Keep Physical Security from Opening Cybersecurity Risk

Best practices reduce the cyber vulnerabilities of cameras and access control systems

Nearly every day brings the news of another data breach or ransomware incident in the public sector. Large or small, any government organization, K-12 school district or higher education institution is vulnerable to a disruptive and costly cyber attack.

How are these attacks gaining entry? Sometimes an employee clicks on a link in a phishing email. Sometimes a default application password was never changed. But sometimes it is through a forgotten, network-connected security camera in the parking lot.

Today it's essential to recognize the cybersecurity risks that can exist in physical security devices such as cameras, door controllers and their monitoring systems. That risk has increased with greater use of these devices during the COVID-19 pandemic.

"Fewer people working in buildings means you need more technology to maintain physical protections," says Morgan Wright, a Center for Digital Government (CDG) senior fellow. "Yet when it comes to protecting those physical security devices, too often the worry is about damage or theft, not that they can be used as an entry point for ransomware."

> "Fewer people working in buildings means you need more technology to maintain physical protections. Yet when it comes to protecting those physical security devices, too often the worry is about damage or theft, not that they can be used as an entry point for ransomware.
>
> *Morgan Wright, Senior Fellow, Center for Digital Government*

ADOBESTOCK

The Growing Risk of Cyber Threats

Data breaches and ransomware attacks can have a significant impact on government operations and services. Recent statistics about breaches and threats indicate why cybersecurity is a top priority for government IT leaders.

For data breaches, the Identity Theft Resource Center reports that as of September 30, 2021, the year-to-date total number of data compromises related to cyber attacks was 27 percent higher than in 2020.[1]

For ransomware, in 2020 the FBI received nearly 2,500 complaints across all sectors.[2] Verizon identified ransomware attacks as a common motivator for theft or discovery of user credentials by hackers.[3]

Large governments and higher education institutions are not the only targets. One study found K-12 schools experienced more than 400 cyber incidents in 2020, an increase of 18 percent from 2019.[4]

An overlooked avenue for cyber attack

A lingering but erroneous view is that only limited threats can be made through a physical security device. For example, recognized threats often include the ability to remotely stop the video feed from a camera, open or lock a door, or disrupt critical building systems.

Yet most cyber attacks are not intended to compromise the physical safety of people or property. Instead, these attacks target applications, files and data managed by IT. An attack that originates in a camera can find its way through the network to block access to critical applications; lock and hold files for ransom; and steal personal data of employees, students, program clients and residents.

For example, the Mirai botnet continues to disrupt systems and networks by attacking them with internet-connected devices, including cameras. To find vulnerable devices, the botnet typically relies on simply trying to log in with factory-default usernames and passwords.

In 2021, security researchers discovered that a Mirai-based botnet, called Moobot, uses another technique to infect video surveillance devices made by the Chinese manufacturer Hikvision, which are embedded in many original equipment manufacturer (OEM) solutions. This technique injects malicious code into the device, then checks the network to find additional devices to infect. Although a software patch is available to close this risk, IT teams may not know which installed cameras should receive it.

An analysis by Genetec found that too many security cameras offered this opening for attack. According to its study, nearly seven in 10 cameras had out-of-date firmware.[5]

"Security cameras and access control systems need to be considered critical network devices," Wright says. "They need to receive a high level of protection and monitoring for operations and cybersecurity."

This view is gaining acceptance within IT organizations as two issues become clearer and more compelling. First is the increasing crossover of network attacks from internet-connected security cameras and door controllers. These devices often give cyber attackers easy network entry, and IT has limited visibility until after the fact. Second, the rising volume and disruption of cyber attacks inherently increases the risk level of any network-connected device that is not adequately secured.

Cybersecurity risks in physical security systems

Many public sector facilities continue to use older model security cameras and door controllers, replacing them only when necessary or when their capital cost has been fully amortized.

However, older devices, especially cameras, often present a significant

cyber risk due to their limited security capabilities. This risk may be why many governments plan to upgrade their fixed surveillance systems in the near term. According to Center for Digital Government research, 55 percent of surveyed cities, 34 percent of counties and 43 percent of states are planning upgrades to surveillance systems, especially those used for public safety.

Today, hackers know that certain cameras are easy to take over and use as an entry point to the connected network. Several factors make cameras easy to breach.

Hackers know that certain cameras are easy to take over and use as an entry point to the connected network.

An outdated network design. In the past, the physical security industry did not need to maintain a strong focus on cybersecurity, creating a lag in feature and technology integration. These devices were typically connected in a closed network design, which does not reflect the different and higher security demands of internet, Wi-Fi or cellular connections.

Inadequate maintenance. Physical security management does not always incorporate common procedures and best practices for cybersecurity, such as frequent changes to passwords. Many physical security devices still in use are aging and no longer receive updated firmware from the manufacturer.

