NETWORK VULNERABILITY & SECURITY DEVICES

How IT & Security Initiatives can work together

OVERVIEW

Network security is one of the most difficult challenges for most companies today. IoT being the dominant means of system connectivity for the past 20+ years has resulted in tasking large companies' network infrastructures and the individuals managing them to balance keeping them up and connected while keeping the network secure. **This is no easy undertaking, to say the least.**

With this in mind, we wanted to share some tips on the correlation between electronic physical security systems and network security.

The link between physical security systems and network security may be closer than you would expect both in helping protect the network and in potentially introducing new vulnerabilities.

COMMITMENT TO EXCELLENCE

At ivelah we take the time to understand your overall business initiatives. This allows us to design & deploy traditional access control & video surveillance technologies in both traditional and non-traditional ways, aligning our solutions directly to your goals.

By delivering consistent, exceptional solutions our goal is to be your go-to trusted security partner at all of your facilities – current and future.

Contact ivelah, the security expert committed to understanding your business.

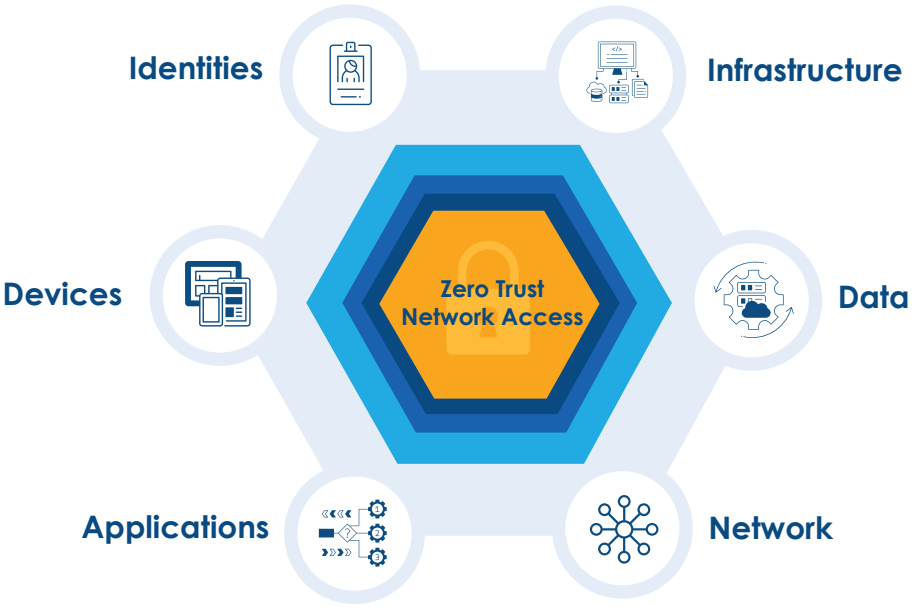
(800) 216-0805

ivelah

PHYSICAL SECURITY'S ENHANCED CYBERSECURITY

First, let's discuss the positive aspects physical security technologies offer to help secure the network. There are admittedly fewer examples of how our physical access control system can help enhance your cybersecurity procedures. However, there are some key features that we believe are important for you to become familiar with. LDAP integration is a feature that most access control systems support, and this is typically used for convenience allowing system administrators to simply log in to the PACS system with the LAN credentials. However, there are some larger enterprise systems that have leveraged this to enhance the end-user's cybersecurity by only allowing a user to log into their PC if they have previously used their access credential to enter the building. Obviously, in today's remote work environment this would not work in every scenario. However, in some higher security instances, this may prove to be an integral part of a cybersecurity program.

The ability to tie the physical access credential to a user account is another method of providing additional security for network log ins. This would require a credential reader on the PC that would need to match either a specific badge credential number or even a biometric template encoded on the credential to enable the user to log into the computer/network.



While the above steps can be implemented to help protect a network environment, unfortunately, there are many more ways for a security system or the components there of to introduce new vulnerabilities to this environment.

Below are some of the best practices that will help avoid these common missteps.

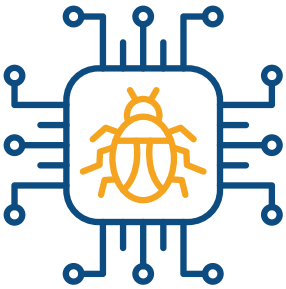
ENCRYPTION

Encryption is not a foreign concept to any legitimate IT manager; however, it is something that a lot of security installers fail to understand or value the importance of. There are numerous instances where we have come across a system that supports basic security encryption, but the encryption was never enabled. Not only that but the default credentials were still in use.

Some manufacturers have endeavored to combat this level of ignorance by forcing installers to enter a new password when installing configuring the devices. But let's not confuse login credentials with encryption. Any reputable security system will support some level of encryption and your higher-end systems will support full FIPS 140 Level 2 compliant encryption.

