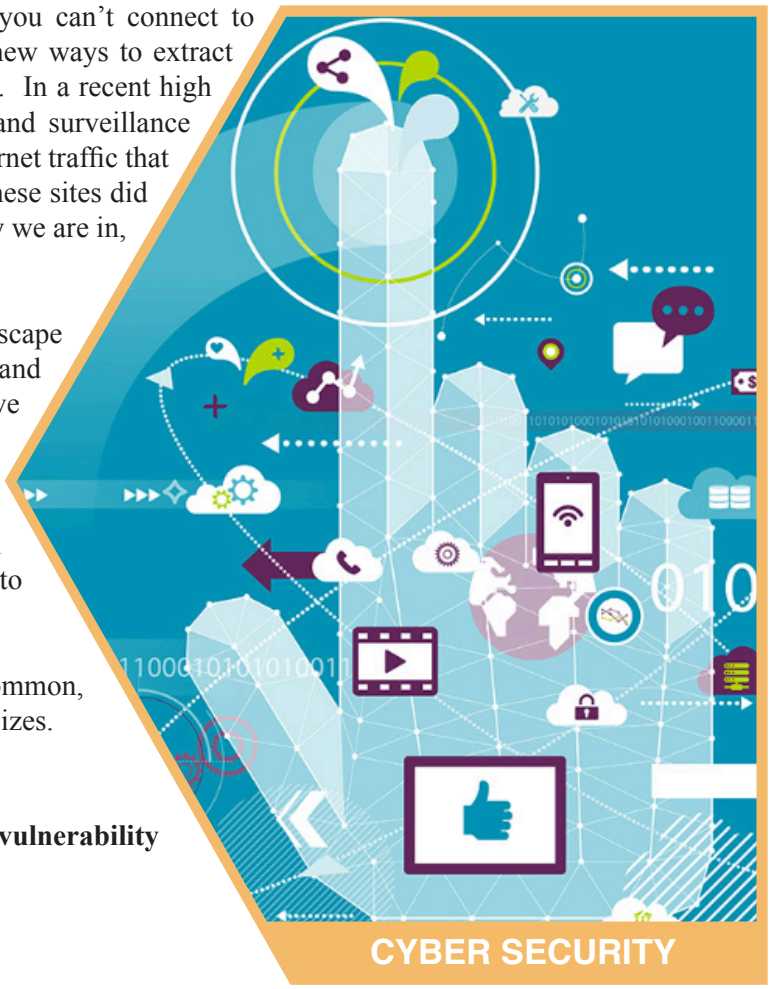
Network Security Cameras and Cyber Security, an Interview with Paul Laughton

With the Internet of things (IoT), there is seemingly nothing you can't connect to the internet. As IoT becomes ubiquitous, hackers are seeking new ways to extract valuable data or disrupt much needed services and infrastructure. In a recent high profile distributed denial-of-service attack, web cams, routers and surveillance cameras were all compromised and used to unleash a flood of internet traffic that crashed sites like Twitter, Netflix and Airbnb. While disrupting these sites did not affect our daily lives, we can see how, no matter what industry we are in, the potential for disruption is stronger now than ever.



There are many things that are so much a part of our normal landscape that may be affected by this type of attack. In our busy cities and organizations, I noticed a quiet but ever present device that I've always thought of as a safeguard, the network security camera and wondered how the companies responsible for designing, manufacturing and selling it are dealing with the new landscape of cybersecurity. Axis Communications, a pioneer and leader in the network camera market, described to me what they have done to ensure both innovation and security of their products.

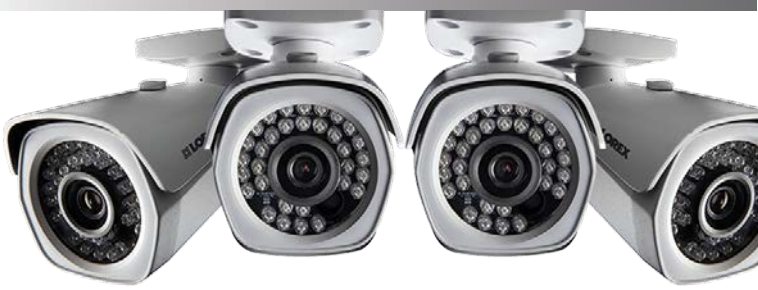
Paul Laughton of Axis shared his insights on some of the most common, current threats and what Axis is doing to work with clients of all sizes.

Threats specific to the camera

There are different types of threats. Specific to a camera, the vulnerability could be:

- A flaw to proprietary source code
- A bug in open source code
- A bug in standard protocols
- A weak product casing
- The ability to gain access to a device reset button
- Theft of SD card (if camera is not mounted properly)

The current standard is that cameras are on a segregated network even though they are using the same hardware. This is a virtual network (VLAN). The segregation happens on a switch. Almost as if it's two separate networks leveraging the same piece of hardware – this allows for better security.



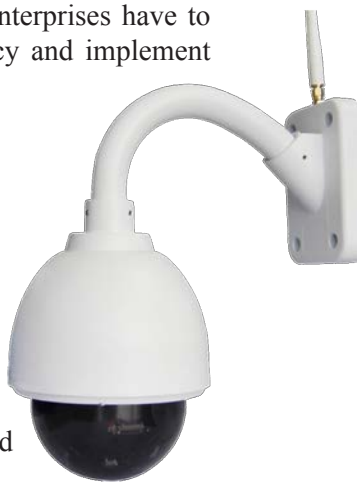
When organizations are purchasing cameras what should they look for in terms of features to minimize cyber threats?

Don't just look at the camera, look at the company providing it, and ask:

- Does it have a hardening guide?
- Does it have an educational program on how technicians can implement security features on a device?
- Does it release and publish a best practices guide?
- Does it publish its process on common vulnerabilities and how threats are handled?
- Does it talk about cybersecurity?

Risk Analysis and Network Security Policy

IP camera cybersecurity could include, multi-level authentication, password protection, SSL encryption and IP filtering. Whether enterprises use all of these elements depends on their risk analysis. Enterprises have to determine, based on their risk analysis, what their vulnerabilities are, come up with a policy and implement features that align with their network security policy.



How can cyber criminals use IP-enabled cameras?

Here are a few scenarios that are both concerning and damaging:

- Denial of service
- Look at video for proprietary information – see manufacturing processes
- Publish video to embarrass a company
- Take down a video surveillance system or other core systems so ability to operate is damaged

According to Laughton, combating cyber attacks is a process and not a product. Encryption, monitoring devices and updating firmware are all worthwhile tactics. The hardware security industry is publishing hardening guides, offering certification training programs, providing design standards to ensure the device is secure and promoting stronger passwords. As simple as it sounds, even having a strong, unique password is enough to stop the majority of breaches.

As cyber crimes continue to proliferate, educating ourselves on companies, products and processes that provide strong cybersecurity is one of the best ways to stay ahead of the curve. Developing a cybersecurity policy and having our organization's video surveillance network align with it is, according to Axis, perhaps our strongest defense.

Article written by **Vickie Gougoulias**, Editor, DRIE Digest

Thank you to Paul Laughton of Axis for his insights and information on the industry and best practices for cybersecurity. Paul Laughton is the A&E Manager, Canada, Axis Communications, Inc. ■