before installation
 - Authenticate patches; verify the update source is trusted.
 - Use patch management tools.
 - Include patches and software versioning in your change management practices.
4. Unencrypted, unauthenticated and uncontrolled wireless communications within systems
 - Proceed like the network is untrusted.
 - Remember wired is always more secure.
 - Bear in mind denial of service protection is more critical when using wireless solutions.
 - Default to HTTPS.
5. Unencrypted, unauthenticated and uncontrolled communications between systems
 - Default to HTTPS.
 - Filter IP addresses.

- 
6. Poor password hygiene and insufficient segmentation of control system networks
 - Disable default passwords.
 - Require strong passwords before other configurations.
 - Use password-tracking tools when available.
 - Segment roles and responsibilities. (Don't use administrator privileges for non-admin duties.)
 7. Lack of auditing and audit monitoring on networks
 - Periodically audit the number of network connections.
 - Periodically audit network connection lengths.
 - Use information from these audits to target anomalies.
 8. Control system networks shared with other traffic
 - Ensure security networks are enterprise grade.
 - Patch regularly just as other enterprise networks are maintained.
 - Use of one network with mixed signals can be risky. When possible, segregate networks either physically or logically (VLAN).
 9. Poor coding of control system software causes failures
 - Enable application whitelisting.
 - Filter out dangerous executables.
 10. Lack of configuration management and tracking for hardware and software
 - Remove dormant code from firmware.
 - Track hardware and software versions when products leave the warehouse.

The SIA Cybersecurity Advisory Board's mission is to enhance SIA's cybersecurity posture and to guide the industry ahead of potential cybersecurity issues in an increasingly networked world.

Composed of several SIA Board of Directors who are cyberexperts both internal and external to the electronic physical security industry, the SIA Cybersecurity Advisory Board provides educational resources to security industry stakeholders and coordinates with other cyberforward organizations.