Learn More about Physical Security vulnerabilities

Today, more and more physical security systems are connected to communication networks for security monitoring, safety and control. These connections leave systems vulnerable to cyber-attack. Increasing numbers of attacks on physical security systems and companies networks deployed in critical infrastructure facilities and corporations must be addressed with a solution that can defend against a broad range of both physical and cyber threats. Surveillance cameras, access control systems, sensors and controllers are connected using Ethernet, IP and other technologies, and rely on unsecured communication networks deployed across the site, as well as in the field. The use of these unsecured networks exposes the site to combined cyber and physical threats. For example:

- Video streams from surveillance cameras can be intercepted or manipulated
- Access control systems can be hacked to open gates and doors
- Perimeter security sensors and controllers can be disabled or blinded
- Industrial controllers and power distribution systems can be taken over and damaged

IP camera security and access control are a big part of the buzz about the Internet of Things (IoT). There should be more concern about how the industry has possible left the customer vulnerable to the threat of Cyber Security. CSI plans to fill the void and play a big part in that education and solutions for its clients.

The security industry has only recently become concerned with cyber security as it relates to physical electronic security. As an early adopter of IP Network Video, companies like mine (ACC) were focused on selling product and were unaware of the impact and vulnerabilities of attaching cameras to company networks. With the studies and concern brought about by the IoT, these problems were brought to light. Hardening of devices was not stressed and in most cases. Camera settings were left open to hacking by improper setup. Some Cyber companies use foreign white hats (i.e. friendly hackers) to avoid American Legal issues and Liabilities. CSI will use only vetted solutions from the security industry. CSI also has the advantage of using Licensed Technicians required in NC 74-D Alarm Licensing Act. CSI's principal has held a security license for over 24 years. CSI will also use credible sources from the industry to further emphasize the problems organizations face today. Most Integrators are just interested in making the sales, getting the system installed and after the sale service. It is obvious why they would not go back and fix Cyber concerns or if they even realize the problem. About 80% of all Integrator fall in that category. I gained this from experts in the area of Cyber Security that I talked with. Some manufactures such as Axis are being proactive in the solution and trying to educate Integrators on the proper techniques of Installing and Setup.