National Institute of BUILDING SCIENCES™

Webinar: Cyber-Physical Impact Modeling

November 28, 2023 | Session Overview

Panel

Hon. Lucian Niemeyer, CEO & Chairman of Board of Directors, Building Cyber Security

EJ Von Schaumburg, Co-CEO, Red Bison

Fred Gordy, Director, OT Risk Assessments, Michael Baker International

Andrew Balster, President, Physical Space Practice, Geniant

Moderator

Ari Reubin, Senior Vice President, KMC Consulting, a division of KMC Controls, Inc.

Cyber-Physical Impact Modeling Webinar Overview

The risk of cyber-physical threats to commercial and institutional building sites cannot be overstated.

Sites include core infrastructure such as electric utilities and water treatment facilities; hospitals; nursing homes; K-12 schools and colleges; airports; hotels and casinos; stadiums; commercial office buildings; data centers; warehouses; factories; courts and prisons; and government buildings. Protecting these sites from bad actions or errors from employees can minimize outside takeover of operational systems, risk to loss of life, personal injury, and harm to the environment.

On November 28, 2023, the National Institute of Building Sciences (NIBS) hosted a webinar on cyber-physical impact modeling (CIM), per the framework developed by non-profit entity Building Cyber Security, and applied to commercial and government facilities.

- BCS is dedicated to advancing cyber-physical security to enhance the protection of data, information, systems, and people part of the commercial real estate ecosystem. It assigns a risk assessment score at each site using the CIM method.
- This approach serves to incentivize comprehensive enhancement of technology, processes, and training to respond to a rapidly evolving cyber-physical threat.
- The strategic intent is to achieve the highest short- and long-term reduction of risk and cost that may be triggered by a disruption or adverse alteration to building operations.

The panel included the Honorable Lucian Niemeyer, CEO & Chairman of Board of Directors, Building Cyber Security; EJ Von Schaumburg, Co-CEO, Red Bison; Fred Gordy, Director, OT Risk Assessments, Michael Baker International; Hon. Lucian Niemeyer, CEO & Chairman of Board of Directors, Building Cyber Security; and Andrew

©2023 The National Institute of Building Sciences | All Rights Reserved.

Balster, President, Physical Space Practice, Geniant. It was moderated by Ari Reubin, who serves as Senior Vice President, KMC Consulting (a division of KMC Controls, Inc.).

The 2023 Operational Technology Cybersecurity Threat Landscape

When it comes to today's operational technology (OT) cyber-physical threat landscape, Red Bison Co-CEO EJ Von Schaumburg said decision makers greatly benefit by thinking about the "people, processes, and technologies" to understand, monitor and ultimately reduce their vulnerability from cyber-physical threats.

"Taking out one of those OT systems can literally impact human safety," he said.

A BlackBerry survey of 1,500 manufacturing IT decision-makers across North America, the United Kingdom, Germany, Japan, and Australia found that leaders were most concerned with malicious attacks through connected devices, including via the Internet of Things (40 percent); unauthorized access to sensitive data by malicious insiders (29 percent); and ransomware attacks (23 percent).

So what drives operational technology cyber risk? According to the BlackBerry survey:

- More than a third of respondents (36%) admit they still use Windows NT, an OS first released in 1993 and last supported nearly 20 years ago in 2004.
- Nearly half (46%) say they still use Windows XP (released in 2001), for which support ended almost nine years ago in 2014.
- Well over half (57%) utilize workstations running Windows 7, for which support expired three years ago. The same number (57%) depends on Windows 8, which Microsoft stopped supporting in January 2023.

Site reference:

- BlackBerry: Operational Technology Cyberattacks and the 2023 Threat Landscape

There Are Many Types of OT Systems

OT systems run the gamut across multiple property types, from stadiums to self-storage facilities.

Systems include, but are not limited to:

- Fire detection (alarms) and protection (sprinklers)
- HVAC (ventilation, chillers, air handling, and purification)
- People transport (elevators, escalators, and moving walkways)
- Lighting (standard and emergency)
- Utilities (gas, water, and electric)
- Physical access (security controls, video surveillance, and people count)
- A/V and digital signage (standard and emergency)
- Building automation (IT, owner network, and property management)

Building Cyber-Physical Security assigns a risk assessment score at each site using cyber-physical impact modeling (CIM) through a framework that it developed.

"We built the controls to support each one of these systems," said Red Bison's Von Schaumburg. "Not every building will have these [systems], but we needed to build a reference [to apply to your individual circumstance]."

Site reference:

- Building Cyber Security

Case Study: Ransomware Attack On MGM Resorts

On September 11, 2023, a ransomware attack on MGM Resorts resulted in 10 days of system downtime and loss of $80 million. The threat actor was dubbed "Scattered Spider" and is alleged to have ties with the ALPHV/BlackCat ransomware gang.

©2023 The National Institute of Building Sciences | All Rights Reserved.

Hon. Lucian Niemeyer, CEO & Chairman of Board of Directors, Building Cyber Security, said when it comes to commercial facilities, if there's an attack to OT, occupant safety comes first.

"If you even suspect that you have critical fire controls that are in any way compromised, you have to evacuate the building," he said. "BCS works with members to mitigate threats … to significantly reduce the physical safety threat to a building."

In the case of the "Scattered Spider" attack, this created havoc to casinos and properties, affecting elevators, digital room keys, and slot machines, ultimately impacting resort revenue.

"Scattered Spider" relied heavily on social engineering to break into company networks, manipulating victims into performing actions by impersonating others and using fear-mongering tactics, targeting individuals through phone calls and text messages with personal information to coerce victims into sharing credentials for corporate access.

MGM still is recovering from its attack, and it could've been much worse.

A second case study covered by the panel involved service providers and ex-employees.

Fred Gordy, Director, OT Risk Assessments, Michael Baker International, shared several pieces of information, including the fact that 75% of insider threat cases involved a disgruntled ex-employee who left with company data, destroyed company data, or accessed company networks after their departure.

The Next Logical Step In Building Information Modeling

Andrew Balster, President, Physical Space Practice, Geniant, said there are many advantages with building information modeling (BIM).

"We have really intelligent models," Balster said. "It's getting more advanced. We're rapidly approaching building modeling in real-time operations … into a unified control system. That's a lot of information to take in, and it's happening at a very fast pace."

He pointed to quote by Niemeyer: "There is the immediate need for digital twin templates/formats that the AEC industry will meet at minimal cost that is the next logical step in BIM."

Movement-level change requires new actors, including technologists of record (TOR) in the cyber-physical space.

"Technology has a huge role to play," he said. "We're going to need a Technologist of Record going forward with every project. As well, there is a clear and present need for BCS to thoughtfully partner with NIBS to create and present at a 2024 NIBS event on Cyber-Physical Commissioning."

What's Next

The next installment of the Building Innovation webinar series takes place December 12. It will cover Innovations and Operations: Developments in Sustainable Precast Concrete.

Register now.

©2023 The National Institute of Building Sciences | All Rights Reserved.