INTELLIGENT BUILDING MANAGEMENT SYSTEMS:

Guidance for Protecting Organizations

David J Brooks **Michael Coole** **Paul Haskell-Dowland**

This guidance provides both the security and facility professional with the necessary information and a framework to protect their organizations against risks associated with Intelligent Building Management Systems (IBMS) vulnerabilities. The guidance aims to support such decision making in combination with relevant standards, guidelines, and other resources.

The guidance provides checklists to assist practitioners in protecting their facilities against vulnerabilities associated with IBMS. The checklists take an organization's risk level into account and then asks a series of directed security questions that lead to mitigation strategies.

DEFINING IBMS

IBMS are automated building systems that converge and integrate the many building technologies and information flow processes to a central decision point.

IBMS are also known by many other terms, such as a Building Automation System, Facilities Management System, Energy Management System, Building Management System, Intelligent Building, and today, Smart Buildings. However, the core principles of IBMS remain the same, regardless of its name.

The scale of IBMS vary from an automated home heating system to a high rise Intelligent Building, which centrally automates and controls all functions including HVAC, lighting, elevators, and life safety systems, along with maintenance, administrative, and business functions. Today, security is also becoming embedded within the function and business of IBMS.

With the advent of the Internet of Things (IoT), IBMS will continue to expand into more diverse and complex areas of everyday life. Connectivity through the IoT means, in simple terms, that anything can be linked and incorporated.

IBMS are growing at approximately 15 to 34 percent each year, due to the demand for energy-efficiency, reduced maintenance, and the greater control and operability. By 2022, the IBMS industry will be worth an estimated $104 billion. Such growth highlights the current and expected impact that IBMS will have in most future built environments.

The growth of the IBMS market is driven by the medium-to long-term requirement to save resources with improved efficiencies and environmental targets imposed by governments. With global rises in energy costs, pollution sanctions, and green government incentives, IBMS initiatives are at the forefront of the majority of future facility projects.

IBMS are integrating a greater number of building technologies and functions of business. Technology is driving an increased integration of other business and building systems into IBMS. Integration includes security systems, such as intruder detection, access control, and surveillance cameras. These aspects will affect the security professional in their ability to effectively protect against the increase in IBMS vulnerabilities.

Examples

There are many examples of these systems in all types of facilities:

Small Scale System

The building has a security access card system. An authorized employee swipes an access card on an external card reader to gain entry to the building. Upon swiping, the entry door automatically opens to allow the employee access and entry lights are automatically turned on. The door automatically closes and lights turn off as the employee moves to their work space.

Large Scale System

The Human Resource (HR) and payroll system transfers personnel data to the security access card system, authorizing access to certain work spaces in the building. This approach facilitates single data entry for all employees of the organization. As the employee swipes an access card, the door opens based on their authorized HR work space. Information gathered from that card swipe is linked back to payroll to monitor time and attendance. Lighting and heating/cooling systems are turned on as the employee moves through the facility to reach his or her work space. IBMS monitor the external and internal environment to ensure that the internal environment is comfortable while minimizing utility use.

An IoT System

The lighting and heating/cooling systems all operate as above; however, the security

access credential is the employee's personal smartphone. As the employee drives to the vicinity of the building, he or she is directed by smartphone into alternative parking at a neighboring building. The building has wireless connected cashless entry machines. The employee's access credential is used at the cashless machines and parking fees are charged back through payroll for automatic deduction.

While the efficiencies and potential savings for organizations embracing these systems are manifold, the vulnerabilities created through the use of these systems are potentially brand damaging and life threatening. The ability to enter these systems at their physical or logical weak points results not only in access to the IBMS, but also to the entire organizational enterprise system. Such access exposes not only the physical building, but also company data and information.

IBMS are modular in nature, formed from the integration of a number of devices, equipment, and common communication platform networks. IBMS architecture is based on three levels: Management, Automation, and Field Devices.

