CYBERSECURITY THREATS TO BUILDING MANAGEMENT SYSTEMS

Are You at Risk?

OVERVIEW

Today's smart buildings contain a myriad of Control System (CS) components. From fire safety systems to detect smoke and fire and alert both building occupants and the fire department to simple heating, ventilation, and air conditioning (HVAC) and lighting control systems that turn lights on or off at predetermined times, automated building management systems keep occupants safe and comfortable while saving thousands on electrical energy and maintenance. There is a downside, however. Many of these systems are connected directly to the Internet without any type of cybersecurity in place, providing easy access for attackers. Parsons has proven solutions for protecting these systems and can help protect your buildings from Internet threats.

WHAT ARE THE CONSEQUENCES?

- **Physical damage to equipment or infrastructure**
- **Theft of high value property**
- **Loss of revenue**
- **Bodily injury or death**
- **HVAC shutdown/manipulation**
- **Door locks disabled**
- **Disabling of physical intrusion detection systems**
- **Loss of building lighting**
- **Data center thermal overloads**
- **Significant loss of revenue**
- **Loss of customer confidence/contracts**
- **Higher insurance premiums**

WHAT SHOULD BE CONSIDERED?

WHAT IS THE BUILDING INDUSTRY DOING TO ENHANCE CYBERSECURITY?

- **The National Institute of Building Sciences (NIBS) conducts several cybersecurity workshops covering cybersecurity basics, basic and advanced securing building control systems, as well as building resilience workshops annually.**

FEDERAL DIRECTIVES

- **Executive Order 13636:** Improving Critical Infrastructure Cybersecurity directs NIST to develop a cybersecurity framework to reduce cyber risks
- **Presidential Policy Directive 21** directs federal agencies to assist critical infrastructure owners to improve cybersecurity and resilience
- **Presidential Policy Directive 8** strengthens US security and resilience through systematic preparation against threats that pose the greatest risk to the nation
- **National Infrastructure Protection Plan (NIPP)** outlines how government and private sector work together to manage risks and achieve security and resilience
- **HSPD-7** establishes a national policy for federal agencies to identify and prioritize critical infrastructures and protect them from terrorist attacks

CYBERSECURITY GUIDANCE

- **NIST Cybersecurity Framework**
- **NIST 800-37**
- **NIST 800-82**
- **IEC 62443**

PARSONS

IT COULD HAPPEN TO YOU

2002 A programmable logic controller (PLC) used to control a reverse-osmosis water purification system at a semiconductor manufacturer was shut down when an unauthorized user gained access through the Internet.

2003 An SQL-Slammer worm infected a corporate network and process network, shutting down the distributed control system and resulting in the loss of historical data.

2010 Stuxnet took control of Windows PLCs and used them to destroy centrifuges at Iran's Natanz Nuclear Facility. This was the first known cyber attack meant to destroy physical assets.

2013 In one of the largest data breaches reported, hackers stole the credit and debit card records of 40 million+ Target customers, as well as personal information such as email and mailing addresses from some 70 million people. Attackers first gained control of the HVAC system then pivoted to the point-of-sale system.

2014 Yahoo, the world's second largest e-mail service provider, was the victim of a major coordinated attack, in which both usernames and passwords were compromised; the information was stolen from an unsecured, third-party database.

WHY PARSONS FOR CYBERSECURITY?

Parsons has worked behind the scenes for 30+ years to deliver cybersecurity services that have protected our nation's most sensitive information and critical infrastructure to federal customers. This experience is enhanced by 70+ years of experience designing, building, and managing these assets around the globe. Parsons has combined its in-depth knowledge of cybersecurity with its expertise in the sustainment of critical assets to offer PARSecure®, a secure suite of services that includes both cyber and physical security. This offering allows us to leverage our experience and become a trusted cybersecurity partner for customers in federal, state, and local government, and the commercial marketplace. Using PARSecure® and our team of cybersecurity experts, we can ensure that cutting-edge cybersecurity people, processes, and technologies are in place—addressing the full spectrum of risks to your business and protecting your most valuable assets.

Setting us apart is our state-of-the-art Cyber Solutions Center, located in Centreville, VA. This hands-on laboratory enables the Parsons team to demonstrate and analyze operational networks, supervisory control and data acquisition (SCADA) systems, and industrial control systems (ICS) that control all critical infrastructure, building systems, manufacturing systems, medical treatment facilities, water and wastewater, transportation, and more. We can then custom design, test, and implement the technical options needed to protect the security of client networks and infrastructure, in addition to providing training to those entrusted to maintain the security of these systems.

Parsons is a leader in technical solutions, continuity of operations, critical infrastructure, and classified facility protection. Together, we create a safer, more secure world.

OUR CAPABILITIES

ASSESSMENTS
Vulnerability Assessments
Certification and Accreditation
Penetration Testing

ANALYSIS & PLANNING
Security Assessments
Analysis
Remediation Plan Development

DESIGN
Plans/Policies Development
Network Security/
Security Monitoring Design

IMPLEMENTATION
Software Development
Software Tool Procurement
Security Solution
Development/Integration/Testing

OPERATIONS/MAINTENANCE
Operational Assurance
Incident Response Management
Continuous Security Improvement
External Stakeholder Coordination

CONTACTS

Jay Williams
ICS/SCADA Cybersecurity
Business Development Director
(315) 706-7154
jay.williams@parsons.com

Bob Talbot
ICS/SCADA Security Solutions Manager
(703) 679-9187
robert.talbot@parsons.com

Design–Build–Protect

For more information or to request a demo, please go to:

www.parsons.com/cyber

EXIM APPROVED Parsons #162 8 Dec 15