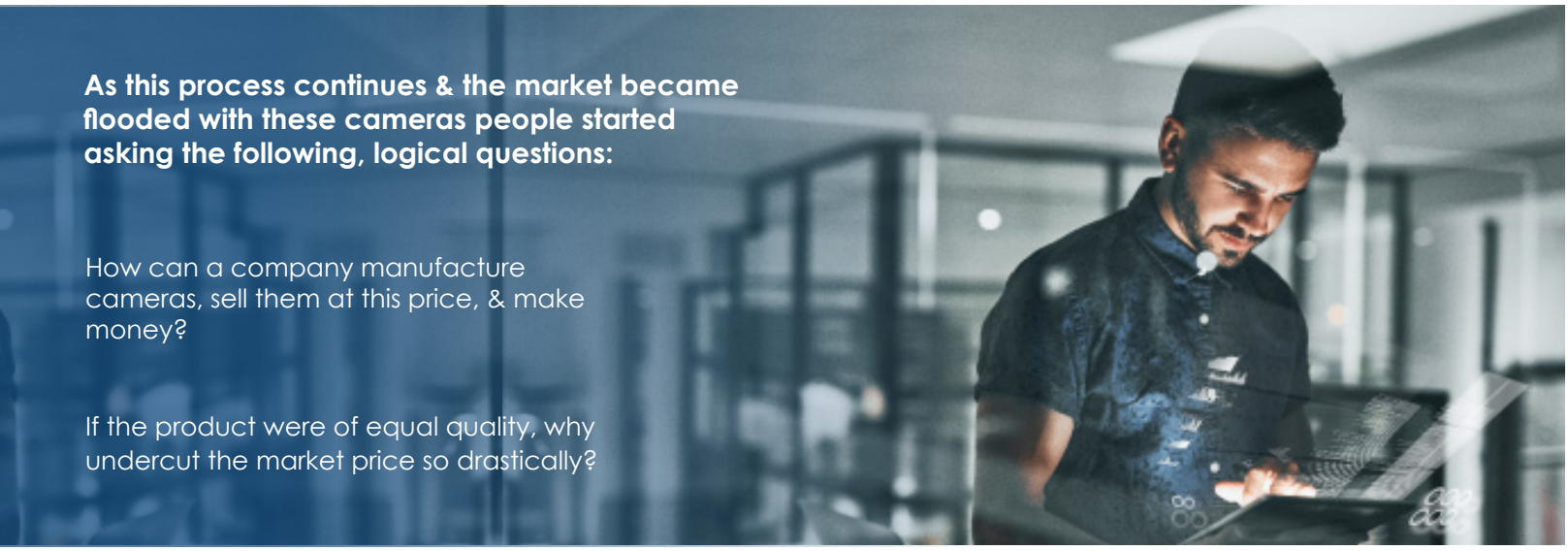
SYSTEM DEVICES

Lastly, but quite possibly most importantly the devices that make up your system could potentially contain a network vulnerability by design.



In the late 2000's or early 2010's, some new manufacturers of camera equipment made their way into the US market. They were viewed as entry-level budget systems at that time by most established security providers and not thought much of it. There was nothing significantly wrong with the cameras, but the user interface was "clunky" and lacked most of the features of larger enterprise systems. However, we started seeing these quickly gain a lot of traction and a larger market share.

This continued to grow at an alarming rate and as people started digging into these devices something shocking emerged. These devices were being sold at such low-price points to the end users that most of the established camera manufactures could not build cameras for the prices that these were being sold at retail prices. Some of them caved and started purchasing cameras from these manufacturers and rebranding them as their own.



As this process continues & the market became flooded with these cameras people started asking the following, logical questions:

How can a company manufacture cameras, sell them at this price, & make money?

If the product were of equal quality, why undercut the market price so drastically?