Management Level

The management level contains the human interface, connected via the enterprise software and communication network. Management level equipment includes workstations, network switches, and servers. IBMS manufacturers provide software packages allowing designers and users to select what suits their facility. The management level software packages range from simple information processing systems that control a single room to complex facility services that monitor and control plant and equipment, providing functions such as energy management, lighting, and maintenance.

Automation Level

The automation level provides primary control devices, connected via networked controllers and operating via open source communication protocols. They provide the interface between the IBMS physical field devices and the management level human interface. Examples of automation equipment includes controllers and routers.

Field Device Level

The field device level provides physical devices, such as sensor or activators connected to specific plant and equipment. These devices connect IBMS to their physical environment. Examples of field level devices include light switches, PIR detectors, fans, temperature sensors, and valves.

Communications

For IBMS to function, there is a requirement for connectivity and common language communication. Connectivity is achieved via various communication networks that integrate the many discrete devices. Connectivity has led to a number of building automation network and communication protocols. Currently, no particular protocol or standard exists for all building automation; however, some common protocols include BACnet, LonWorks, Internet Protocol and Hypertext Transfer Protocol, to name a few.

Connectivity is a significant element of IBMS. The technical architecture facilitates connectivity, which in turn supports communication and automated control functions. The many IBMS vulnerabilities lie in this architectural level of connectivity and common communication protocols. Consequently, security and facility professionals need to understand this architecture to understand IBMS vulnerabilities and mitigation strategies.

IBMS VULNERABILITIES

IBMS generic vulnerabilities have been broken down into the three architectural levels of automation, management, and field device levels. IBMS are prone to attack at all levels. Vulnerabilities are situational and are best

understood through understanding the facility's threats, criticalities, and context. The following hypothetical examples can help practitioners better understand these vulnerabilities.

IBMS Vulnerabilities Case Studies

Automation level vulnerabilities

A contract maintenance worker is granted access to all plant rooms and electrical risers throughout the facility. The plant rooms contain IBMS automation network cabling and controllers, which control and monitor the local HVAC, lighting, access control, and security detectors for that floor. The maintenance worker wants to gain illegal access to the facility after hours and knows that IBMS monitor the security detectors. The controllers are mounted on the wall in an open enclosure, which allows the worker to plug their laptop into the controller's service port rather than take the time to strip the network cable to connect a wiretap. Once plugged into the controller, they find that there are no security restrictions on viewing the automation level program and network traffic. The worker reprograms the security alarms, to automatically turn off at night. In addition, sets the door locks to open. The worker arrives that night, with clear and open access into and out of the facility.

Management level vulnerabilities

An organized crime group targets a retail company, with the intent to steal credit card information. They send an email with an embedded virus to an account at the IBMS integrator. The integrator maintains IBMS for a number of different organizations, including the targeted retail company. The IBMS integrator has remote access to many of their clients' IBMS to provide fast and efficient 24/7 technical support. On opening the email, a virus configures third party access to the IBMS's management software, providing access to the target organization's information technology network. The crime group gains unauthorized access to credit card details.

Device level vulnerabilities

A disgruntled employee wants to get back at his or her employer by anonymously causing the business harm. The business operates in a facility that has a public foyer, shared by other organizations. The dismissed employee has open access to the foyer that has a HVAC temperature sensor with a cover fixed by a simple screw. Standing in front of the sensor, the dismissed employee removes the cover and places a resistor across its output terminals. This results in the IBMS controllers sensing that the foyer is far warmer than the actual room temperature, which commands the HVAC to cool the foyer. This excessive cooling makes the foyer uncomfortable to use and causes a disruption of service as well as raising operational costs. It takes the technician a number of hours to track down the cause of the misreading sensor at cost and inconvenience to the organization.

HOW TO USE THE IBMS MITIGATION GUIDANCE

The guidance identifies and mitigates IBMS risks through a facility level checklist. The security questions answered are dependent on the risk level of the facility. Questions are divided into criticality levels, from level 1 (low) to level 5 (critical).