Knowledge gap. Employees who installed and managed physical security systems may have retired or left the agency, leaving a gap in knowledge about devices, configurations and maintenance.

Vulnerable devices. Many cameras made by certain Chinese manufacturers have been identified as presenting a high level of cyber risk. The U.S. government has banned these cameras for federal agencies, based on cybersecurity concerns and as a sanction against use of surveillance by the Chinese government to repress minority groups and commit human rights violations.[6]

With the 2021 passage of the Secure Equipment Act, the FCC must issue rules that revoke authorization for equipment from several Chinese manufacturers. Although these rules initially cover future equipment purchases, the FCC may also revoke use authorization, which would require replacement of installed cameras and systems from these companies. This federal legislation and potential rulemaking raises concerns about the presence of Chinese-manufactured cameras in all public and private networks.

At-risk cameras may be particularly hard to detect if they were built into private-label systems sold by video surveillance solution providers.

The following steps can help identify devices of concern:

- ✓ Create an up-to-date inventory of all cameras and control systems connected to the network, including via Wi-Fi or cellular connection.
- ✓ Verify the inventory with in-person, on-premises checks to detect devices that may have been forgotten.
- ✓ Maintain detailed information about each physical security device, e.g., age, manufacturer and firmware version.
- ✓ Identify the types of encryption and cybersecurity capabilities supported on each device or firmware version.

Cybersecurity receives priority attention

Center for Digital Government research indicates state and local leaders continue to prioritize cybersecurity improvements.[7] The changes brought by the COVID-19 pandemic have reinforced that view; nearly 70 percent of IT practitioners say cybersecurity has become a more important priority in their organizations.

IT practitioners and agency senior managers agree on current challenges facing their cybersecurity efforts. Nearly 60 percent say the biggest challenge comes from threats that evolve faster than their organizations are equipped to handle.

Nearly 70% of IT practitioners say cybersecurity has become a more important priority in their organizations.

Nearly 60% say the biggest challenge comes from threats that evolve faster than their organizations are equipped to handle.

- ☑ Verify the source and legitimacy of each software update before installation; an update may be used to install malicious code.
- ☑ Check device inventory against published information about manufacturers and models that have identified security risks. Determine if these devices should be prioritized for early replacement.

Another, albeit bigger step to take: Bring physical security and cybersecurity together into a single team with integrated operations.

Joining physical security and cybersecurity

In many organizations, a long-held perspective is that IT and physical security are separate realms, and their work and concerns do not intersect. However, this perspective needs to change in light of the growing cyber risk that physical security technologies can present.

The change comes from a new view of how to best structure security management across all systems and devices. It begins when the IT and physical security teams join into a single organization that is focused on a comprehensive security program. This program is based on a common understanding of risk, responsibilities, strategies and practices.

> "Physical security needs to be integrated into the network security team, not viewed as an ancillary function."
>
> *Morgan Wright, Senior Fellow, Center for Digital Government*

An integrated team is recommended by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Although a federal agency, CISA offers guidance that is relevant to all levels of government. In recommending integration of physical security and cybersecurity, CISA notes several benefits can be gained.[8] In particular, a holistic view of security threats across the organization leads to improved information sharing and preparation for threat response. Unified policies and shared practices give the organization greater flexibility and resilience for security management.

CISA also recommends specific steps to ease the integration of these teams, including:

- ☑ Encourage information sharing and collaboration on shared goals and practices.
- ☑ Formalize roles and responsibilities for the combined team.
- ☑ Identify linked assets and assess the risk level created by that linkage.
- ☑ Conduct a vulnerability assessment to identify gaps that can be closed through convergence of physical and cybersecurity.
- ☑ Create a new baseline to guide security operations and incident management moving forward.
- ☑ Develop and implement risk-driven security policies and best practices.

Wright agrees with the CISA recommendation for team convergence, noting, "Physical security needs to be

integrated into the network security team, not viewed as an ancillary function."

Improving the cybersecurity of physical security

An integrated security team can review needed cybersecurity improvements across physical security devices and systems. This review should include several key areas of focus.

Improve security monitoring. Ensure all network-connected physical security devices are monitored and managed by IT tools for network and security management. Also check for features in the video management system (VMS) and access control system (ACS) that provide alerts or data for use by IT's network and security monitoring tools.

Strengthen protection measures. Look for ways to improve existing configurations and management practices for physical security devices, including:

- ☑ Using secure protocols to connect the device to the agency network
- ☑ Disabling access methods that support a low level of security protection
- ☑ Verifying configurations of security features and alerts
- ☑ Replacing defaults with new passwords that are changed on a regular and verified schedule

Implement encryption. End-to-end encryption offers the most security to protect video streams and data as they travel from the physical security device to a management system for viewing. Also ensure encryption protects these files and data while in storage.

