

## New Workshop Looks at What to Do When Building Control Systems Get Hacked

A new workshop, sponsored by the National Institute of Building Sciences, answers the question of what to do when building control systems have been hacked or taken over by ransomware. Intended for building owners, facility managers, engineering, physical security, information assurance and other professionals involved with the design, deployment and operation of building control systems, the “**Your Building Control Systems Have Been Hacked, Now What? Workshop**,” to be held **Tuesday, October 4, from 8:00 am to 5:00 pm**, in Arlington, Virginia, will provide a combination of classroom learning modules and hands-on laboratory exercises to help attendees learn how to detect, contain, eradicate and recover from a cyber event.

The workshop, taught by Michael Chipley, PhD, GICSP, PMP, LEED AP; Daryl Haegley, OCP, CCO; and Eric Nickel RCDD, CEH, CEP, is built around the Advanced Control System Tactics, Techniques and Procedures (TTPs) developed by the U.S. Cyber Command (USCYBERCOM), which provide detailed step-by-step guidance to respond to a cyber attack.

During the one-day workshop, attendees will use the Cyber Security Evaluation Tool (CSET), GrassMarlin, Glasswire and Belarc tools to create a fully mission-capable (FMC) baseline, which consists of documentation that characterizes the control system, such as the topology diagram, enclave entry points, user accounts, server/workstation documentation and network documentation.

Next, attendees will conduct footprinting and learn how to find building control systems exposed on the internet using Google Hacking, Shodan and WhiteScope discovery tools. Attendees will then build a Recovery Jump-Kit that contains the tools the control systems team and information technology (IT) team will need to restore a system to its last FMC state during mitigation and recovery. Using the Recovery Jump-Kit, attendees will then find and eradicate the malware using tools such as MalwareBytes and the Microsoft Internals suite, and learn how to perform data collection for forensics, which involves the acquisition of volatile and non-volatile data from a host, a network device and control system field controllers. Lastly, attendees will evaluate the cyber severity of the incident and prepare an incident report.

Attendees will need a laptop with administrative privileges to load software. Course content, tools and lab exercises will be provided on a CD at the beginning of the workshop.

Registration for the “**Your Building Control Systems Have Been Hacked, Now What? Workshop**” is \$600 per person. Because the Institute is offering this course for the first time, participants who attend the “trial run” of the workshop will receive a discounted rate of \$300. Space is limited to 20 students. [View the workshop schedule.](#) [Register now](#)

### About the National Institute of Building Sciences

The [National Institute of Building Sciences](#), authorized by public law 93-383 in 1974, is a nonprofit, nongovernmental organization that brings together representatives of government, the professions, industry, labor and consumer interests to identify and resolve building process and facility performance problems. The Institute serves as an authoritative source of advice for both the private and public sectors with respect to the use of building science and technology.