Addressing the basics of cyber security

Jeff Whitney, VP Marketing, Arecont Vision & Member SIA Cyber security Advisory Board

Installers and integrators should choose products that provide adequate cyber security protection, only using devices that include basic security protection, such as user ID and passwords that can be enabled during or after system commissioning. Passwords are far from perfect, but are an essential first step with most systems.

Password practices should adhere to the current industry standard of up to 16 ASCII characters in length, and vary from device to device. For large networks, a secure password management system is recommended.

Equally important is that the balance between the user experience and cyber security protection is not a 'one-size-fits-all' solution. It must be adjusted for the specific requirements of the environment and associated risk.

Products selected should only be from manufacturers who have a demonstrated commitment to cyber security awareness, education and protection, and who are supportive of industry efforts and standards.

A growing number of devices, ranging from tablets and phones, home appliances, security alarms, manufacturing equipment, and even entire buildings are part of the growing IoT infrastructure. None of these devices should be allowed onto the network without verification that they are cyber-secure to current standards.

It is good policy to separate surveillance systems onto individual, dedicated IP networks or subnets. Sharing a single network for different systems and purposes increases both performance issues and the risk exposure to cyber attack. Typically, IT professionals will implement network segmentation as a standard practice.

Separate networks or subnets lessen the risk of a breach or cyber attack spreading beyond the targeted system, as well as lessening the risk of QoS (Quality of Service) impact.

'Air gapping' segments or entire networks, especially those that do not require Internet access or connection to the wider corporate network on a regular basis, is a good step for cyber protection.

Only use devices that support firmware and security updates. This is often overlooked for IoT devices. Any device connected to the network should be regularly checked for new firmware updates, tested and updated, just as IT typically does for devices under its control.

Limit access to systems, data and infrastructure to those who require it on a regular basis. A single password for all cameras, DVRs, NVRs, data storage, etc. is not secure. Enforce password changes on a regular basis.

Never use default passwords! An increasing number of breaches and cyber attacks are made using default log-ins. Security devices are no exception. Implement a strong password policy and enforce it.

Manufacturers that are serious about cyber protection should have a documented strategy for testing and integrating other components of the network infrastructure securely. A testing and/or certification lab for third party products is a strong indicator that they are serious about cyber security.]

Regularly scan the network for viruses and malware, as well as for security vulnerabilities. This basic step is often overlooked for security networks.

Installers and integrators need to ensure that all staff are aware of and educated in the risks and challenges of cyber security. Everyone needs basic cyber security awareness, and it should be part of the staff training and development.

Both IT and security departments should include cyber security as part of their regular reviews and assessments of the infrastructure and system.

Mitigation and recovery plans are key. Having a disaster recovery plan in place for the aftermath of potential cyber attacks shows end users that the system installer or integrator had adopted a responsible approach.

Finally, consider the risk and potential for damage to your company, its partners and its customers. It may be that cyber security insurance is key to mitigating the financial aspect and liability of such a risk.

Risk levels will vary based upon environment and organisation, and not every application will be appropriate for this type of protection.