To use the IBMS Guidance:

1. Identify your organizational criticality level.
2. Respond to the IBMS security questions for your identified criticality level.
3. Check off compliance with each question, and
4. Where compliance is not achieved, define a responsible person and date of action.

LOW LEVEL CHECKLIST

The following criteria indicate a low level security designation.

- Expected to harm government agency operations, commercial entities or members of the public
- No measurable operational impact
- Local management intervention required
- Financial loss of <1%
- No measurable reputational loss
- Injury or occupational illness not resulting in a lost work day
- No effect on statutory accreditation or operations
- Limited operational information exposed
- No effect on occupancy

MANAGEMENT

- [ ] Do you have a written and endorsed security policy?
- [ ] Do you have written and endorsed security procedures?
- [ ] Is IBMS formally assigned to the facility manager?
- [ ] Do you have a committee or working group of relevant IBMS stakeholders that meets regularly?

SECURITY RISK MANAGEMENT

- [ ] Does your facility have a designated criticality or business impact rating?
- [ ] Are your IBMS risks noted assessment?

PERSONNEL SECURITY

- [ ] Do you have personnel security policies and procedures in place?
- [ ] Are your personnel security policies and procedures current?
- [ ] Do your personnel security practices include pre-employment screening?
- [ ] Do you have an auditable procedure to authorize access IBMS?

PHYSICAL SECURITY

- [ ] Do you have policies and procedures for assigning physical access rights?
- [ ] Do your physical security strategies protect the facility's IBMS infrastructure?
- [ ] Is physical access to all IBMS infrastructure controlled?
- [ ] Are the facility's IBMS Controllers, routers, and network switches physically protected?
- [ ] Are IBMS enclosures in a secure and protected area?
- [ ] Are IBMS Enclosures locked?
- [ ] Do you have a procedure for ensuring that (mechanical) keys related to IBMS are controlled?

CYBERSECURITY

- [ ] Do you have policies and procedures to authorize and assign IBMS logical access privileges?
- [ ] Is logical access to your IBMS restricted and authorized based on role?
- [ ] Is there a register of who has logical access to your IBMS?
- [ ] Do you have an auditable access log for all individual IBMS users and/or maintainers?
- [ ] Do you control your IBMS remote and/or external logical access?
- [ ] Do your IBMS logical access have rules of password complexity?
- [ ] Do your IBMS have session time out lock?
- [ ] Do your IBMS have the most current software patches?
- [ ] Are your IBMS's master access codes, PINs, or IDs held in a secure location?

- [ ] Have the factory or default password or other access means been deactivated?
- [ ] Do you know who is responsible for updating your IBMS logical and configuration back-ups?
- [ ] Are your IBMS logical program and configuration details held in a secure location to enable recovery and reconstitution?

INCIDENT RESPONSE

- [ ] Are your IBMS able to maintain capably during a routine or nonroutine incident to support an emergency response?
- [ ] Are your routine or nonroutine incident response plans tested through desk-top exercises' to a defined schedule?

CONTINUITY PLANNING

- [ ] Do the IBMS feature in your continuity plans?
- [ ] Are you able to take manual control of your facility sub-systems from IBMS, such as heating/cooling, lighting, etc., to maintain operations?

MAINTENANCE

- [ ] Do your IBMS have a scheduled maintenance plan?
- [ ] Are your IBMS maintained by a known IBMS maintainer?
- [ ] Do you have policies and procedures that authorize connection to IBMS communication network cable or its devices, including controllers, routers, and network switches.
- [ ] Are your IBMS part of the facility's asset tracking system?

MODERATE LEVEL CHECKLIST

The following criteria indicate a moderate level security designation.

