Homeland Security
Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)
National Protection and Programs Directorate
Office of Infrastructure Protection
Infrastructure Protection Note

IP Note: Mitigating Cyber-Physical Impacts at Commercial Facilities

June 24, 2013, 1300 EDT

SCOPE

The Department of Homeland Security's National Protection and Programs Directorate Office of Infrastructure Protection Homeland Infrastructure Threat and Risk Analysis Center (DHS/NPPD/IP/HITRAC) produces IP Notes to address issues impacting the infrastructure protection community. This IP Note presents cyber-physical analysis—examining potential physical consequences stemming from exploited control system vulnerabilities—and lessons learned drawn from vulnerability and consequence assessments at select commercial facilities. This IP Note does not address specific threat actors or extensive details of the attack techniques they could employ against such vulnerabilities. Rather, it relays key findings and protective measures to inform the Commercial Facilities Sector broadly. HITRAC developed this IP Note with contributions from the NPPD/IP/Strategic Outreach and Partnership Division and the NPPD Office of Cyber Security & Communications Industrial Control Systems Cyber Emergency Response Team (NPPD/CS&C/ICS-CERT).

KEY FINDINGS

- **A successful attack on a facility's network could allow threat actors to gain control of the facility's building management control systems and manipulate settings through unauthorized changes—e.g., to a facility's temperature, lighting, and access control.**
- **Remote access via Internet connectivity, compromised user credentials, physical access to network assets, and the openness of building automation protocols can all pose risks to commercial facilities that employ control systems.**
- **Information on control systems protocols and component interconnectivity is readily available on the Internet, which presents opportunities for threat actors to gain and leverage such knowledge to exploit facilities' control systems.**

OVERVIEW

The NPPD Integrated Analysis Task Force (IATF) initiated a proof-of-concept effort in 2012 to merge and leverage capabilities from across NPPD and integrate physical and cyber infrastructure expertise. The IATF coordinated the effort with Protective Security Advisors (PSAs) from the IP/Protective Security Coordination Division alongside State and local partners. In addition, the IATF applied resources from HITRAC and ICS-CERT—specifically, their Cyber

Security Evaluation Tool (CSET), Cyber Resilience Review, and subject matter expertise—to conduct vulnerability and consequence assessments of select commercial facilities.

The CSET provided a baseline assessment of the facilities' information and operational systems, policies, and procedures. To integrate wholly NPPD physical and cyber infrastructure expertise, the IATF supplemented the CSET baseline with analysis focused on mapping potential consequences to identified system vulnerabilities. For example, one facility had physical heating, ventilation, and air conditioning (HVAC) controllers in meeting spaces. The control units had Ethernet ports to facilitate technical adjustments through the HVAC network.

The IATF assessed such physical and cyber vulnerabilities individually and in combination to identify how they posed risk to the facilities. In its assessments, the IATF determined threat actors that successfully exploit such vulnerabilities could gain control of a facility's control systems and manipulate settings through unauthorized changes—e.g., remote attacks that exploit Internet-facing systems' vulnerabilities, or a threat actor with physical access connecting a laptop to the HVAC network via the Ethernet port to manipulate the facility's temperature. Such changes could lead to equipment damage due to improper room temperature or command input. In addition, they could create uncertainty around facility operations that decrease customer confidence and future revenue opportunities, cause disruption, lead to physical discomfort, or prompt the need for evacuations.

In addition to HVAC controls, some commercial facilities use automated control systems to manage other aspects of building management, such as lighting, public address systems, elevators, fire suppression, and other systems—all of which may be subject to cyber intrusions that create unauthorized changes to system configurations.

Collectively, these commercial facility vulnerabilities mirror what ICS-CERT has observed across numerous ICS installations: an overall lack of defense. Past DHS site assessments have found that the most common configuration problem was credential management (i.e., weak passwords and insufficiently protected credentials), followed by weak or non-existent firewall rules and network design weaknesses.[1] Protective measures can address such problems, however, and broaden the breadth and depth of a facility's cybersecurity posture.

PROTECTIVE MEASURES

Commercial facilities for which the IATF conducted assessments did not have mandated requirements to apply specific cybersecurity standards—a position that other commercial facilities may share. In lieu of such standards, the IATF assessed the facilities' control systems and information technology network security practices against recognized industry standards from the National Institute of Standards and Technology (NIST).[2]

In addition, ICS-CERT provides substantial publicly available information regarding best practices that facilities can pursue. Such practices are recommendations, not prescriptions, for critical infrastructure stakeholders to enhance security and risk management decisionmaking.

