SECURITY INFOWATCH.COM

# Cyber Threats Take Aim at Mission-Critical Video Data

Hackers can find out if your video surveillance cameras are insecure within five minutes. Here's how to avert their cyberattacks.

Sponsored by

i-PRO

**Video surveillance technology offers several significant benefits. It enhances the safety and security of the people and property associated with your organization, including employees and customers.** In addition, it provides data that can be used to innovate or help identify new business opportunities. It's no surprise then that the global video surveillance camera market is growing fast — from a value of $35 billion in 2022 to an expected $105 billion by 2029, according to recent research from Fortune Business Insights.

The devices that are designed to be used for protection and innovation are also prime targets for cyberattackers. In particular, the Fortune report found that distributed denial-of-service (DDoS) attacks are among the top concerns associated with video surveillance equipment. As with any devices that are deployed on a network, if they are not configured carefully, they can create vulnerabilities in the environment.

For example, attackers hacked into internet-connected cameras to exploit them and turn them into a botnet army, which then delivered a significant DDoS attack. The botnet sent enormous volumes of web traffic to a site run by a security journalist, causing the site to be knocked offline. A Vice article about the attack revealed that hackers found a vulnerability in a particular brand of security cameras connected to the web. This vulnerability allowed them to launch malware on the devices, ultimately carrying out the DDoS attack.

In another instance, Bloomberg reported that bad actors hacked into 150,000 surveillance cameras used by schools, police departments, hospitals, and other organizations. Here again, the attackers gained access via the internet by exploiting a vulnerability in the devices' systems. In turn, this access led them to both live and archived video feeds from within these organizations.


The potential damage from a cyberattack can be devasting — including the theft of sensitive or confidential data, financial loss, regulatory fines, loss of customers, and more. Although organizations have increased their attention to cybersecurity, surveillance — along with other operational technology such as HVAC and lighting systems, as well as cameras — tend to get overlooked. Read on to discover how to overcome these issues and better protect your organization's mission, as well as its mission-critical intellectual property.

## Cyber risks and challenges for cameras

Most businesses and organizations understand that cyber threats have grown in volume and sophistication. However, if you had any doubts, 73% of small businesses in the U.S. — a record high — reported a cyberattack between September 2022 and September 2023, according to the Identity Theft Center. Among those that suffered an attack, 42% lost business revenue.

In addition to higher numbers of cyber events, bad actors are becoming increasingly clever. CSO magazine reports that hackers use artificial intelligence (AI) to accelerate, automate, and scale their attacks. The situation is expected to worsen for two reasons:

1. Companies are increasing their digital transformation efforts, moving data and applications to cloud computing environments and Internet of Things (IoT) devices. In tandem, this gives attackers more potential targets.
2. The use of AI to "supercharge" attacks will intensify as the technology evolves. AI and machine learning tools are becoming more widespread, enabling hackers at all skill levels to automate and deploy cyberattacks.

The accelerated use of video surveillance cameras adds to the potential risks. For example, video file data is increasingly sent to and stored in cloud-based data lakes to conserve on-premises or data center server capacity. Yet, this data is typically mission-critical; it likely includes employee and/or customer information or imagery, as well as sensitive data about proprietary products and services. Any hack into data lakes or cloud-based servers could cause irreparable harm.

Many institutions have taken steps to better secure their applications and networks and are prioritizing strategies such as using zero-trust practices and technologies,


according to Statista. Zero trust works on the premise that identity must be authenticated in order to gain access to applications, machines, networks, etc.

However, zero trust and similar cybersecurity strategies have largely focused on applications, computers, servers, and networks, while the security of video surveillance cameras has lagged. That's a problem because attackers are finding ways to exploit these devices. For example, cameras offer multiple entry points and potential vulnerabilities that, if not properly secured, hackers can use to their advantage:

- Default configurations on cameras and network systems, especially when factory-set passwords are not updated at installation
- Companies not conducting basic cyber hygiene like running patches or updates
- Cameras that use Linux kernel with open ports
- Ethernet cables that are open entry points to networks if not locked down
- Remote-access video management systems (VMS) that don't protect against unauthorized access
- Lack of firewalls to protect network access to devices
- Weak web interfaces or operating systems
- Cameras that don't incorporate data encryption

Hackers' use of AI technologies has included the development of bots that can rapidly scale up a security attack once they find a device vulnerability.

