When security cameras become a backdoor: network risks in physical security

Physical security systems used to live on their own wires. Cameras connected to a closed-circuit monitor, and access control meant a card reader wired to a local controller. That world is gone. Today's cameras, door controllers, and intercoms are network devices, and they carry the same vulnerabilities as any other device on an IP network. For organisations that treat them as "just security gear," the surprise can be expensive.

The problem is not that the equipment is badly made. It is that the people who install and manage it often come from a physical security background, not an IT security one. A technician who knows how to run cable and mount a dome camera may not think about firmware updates, default passwords, or VLAN segmentation. The result is a network that has a dozen new doors into it, and nobody is watching them.

How cameras and access control sit on the network

A modern IP camera is a small computer. It runs an operating system, usually a stripped-down Linux, and it serves video over the network using protocols such as RTSP, ONVIF, or HTTP. Some cameras also support audio, motion detection, and on-board storage. An access control controller does similar work: it talks to card readers, manages door strikes, and logs events to a central server over the network.

Both types of device have IP addresses. They communicate with a video management system (VMS) or an access control server, and in many cases they also accept management traffic from a configuration tool. That means they also accept network traffic from anything else on the LAN, unless something stops it.

In a typical small or medium installation, the cameras and door controllers share the same switch as the office workstations and the guest Wi-Fi. The security team may not have asked for that, but the IT team may not have thought to isolate them. The devices sit there, often with their default passwords still active, broadcasting their presence via mDNS or UPnP.

What can go wrong

Four common issues turn a security camera into a network liability.

- **Default or weak credentials.** Many cameras ship with admin / admin or a blank password. Attackers scan for these devices using tools like Shodan and then use them as a foothold inside the network. Once inside, the camera becomes a pivot point to reach other systems.

- **Unpatched firmware.** Camera vendors release firmware updates to fix vulnerabilities, but the update process is often manual. Devices that are not checked for months or years run known exploits. Some older cameras no longer receive updates at all.
- **Unencrypted traffic.** Video streams and access control logs often travel over the network in plain text. An attacker who gains access to the switch can capture credentials, card numbers, or video footage without triggering any alarm.
- **Over-permissive network access.** Many installations put cameras and the VMS on the same flat network segment. A compromised camera can then talk directly to the VMS server, the domain controller, or the file server.

Access control controllers add their own risk. If an attacker can reach the controller, they may be able to unlock doors, suppress alarms, or alter event logs. In a physically secure building, the network side of the door may be the weakest point.

Why standard IT security controls do not always apply

Network security teams are used to managing laptops, servers, and mobile devices. Those devices support endpoint protection agents, can be patched on a schedule, and communicate with known servers. Cameras and door controllers are different. They often run custom firmware that cannot accept a standard antivirus agent. They may stop working if the network team applies a port scan or a vulnerability scanner too aggressively. And they are built for a long service life: a camera installed seven years ago may still be in production, running firmware that was last updated when it was new.

In addition, the people who maintain physical security systems are rarely the same people who manage the network. The security installer has the credentials to the camera web interface. The IT team has the credentials to the switch. Neither group has a complete picture. That split creates gaps. A camera that was configured with a static IP address and a default password years ago may still be on the network, invisible to the IT asset inventory, and unmanaged by the security team.

What good practice looks like

Fixing these problems does not require specialised security hardware, but it does require coordination between the physical security team and the IT network team. A few practical steps reduce the risk considerably.

Segment the network. Cameras and door controllers should sit on their own VLAN, with access to the VMS or access control server only. The monitoring station needs to see the video feed, but nothing else on the network needs to talk to the camera directly. A properly configured firewall rule allows the VMS to initiate connections to the cameras, not the reverse.

Change the defaults. Every device should have a unique, strong password. Some organisations use a password manager or a central credential store for this. Default SNMP community strings and default SSH keys should also be replaced.



Keep firmware current. The person responsible for the physical security system should check for firmware updates at least quarterly. If the vendor has stopped supporting the device, plan for replacement. Running a camera that no longer receives security patches is like running a Windows 7 PC on the same network.

Monitor the devices. Network monitoring tools can detect when a camera starts communicating with an unknown IP address or when its traffic volume changes. Anomaly detection is especially useful because cameras tend to have consistent traffic patterns. A sudden spike in outbound traffic from a camera may indicate that the device is being used for a data exfiltration attempt or as part of a botnet.

Audit access. Who can log in to the camera web interface? Who can modify the access control server configuration? These accounts should be reviewed regularly, and multi-factor authentication should be used wherever the device supports it.

Organisations that lack the in-house expertise to perform this kind of review can benefit from an external perspective. A consultant who understands both physical security systems and network security can identify gaps that neither team sees. That is the kind of work that firms like Hans Study specialise in. Their focus on independent IT and OT infrastructure consulting means they can evaluate a CCTV deployment without being tied to a specific vendor or

installer. They look at the whole picture: how the devices are configured, how they connect, and what access they have to the rest of the network.

The cost of ignoring the problem

A compromised camera does not just leak video. It can be used to launch attacks on other systems, to map the internal network, or to exfiltrate data. In one common attack pattern, an attacker finds a camera with a default password, uses it to discover the VMS server, and then exploits a vulnerability in the VMS to gain administrative access to the server. From there, the attacker can reach the rest of the corporate network. The camera was the door, but the real prize was the data on the server.

Access control systems present a different kind of risk. If an attacker can reach the controller, they may be able to unlock a door remotely, disable a door alarm, or delete event logs. A physical intrusion that is not recorded cannot be investigated. In environments that need to comply with standards such as PCI DSS, HIPAA, or ISO 27001, a breach of the access control system can also mean a compliance failure.

The cost of a breach is far higher than the cost of a proper network assessment and segmentation project. Yet many organisations continue to treat their cameras and door controllers as appliances that do not need the same attention as a server. That assumption is no longer safe.

As the line between physical and network security blurs, the teams that manage them must blur too. The security installer and the network administrator need to talk regularly. The physical security budget should include network equipment, software, and consulting hours, not just cameras and cabling. And the organisation should treat every network-connected device as a potential attack surface, whether it is a laptop, a printer, or a door controller.

Independent consultants such as **Hans Study** can help bridge that gap. They offer the kind of cross-domain knowledge that is hard to build inside a single department. By reviewing the entire infrastructure, from the camera firmware to the firewall rules, they help organisations close the backdoors that physical security systems can create. For any business that has invested in CCTV and access control, that review is worth making a priority.

Hans Study on social media Twitter LinkedIn Instagram YouTube