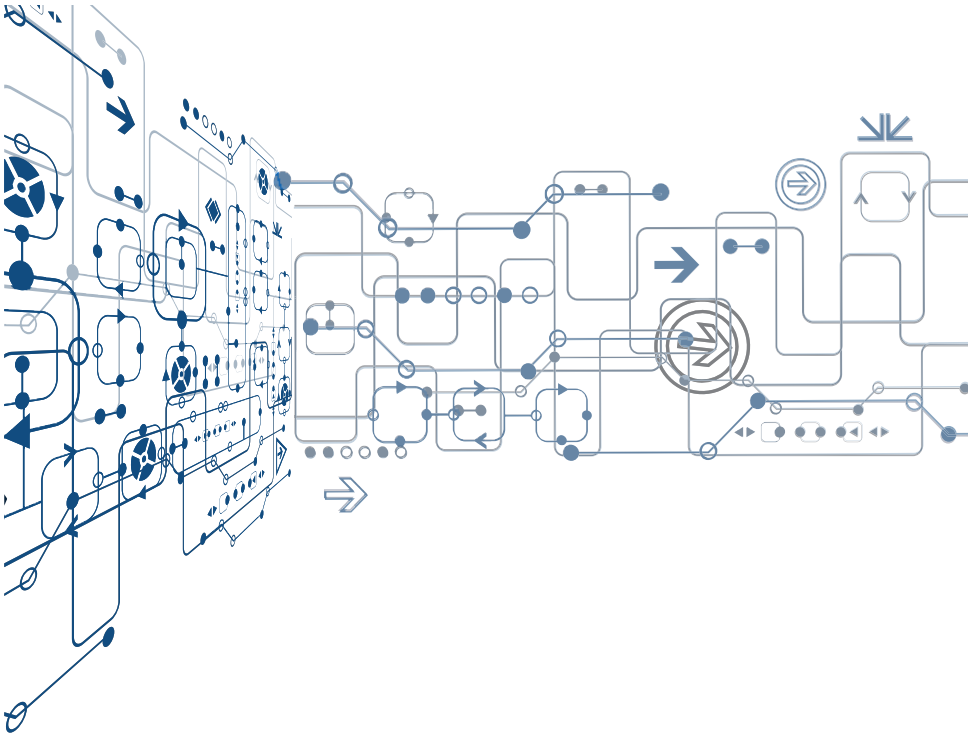
What was found was extremely disturbing.

These manufactures, while selling millions of devices each year were not making money, but they were not adjusting their pricing to compensate. They were continuously being given substantial amounts of money from the Chinese government. These manufacturers were based in China so it would not seem extraordinary for this to happen once, but it didn't happen just once. It happened repeatedly. To the point where both companies are now roughly 50% owned by the Chinese government.

This led to the obvious question of why would any government continuously invest in any company whose business model was to manufacture and sell products at loss? The answer is obviously that there is an outside benefit that the government is receiving from these products being widespread all around the world. This led to some in-depth testing of these devices where it was discovered that not only were there some extreme network vulnerabilities in these cameras with back door login accounts but also numerous reports of "spyware" embedded in them as well as bots that were connecting to "unknown" IP addresses outside the end users' network.

Things started to fall into place as to why it was so important that these companies continue to survive and produce these devices that were being used all over the world including in foreign embassies and even some military installations. It was a brilliant albeit unethical means of data collection. In 2018 congress passed the NDAA which bans the use of all devices from these manufacturers and all other companies that are rebranding these devices as their own.

As the law was announced it was alarming to learn how many different companies had taken to rebranding these cameras and associated equipment (recorders, encoders, etc.). Some companies were particularly surprising as there were established brand that had been manufacturing cameras for years prior to the emergence of these questionable manufacturers. Bottom line, if it had an IP address it was being used to collect data from you network and/or provide access to your video outside of your network without your knowledge or permission.



OUR COMMITMENT

At ivelah we proud to say that we have never sold or installed any of the devices that were associated with these companies rather, we were at the for front of those raising questions over the security and viability of these products.

With the emergence of cloud-based video there is another layer of network security complexity with trusting a third party to safeguard your proprietary data. There have been some significant breaches with some of these cloud providers in recent years and the adage continues to be true that, you can never be too careful as nothing is guaranteed.

We are committed helping end users make better informed decisions when it comes to your security system and as such are committed to provide you with only items that are not only NDAA compliant but also meet your needs form a security perspective, both physical and network, and allow you to safely expand as your business grows.

Next Level Security Starts Here! Inquire at
about.ivelah.com/needs

or call us today at
800.216.0805

A ROBUST PHYSICAL SECURITY SYSTEM & SECURE NETWORK ARE SIMULTANEOUSLY POSSIBLE WITH THE RIGHT SECURITY PARTNER & EQUIPMENT.

If you are consistenly getting (or giving) pushback on access control & video surveillance solutions due to network integrity concerns, let our team come in and help bridge to gap.

At ivelah, we are committed to designing & deploying security strategies that are NDAA-compliant, smart, dependable, & scalable.

SCHEDULE A DISCOVERY CALL WITH OUR TEAM →

ivelah IS COMMITTED TO DOING WHAT'S RIGHT FOR YOU

the right **choice**

Make better-informed security decisions on what equipment to use in your security designs & technologies.

- **Access Control**
- **Video Surveillance**
- **Perimeter Security**
- **Critical Integrations**

the right **process**

Ensure your deployment & ongoing system management is running efficiently & in a cost-effective manor.

- **Technology Choice**
- **Deployment Practices**
- **Reduce Cost of Ownership**
- **Scalable Solutions**

the right **connects**

Maximize the benefits your security system offers while connecting seamlessly to other business critical systems.

- **Human Resources**
- **Finance**
- **Compliance**
- **Information Technology**

the right **support**

Finally a support solution customized around you, your business needs, & budget.

- **Comprehensive Service Plans**
- **Synchronized Warranties**
- **System Longevity Planning**
- **Managed Services**

Next Level Security Starts Here! Inquire at
about.ivelah.com/needs

or call us today at
800.216.0805