- Expected to damage government agency operations, commercial entities, or members of the public
- Moderate degradation of parts of operations, loss of function will have limited effect on ability to maintain operations
- Executive intervention required
- Financial loss of <2%
- Some measurable reputational loss to some parts of the business
- Injury or occupational illness resulting in 1 or more lost work day(s)
- Limited effect on statutory accreditation, with no operational impact
- Restricted operational information exposed
- Some effect on parts of the facility to occupy

MANAGEMENT

- ☐ Do you have a written and endorsed security guideline or basis of design document, which define security zones?
- ☐ Is physical access to security zones based on role and personnel screening?
- ☐ Do you have a written and endorsed facility security policy?
- ☐ Are IBMS workstations positioned according to security zoning policies?

PERSONNEL SECURITY

- ☐ Do your personnel security policies and procedures include signed acceptable expectations of conduct, terms and conditions of employment and entry and legal rights and responsibilities?
- ☐ Do your personnel security policies cover access to IBMS?
- ☐ Do you have policies and procedures for authorizing access to individual IBMS equipment or devices?
- ☐ Are IBMS access authorizations audited and anomalies investigated?
- ☐ Are new personnel inducted with security awareness training?

PROCEDURAL

- ☐ Are access authorization procedures followed before a person, either employee or third-party contractor, is given access to IBMS network infrastructure?
- ☐ Do IBMS security breaches get reported and investigated by appropriate personnel?
- ☐ When a person exits the organization or changes roles, are physical access rights removed or adjusted?
- ☐ Are security awareness training programs documented?
- ☐ Do you have policies and procedures to control the use of mobile storage devices?
- ☐ Do you have policies and procedures to control the use of “bring your own” device?

PHYSICAL SECURITY

- ☐ Are IBMS enclosures resistant to unauthorized access?
- ☐ Are the IBMS Field level devices connected using supervised (monitored) cables between the device and its controller?

CYBERSECURITY

- ☐ Do you have “as built” IBMS architecture schematics or drawings, including IP addresses, hardware, locations, etc?
- ☐ Are your IBMS network integrated with external devices, such as cloud computing services?

- [ ] Do you have a database of logical access privileges for IBMS users and maintainers?
- [ ] Can you identify and authenticate persons through events logs, etc., who have logical access to your IBMS?
- [ ] Do you have an alert system for unauthorized logical access attempts?
- [ ] Do you have an alert system for unauthorized logical traffic?
- [ ] Do you have an appropriate level of protection for your IBMS enabled wireless connectivity?
- [ ] Are there user and IBMS maintainer restrictions for IBMS wireless connectivity?
- [ ] Are your IBMS logical program and configuration details held in a secure off-site location?

INCIDENT RESPONSE

- [ ] Are your incident response plans tested through desk-top exercises' to a defined schedule?

CONTINUITY PLANNING

- [ ] Are your continuity plans tested through desk-top exercises' to a defined schedule?

MAINTENANCE

- [ ] Has your IBMS maintainer demonstrated an understanding and compliance to maintaining IBMS security?
- [ ] Are all IBMS hardware and software changes authorized and documented?
- [ ] Do you have a IBMS legacy plan?

HIGH LEVEL CHECKLIST

The following criteria indicate a high level security designation.

- Expected to damage national security
- Substantial degradation of operations impact on multiple business functions
- Substantial executive intervention required
- Financial loss of >3%
- Measurable reputational loss to multiple parts of the business
- Partial disability, injuries, or occupational illness that result in hospitalization of > 1 person
- Record of noncompliance against statutory accreditation, with some operational impact
- Restricted commercial information exposed
- Unable to occupy major parts of the facility for an extended period

MANAGEMENT

- [ ] Are IBMS specifically included in your security policy
- [ ] Do you undertake and propagate environmental scanning to stay informed on best practice to protect IBMS?
- [ ] Do you maintain liaisons with external agencies, departments, industry groups, and other organizations for IBMS security?
- [ ] Do you undertake periodic audits to ensure that all security strategies are applied and operating as intended?
- [ ] Are IBMS security audits undertaken?
- [ ] Are periodic meeting scheduled with IBMS stakeholders, such as facilities, IT, cybersecurity, and IBMS Maintenance, in regard to the security of IBMS?
- [ ] Are your IBMS security meetings documented?
- [ ] Are proposed and/or changes to IBMS reviewed by relevant stakeholders?

