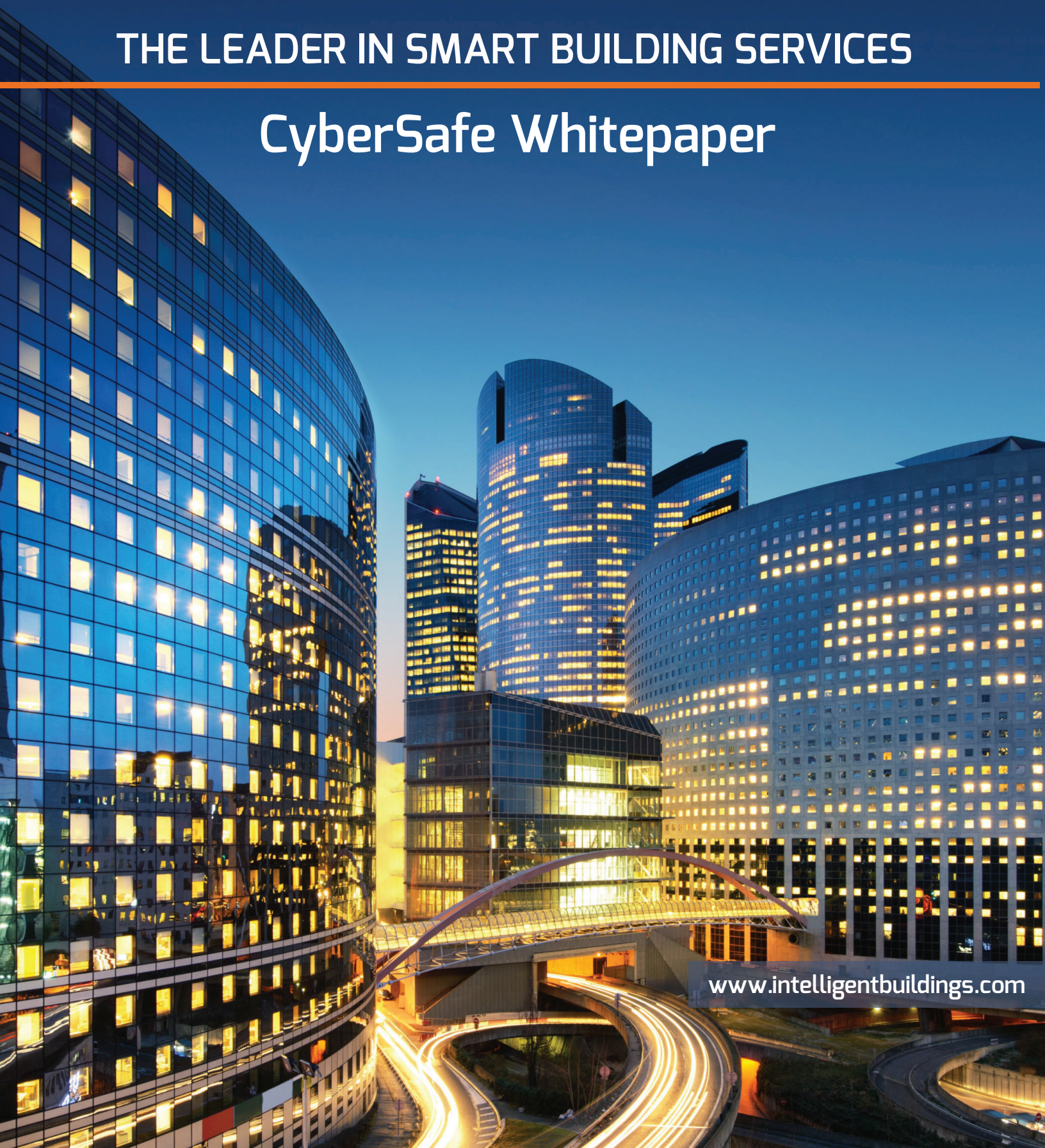
IntelligentBuildings®

THE LEADER IN SMART BUILDING SERVICES

CyberSafe Whitepaper



www.intelligentbuildings.com

SUMMARY

The real estate industry is awakening to the significant cybersecurity risks for existing building monitor and control (M&C) systems such as HVAC, lighting, fire life-safety, elevator and meters.

THE NATURE OF BUILDING SYSTEMS

Building (M&C) technology has changed faster than the traditional industry support structure, such as architects, engineers and contractors can keep up with.

