Axis Communications' Top 10 Cybersecurity recommendations

1. Make a risk analysis of potential threats and the possible damage/cost if the system is attacked.

2. Gain knowledge on system protection and possible threats. Work closely with resellers, system integrators, consultants, product vendors. The internet is a fantastic resource.

3. Secure the network. If network protection is breached it increases the risk of snooping for sensitive information and attack individual servers and network devices.

4. Use strong, unique, passwords and change them on a regular basis.

5. Do not rely on a network device's factory default settings
   > Change default password.
   > Enable and configure device protection services.
   > Disable services that are not being used.

6. Use encrypted connections when possible, even on local networks.

7. To reduce exposure video clients should not be allowed to access cameras directly unless it is required by the system/solution. Clients should only access video through a VMS (Video Management System) or a media proxy.

8. Check access logs on a regular basis to detect attempts on unauthorized access.

9. Monitor devices on a regular basis. Enable system notifications when applicable and supported.

10. Use the latest applicable firmware as it may include security patches.

www.axis.com/support/product-security

AXIS COMMUNICATIONS