IP camera security and access control are included on the Internet of Things. There should be more concern about how the industry has possibly left the customer vulnerable. Today, more and more physical security systems are connected to communication networks for security monitoring, safety, and control. These connections leave systems vulnerable to cyberattack. 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. 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. The common factor in most of data breach class-action lawsuits, as well as investigations by regulatory agencies, is the allegation that the breached companies failed to implement "reasonable security or protections" to prevent the breach. Logically, then, if you implement "reasonable security and protections," you should be able to confidently defend your security practices and Actions.

Cameras and other internet connected devices have been tied to some of the Major Breaches including Ransomware.

Forbes

Fueled IoT Botnet Behind DDoS Attacks on DNS Providers

A massive, distributed denial of service (DDOS) attack on Friday slowed down or knocked offline a whole group of major websites, including Twitter, Spotify, Amazon, Reddit, Yelp, Netflix, and The New York Times

Hacked Cameras, DVRs Powered Today's Massive Internet Outage

October 21, 2016

The New York Times

Millions of Anthem Customers Targeted in Cyberattack

– The New York Times, Feb 2015

Bloomberg

Target's Data Breach: The Largest Retail Hack in U.S. History *– Bloomberg, 2014*

theguardian

Facebook hacked in 'sophisticated attack'

– The Guardian, Feb 2013

Bloomberg

Saudi Arabia Says Aramco Cyberattack Came From Foreign States *– Bloomberg, Dec 2012*

THE WALL STREET JOURNAL.

Fed Acknowledges Cybersecurity Breach

– The Wall Street Journal, Feb 2013

THE WALL STREET JOURNAL.

NASDAQ Confirms Breach in Network

– The Wall Street Journal, Feb 2011

THE HUFFINGTON POST

Apple Hacked: Company Admits Development Website Was Breached

– Huffington Post, July 2013

CNN

South Carolina taxpayer server hacked, 3.6 million Social Security numbers compromised

– CNN, Oct 2012

WIRED

Chinese hacking of US media is 'widespread phenomenon'

– Wired, Feb 2013

AXIS