SECURITY RISK MANAGEMENT

- [ ] Do you undertake vulnerability assessments of your IBMS?
- [ ] Are IBMS risks updated in the risk register?

PERSONNEL SECURITY

- [ ] Are personnel who will have direct access to IBMS management level workstations, terminals and networks screened for access?
- [ ] Do you undertake pre-employment screening (including third parties and contractors) of your IBMS maintainance personnel?
- [ ] Are regular audits of IBMS maintenance personnel status undertaken?
- [ ] Do you have formal review policies and procedures in place for when a person moves roles?
- [ ] Are the IBMS part of the security awareness training process documented?
- [ ] Are regular reviews of IBMS maintenance personnels' access undertaken, for example ensuring that access credentials align to a person, etc?

PROCEDURAL

- [ ] Do you have formal procedures for security breaches involving suspected unauthorized IBMS access?
- [ ] Are exit interviews undertaken for staff using or maintaining your IBMS?

PHYSICAL SECURITY

- [ ] Are the IBMS physical vulnerabilities documented?

- [ ] Are the IBMS Automation level communication network cables protected?
- [ ] Do the IBMS enclosures have door and rear-mount tamper detection?
- [ ] Are your IBMS Field level devices connected using a three-state supervised circuit (monitored) cable between the device and its controller?
- [ ] Are your IBMS intruder and/or fault alarms monitored on a real time basis?
- [ ] Are IBMS logical access points located in a secure room or zone?

CYBERSECURITY

- [ ] Are your IBMS network logically separated from your enterprise network?
- [ ] Do you control remote wireless IBMS connectivity through restricted and managed access points?
- [ ] Do you have appropriate protection over embedded IBMS wireless connectivity?
- [ ] Does your IBMS logical access have multi-factor Secure ID Key?
- [ ] Does your IBMS logical access passwords have unsuccessful login attempts, automatic lock out and access attempt rules?
- [ ] Are your IBMS device configurations audited to a defined schedule?
- [ ] How often are your IBMS unauthorized logical access alert detection system updated?

INCIDENT RESPONSE

- [ ] During incident response training, are the facility's IBMS included in response strategies?
- [ ] Are your incident response plans tested through physical exercises to a defined schedule?
- [ ] In a routine or nonroutine incident when site power is lost, do your IBMS maintain capability to support the emergency response?
- [ ] Following a routine or nonroutine incident, do you undertake a post incident investigation?

CONTINUITY PLANNING

- [ ] Have you tested your IBMS logical program and configuration to exercise recovery and reconstitution?

MAINTENANCE

- [ ] Do your IBMS have a predefined response and recovery period to a defined schedule?
- [ ] Do your IBMS have an auditable log of all hardware and software changes and alterations?
- [ ] Do your IBMS maintenance personnel securely store and control authorized and accountable access of your IBMS knowledge, for example documentation, configurations, etc?

EXTREME LEVEL CHECKLIST

The following criteria indicate an extreme level security designation.

- Expected to seriously damage national security
- Impact on multiple critical business functions, loss of function will effect the ability to maintain parts of operations
- Immediate senior executive intervention required
- Financial loss of >5%
- Significant but short term loss of trust across all parts of the business
- Permanent partial disability, injuries or illness that result in hospitalization of >3 people
- Loss of statutory accreditation to operate for a short period
- Significant commercial information exposed
- Unable to occupy the whole facility for a short period

MANAGEMENT

- [ ] Does your security guideline or basis of design document explicitly include IBMS and its sub-systems?
- [ ] Do you have security zoning for IBMS Automation and Management levels?
- [ ] Are mobile recording or storage devices subject to restricted access into defined security zones or areas?

SECURITY RISK MANAGEMENT

- [ ] Do you have a security context (threat) statement for the facility?
- [ ] Do your security risk assessments specifically capture IBMS risks?