Enhance access defenses. Strengthen the security of user and device access with a multilayer strategy that includes multifactor access authentication and defined user authorizations.

Improve update management. One management function that can be overlooked when teams are separate is installation of software updates and patches. When the teams are joined, define who has responsibility for maintaining awareness of available updates. Then, define who has responsibility for vetting, deploying and documenting updates on all eligible devices and systems.

Planning a replacement program

After an assessment of current physical security elements, it may be clear that some devices — and perhaps the VMS or ACS — present a high cyber risk and should be replaced. Replacement priorities can also be determined by location, use case, device type or age.

Security improvement checklist

Current posture assessment

- ✓ Create an up-to-date inventory of all network-connected cameras, door controllers and associated management systems.
- ✓ Perform a thorough vulnerability assessment of all connected physical security devices to identify models and manufacturers of concern.
- ✓ Consolidate and maintain detailed information about each physical security device, including connectivity, firmware version and configuration.
- ✓ Improve the network design as needed to segment older devices and reduce potential for crossover attack.
- ✓ Identify all users who have knowledge of physical security devices and systems and document that knowledge for broader use and retention.

Physical security and cybersecurity unification

- ✓ Begin discussions about combining the physical security and cybersecurity teams; formalize roles and responsibilities.
- ✓ Monitor and share intelligence about current cyber threats and trends across the teams and encourage collaboration on preventative actions and response capabilities.
- ✓ Develop common policies and practices for security operations and incident management.

Improvements to make now

- ✓ Determine if installed physical security devices have the latest version of firmware and other software recommended by the manufacturer.
- ✓ Confirm that software for the VMS and ACS is up to date on the physical security devices as well as servers used for storing data and hosting monitoring consoles.
- ✓ Change any default passwords in use and establish a policy and process to require frequent password changes.

Planning for device and system replacement

- ✓ Identify any devices that need replacement because of age or potential security risk.
- ✓ Develop a plan that will modernize security features and management on a unified platform.
- ✓ Evaluate the compliance standards of all vendors in the proposed solution's supply chain.

"Improving protections for physical security is a critical IT modernization project because these elements are being plugged into the internet when they weren't designed for it," says Wright.

When ready to issue an RFP, consider incorporating requirements that will support modernization for both physical security and cybersecurity.

These include:

- ☑ Unification of cybersecurity and physical security devices and software on a single platform, with centralized management views and tools. This should be an open architecture that will support a cloud-based or hybrid deployment of security solutions, as well as flexible integration options for future devices and management systems.
- ☑ Cybersecurity features, such as data encryption, that are built into the device firmware and management software.
- ☑ Compliance with security standards and audits for all suppliers and system integrators involved in providing the solution (i.e., the supply chain). Include a list of prohibited vendors for equipment and software components.
- ☑ Vendor capabilities to support a solution life cycle of up to 10 years, including ongoing availability of updates for device firmware and management system software.

Federal funding may be available to help with the costs of replacement systems. The 2021 Infrastructure Investment and Jobs Act includes $1 billion in funds, managed by the Department of Homeland Security, that are designated to help state and local governments modernize their cybersecurity systems.

Improving security across the board

"The pandemic showed there are gaps in how we deploy protection technologies, and we need to become more intelligent about how we control access to sensitive or restricted areas," Wright says. "But we also know there are ways to change these deployments to make them more effective for both physical and cybersecurity."

By understanding that physical and cyber domains are closely tied, governments can implement the new technologies, staff roles and practices that will strengthen security overall.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Genetec.

Endnotes
1. https://www.idtheftcenter.org/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/
2. FBI 2020 Internet Crime Report
3. Verizon 2021 Data Breach Investigations Report
4. EdTech Strategies, K-12 Cybersecurity Resource Center and K-12 Security Information Exchange: State of K-12 Cybersecurity: 2020 Year in Review Report
5. Genetec 2019 analysis
6. https://techcrunch.com/2021/05/24/united-states-towns-hikvision-dahua-surveillance/
7. CDG surveys conducted in 2020 and 2021
8. CISA Cybersecurity and Physical Security Convergence

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: Genetec™

Genetec Inc. is an innovative technology company with a broad solutions portfolio that encompasses security, intelligence, and operations. The company's flagship product, Security Center, is an open-architecture platform that unifies IP-based video surveillance, access control, automatic license plate recognition (ALPR), communications, and analytics. Genetec also develops cloud-based solutions and services designed to improve security, and contribute new levels of operational intelligence for governments, enterprises, transport, and the communities in which we live. Founded in 1997, and headquartered in Montréal, Canada, Genetec serves its global customers via an extensive network of resellers, integrators, certified channel partners, and consultants in over 159 countries. **www.genetec.com/**