[1] DHS Control Systems Security Program, "Common Cybersecurity Vulnerabilities in Industrial Control Systems," May 2011, vi.

[2] Facilities that are not required to follow specific cybersecurity standards can consider recognized industry standards—e.g., from NIST—to establish network security practices and improve their cyber hygiene. The IATF applied NIST Special Publication 800.82, which is tailored for control systems.

Commercial facilities can consider ICS-CERT security recommendations[3] that advise owners and operators to:

- Redesign network layouts to take full advantage of firewalls, virtual private networks, etc.;
- Implement a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer;
- Restrict physical access to the ICS network and devices;
- Expeditiously deploy security patches after testing all patches under field conditions (on a test system if possible) before installation on the ICS;
- Work with vendors to test and apply patches for all operating systems and software on the ICS networks;
- Customize intrusion detection systems for the ICS hosts and network;
- Restrict ICS user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of lease privilege); and
- Develop a password management plan to enforce strong passwords with minimum length, mixed character sets, expiration, no password reuse, etc., and change all default passwords.

In addition to considering these ICS-CERT recommendations, commercial facilities can seek to limit publicly available information about their systems to only the information required by law. Unnecessarily public information presents opportunities for threat actors to gain and leverage the knowledge needed to exploit systems. Although limiting information about open-source protocols—such as the building automation and control networks protocol (or BACnet)—is not possible, purposeful limitations about assets, network configurations, and the use of communications protocols like BACnet can complement other protective measures in place.

Commercial facilities may also consider temporarily limiting or disconnecting Internet-facing connections during critical operations (i.e. large-scale events) and using alternative control measures to reduce the possibility of system compromise. For example, the select commercial facilities that IATF assessed decided to implement a standard operating procedure to temporarily disable their remote network connections to preclude possible cyber attacks—preceding and during large-scale events with substantial media attention.

RESOURCES

NPPD/CS&C manages and operates ICS-CERT, which provides focused operational capabilities for defense of control system environments against emerging cyber threats. The ICS-CERT Web site (http://ics-cert.us-cert.gov/ics-cert/) offers recommended practices and numerous information products that address issues related to ICS, including products focused on common cybersecurity vulnerabilities in ICS, configuring and managing remote access for ICS, and practices to improve cybersecurity of supervisory control and data acquisition networks.

[3] DHS, "Common Cybersecurity Vulnerabilities in Industrial Control Systems," 57.

ICS-CERT encourages reporting of suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems, and they can be contacted at (877) 776-7585 and ics-cert@hq.dhs.gov. ICS-CERT can assist asset owners and operators in restoring service.

Another resource is the Industrial Control Systems Joint Working Group (ICSJWG), a collaborative and coordinating body that operates under Critical Infrastructure Partnership Advisory Council requirements. The goal of the ICSJWG is to continue and enhance the collaborative efforts of the industrial control systems stakeholder community in securing critical infrastructure. To participate, email icsjwg@hq.dhs.gov. To learn more about cybersecurity efforts in the Commercial Facilities Sector, including the Commercial Facilities Cyber Security Work Group, please contact cfsteam@hq.dhs.gov.

Finally, the Homeland Security Information Network (HSIN) Web site (www.hsin.gov) has more information related to cyber protection, indicators, and vulnerabilities. HSIN is the primary DHS information sharing platform. Partners can email CIKRISEAccess@dhs.gov to gain access to HSIN, and can contact a local PSA at FOBAnalysts@dhs.gov for additional resources.

The Homeland Infrastructure Threat and Risk Analysis Center produces Infrastructure Protection Notes, which scope the infrastructure protection community's risk environment from terrorist attacks, natural hazards, and other events being reviewed and highlight the analytic capabilities required to produce infrastructure protection related risk analytic products. The information is provided to support the activities of the Office of Infrastructure Protection and to inform the strategies and capabilities of Federal, State, local, and private sector partners. For more information, contact risk@hq.dhs.gov. For more information about the Office of Infrastructure Protection, visit www.dhs.gov/criticalinfrastructure.