PERSONNEL SECURITY

- [ ] Do you categorize and assign a risk to all positions that use and/or have access to your facility's IBMS?
- [ ] Are your IBMS maintenance personnel (including third parties and contractors) managed as internal employees?
- [ ] Do you have a procedure to positively identify and log IBMS maintenance personnel prior to and during IBMS access?
- [ ] For IBMS users and maintainers, are ongoing screening audits undertaken?
- [ ] Is the IBMS security awareness training package assessed and results documented?

PROCEDURAL

- [ ] Do you have escort policies and staff for your IBMS maintainer?

PHYSICAL SECURITY

- [ ] Is physical access to all IBMS hardware and software strictly controlled?
- [ ] Do the IBMS enclosures have security tamper seals to detect actual or attempted manipulation?
- [ ] Are the IBMS controllers, routers, and network switches protected by a volumetric security detector?
- [ ] Do the IBMS (mechanical) access keys remain onsite and are not removed from site at any time?
- [ ] Are your IBMS Field level devices connected using a four-state supervised circuit (monitored) cable between the device and its controller?
- [ ] Do your IBMS supervised (monitored) cable detect both fault and tamper when unarmed?

CYBERSECURITY

- [ ] Do you monitor the IBMS logical access from the enterprise network?
- [ ] Is logical access authorization to your IBMS gained through positive identification and authentication?
- [ ] Is IBMS information flow between other connected systems or networks documented, controlled and authorized?
- [ ] Do you enforce the “least privilege” for IBMS users and maintenance personnel.?
- [ ] Do you have policies and procedures to restrict the use of “bring your own” device?
- [ ] Are your IBMS logical program and configuration details regularly audited by authorized persons?
- [ ] Do you undertake IBMS penetration testing on a scheduled basis?

INCIDENT RESPONSE

- [ ] Following a routine or nonroutine incident, do you undertake a post incident investigation?
- [ ] Do you have a continuity plans for the compromise (fire or similar) of workstations or other central control points used by IBMS during an incident response?
- [ ] Are your IBMS connected to an uninterruptible power supply system to maintain critical operational functions?

CONTINUITY PLANNING

- [ ] Are your continuity plans tested through physical exercises to a defined schedule
- [ ] Do you have remote IBMS control room capability?

CRITICAL LEVEL CHECKLIST

The following criteria indicate a critical level security designation.

- Expected to cause exceptional grave damage to national security
- Impact across all critical business functions, vital to business operations, loss of function will have extreme effect on the ability to maintain operations
- Immediate Board intervention required
- Financial loss of >10%
- Significant and long term loss of trust across all parts of the Business
- Multiple deaths and/or permanent total disability of >3 people
- Loss of statutory accreditation to operate for an extended period
- Significant commercially sensitive information exposed
- Unable to occupy the whole facility for an extended period

SECURITY RISK MANAGEMENT

- ☐ Do you undertake a IBMS specific threat assessments?

PROCEDURAL

- ☐ Are IBMS equipment or device security tamper seals audited on a regular basis?

PHYSICAL SECURITY

- ☐ Does your physical protection of IBMS equipment or devices provide evidence of attempted or actual unauthorized access?
- ☐ Are clear conduits used for all IBMS Automation level connection cables and components?
- ☐ Are the IBMS controllers, routers, and network switches protected by a two over-lapping volumetric security detectors?
- ☐ Are your IBMS Field level devices connected using a two-way polled 56 bit DES key encryption supervised (monitored) cables between the device and its controller?
- ☐ Do you carry out technical surveillance counter measure evaluations on your IBMS on a regular, but random schedule?

CYBERSECURITY

- ☐ Do your scan for unauthorized wireless IBMS connectivity to a defined schedule?
- ☐ Are all wireless connectivity devices disabled?

MAINTENANCE

- ☐ Are your IBMS maintenance personnel escorted at all times while on-site?
- ☐ Is your IBMS equipment, devices or software verified prior to installation and/or replacement?