Digital M&C systems installed in the past twenty years leverage information technology (IT) because they are run by a computer server, connected via local area networks (LAN) and allow remote access.

However, the traditional real estate processes have not integrated IT into the design, construction and operations standards and real estate organizations have not aligned their internal departments to this new reality of IT in M&C systems. What's more, the system vendors themselves are ill equipped to design, install and manage the very IT networks required for their products. Since many buildings have a dozen or more M&C systems the problems and risks are compounded.

THE LANGUAGE OF BUILDING SYSTEMS

For decades, building M&C systems have leveraged communication protocols, as a way for the main computer and floor level controllers to send commands to field devices (such as an VAV box or air vent for HVAC) and also to report status and performance information.

There have been many advances in translating tools to allow disparate protocols to communicate with each other and to foster a new generation of operational procedures such as system interoperability, remote monitoring, centralized command & control, building system analyitcs, unified user interfaces and other big data tools that help make data driven decisions and operational efficiency.

Regretiably, these advances have come without an eye for common IT practices for reliability and security and have left many critical systems exposed to failure due to skills gaps, mismanagement or malicious intent.

COMMON IT ASPECTS IN BUILDING SYSTEMS

Today's building systems leverage best-in-breed operating systems such as Microsoft Windows and RedHat Linux as well as supporting software components like web servers and browsers, relational databases, JAVA virtual machines and remote desktop and access features allowing for rapid system deployment using low-cost, off-the-shelf IT computing equipment and intuitive end-user interfaces requiring little to no formalized training.

The adoption of well known underlying hardware, operating systems and softwares implifies deployment thereby keeping costs down. The consequence, however, is an insecure implementaton of operating system, firmware and leaving supportng software vulnerable to known exploits.

Secure configuration of these core components are typically not part of building control system installation standard operating procedures.

IOT IN REAL ESTATE

Real Estate is not immune to the increasing phenomenon of the "Internet of Things" (IoT). Society continues to see and demand a seemingly endless number of devices connected to the internet, and so it is in our facilities.

Not only are building monitor and control systems nearly all IT-centric and web-enabled but so are many devices, appliances and other electronics in our buildings. This puts pressure on organizations, not only to enable connectivity but also to evaluate the cyber-security implications for our core M&C systems such as network hopping from non-M&C systems to M&C systems.

JUST THE BEGINNING

While there is clear agreement on the architectural and operational vulnerabilities of nearly all digital building M&C systems there are also a growing number of stories that show the tip of the iceberg on actual events including the following examples.
[Hackers] penetrated the building energy management system (EMS) of a New Jersey manufacturing company (Q1 2013, U.S. Dept. of Homeland Security ICS-CERT Monitor)

- A state government facility's building EMS was compromised by an intruder who was able to manipulate set points to change the temperature settings (Q1 2013, U.S. Dept. of Homeland Security ICS-CERT Monitor).

- Investigations by the security firm assisting in the Target store breach have now determined that many of the heating, ventilation, and air conditioning (HVAC) systems connected to the Internet over the past few years have vulnerabilities hackers can exploit ("Hackers and Malware Are Geeng Smarter" Curt Hall, CuVer Consortium, February 2014).

- Researchers hack building bontrol system at Google Australia office (Kim ZeVer, Wired, May 2013).

- Hacker finds a flaw that gives remote hackers the ability to download all the user names and passwords for all the users on the Niagara server.The attack is trivial and very reliable (Washington Post article entitled Tridium's Niagara Framework: Marvel of connectivity illustrates new cyber risks, By Robert O'Harrow Jr., Published: July 11, 2012.

STEPS TOWARDS CYBER SECURITY

The first step towards a more cyber-secure state is an inventory and vulnerability assessment. This requires several skill sets in several areas including IT, facility management, controls systems and risk management.

The assessment should include a risk rating in key categories such as software/firmware, remote access, organizational and vendor policy and others. Only then can a proper remediation plan be instituted. The inventory and remediation process should be based on the established NIST Risk Security Framework (RSF) and grafted into the building M&C environment.

There are different risk event possibilities in real estate facilities than in typical enterprise IT; although the NIST framework is still an appropriate methodology, given the consultant has both IT and M&C expertise.

ASSESS KEY CATEGORIES

FIND ANY VULNERABILITIES

UPDATE YOU PLAN