"On average, a bot can scan an IoT device within five minutes of that device being connected to the internet," said Will Knehr, senior manager of information assurance and data privacy at i-PRO Americas Inc. "That happened to a school; they hired an integrator

to carry out an implementation, and they plugged a security device directly into the school's router. Within five minutes, their server was locked out with ransomware."

No organization can afford its mission-critical data to be widely exposed or held for ransom due to an undetected misconfiguration or open access point in a camera.

## Tips to improve video cybersecurity

There are several steps your organization can take toward improving your video surveillance security posture. First, know your responsibility to security. If you're using internal staff to install devices, they should be trained on the risks and potential vulnerabilities to take the proper cybersecurity precautions. Alternatively, if you're using a system integrator, discuss who is responsible for all of those potential entry points that hackers exploit, such as configurations, default settings, access protocols, etc.

Next, modernize your devices. Fortunately, leaders in the video surveillance space are addressing exploitable weaknesses. For example, some firms are introducing surveillance equipment with powerful cybersecurity capabilities already built in.

If budget is an issue, there is no need to rip and replace your entire network of cameras. Start with several devices that will be used for mission-critical surveillance and that are manufactured for proactive cybersecurity. That means they include functionality such as:

- **Authentication:** Go beyond usernames and passwords and seek devices that support features such as digest and host authentication. Furthermore, they should be built to the IEEE 802.1 standard, a port-based standard that provides protected authentication for secure network access.
- **Secure communication certificates that are pre-installed to provide encrypted communications:** For example, a certificate authority such as GlobalSign uses trust-verification protocols to confirm that a machine or device offers secure access and communications. These certifications not only authenticate identity; they also ensure the use of encryption and the integrity of data.
- **Data encryption support:** Cameras should have the capability to ensure that data is encrypted as it is sent across the network. That means devices should support secure protocols such as HTTPS, SSL, SRTP, and RTSP. Also, check to see if the vendor's products can protect data at rest by encrypting the secure digital card (a memory card) in case the camera is lost or stolen.
- **Alteration detection features:** These can determine whether video or audio files have been modified.

Then, at your own pace, continue a slow rollout. As legacy cameras and equipment reach their end of life, replace them with systems with these baked-in cybersecurity capabilities.

Another tip is to seek a VMS that helps teams easily manage distributed devices and uses secure protocols and easy-to-use configuration tools. "The VMS is sometimes overlooked, yet can be just as vulnerable to hacks," Knehr said. "We know of instances where these systems were exploited by hackers to mine for bitcoin."

Finally, and especially if your organization operates within a highly regulated industry, work with vendors that take compliance seriously. For example, manufacturers that support a trusted supply chain offer built-in components that prevent unauthorized access and comply with Federal Information Processing Standards (FIPS). These standards were developed by the National Institute of Standards and Technology and meet the requirements set out by the Federal Information Security Management Act (FISMA), legislation that defines how government information should be protected. In other words, FIPS guidelines satisfy the most stringent needs for securing government data. To that end, look specifically for devices that support FIPS 140-2 Level 3, which is very secure encryption.

Another valuable feature is the Secure Element (SE) chip, which generates and stores cryptographic keys that are used to encrypt data in transit. In addition, some vendors now provide secure boot-up functionality that ensures the firmware has not been modified. It stops the device from launching if malware has been added.

You might ask your vendor if their equipment is production-grade and externally tested. Also, ask whether their hardware is shipped with features designed to show evidence of any physical tampering during its journey to your doorstep. And find out if the devices have baked-in, role-based authentication for the hardware.

## Key video surveillance takeaways

Many factors make the case for cyber-secured cameras,

including the sophisticated threat landscape, the business risks of data breaches, and the multiple vulnerabilities in legacy or improperly configured video surveillance tools. There is significant business value to be gained by investing in devices built to a higher standard with powerful security capabilities to protect your mission-critical data.

To learn more about why the right video surveillance cameras instill confidence with their unique capabilities, visit the i-PRO website.

Learn More