1-1-2020

Intelligent building systems: Security and facility professionals' understanding of system threats,vulnerabilities and mitigation practice

David J. Brooks
Edith Cowan University

Michael Coole
Edith Cowan University

Paul Haskell-Dowland
Edith Cowan University

10.1057/s41284-019-00183-9

Intelligent Building Systems: Security and Facility Professionals' Understanding of System Threats, Vulnerabilities and Mitigation Practice

David J Brooks, Michael Coole & Paul Haskell-Dowland

ABSTRACT

Intelligent Buildings or Building Automation and Control Systems (BACS) are becoming common in buildings, driven by the commercial need for functionality, sharing of information, reduced costs and sustainable buildings. The facility manager often has BACS responsibility; however, their focus is generally not on BACS security. Nevertheless, if a BACS manifested threat is realized the impact to a building can be significant, through denial, loss or manipulation of the building and its services, resulting in loss of information or occupancy. Therefore, this study garnered a descriptive understanding of security and facility professionals' knowledge of BACS, including vulnerabilities and mitigation practices.

Results indicate that the majority of security and facility professionals hold a general awareness of BACS security issues, although they lacked a robust understanding to meet necessary protection. For instance, understanding of 23 BACS vulnerabilities were found to be equally critical with limited variance. Mitigation strategies were no better, with respondents indicating poor threat diagnosis. In contrast, cybersecurity and technical security professionals such as integrators or security engineering design professionals displayed a robust understanding of BACS vulnerabilities and resulting mitigation strategies. Findings support the need for greater awareness for both security management and facility professionals of BACS vulnerabilities and mitigation strategies.

Keywords: Intelligent, smart, cybersecurity, risk, threat, mitigation, professional, convergence

INTRODUCTION

Intelligent Buildings or more accurately, Building Automation and Control Systems (BACS) is a system that integrates many disparate building systems and services, such as HVAC, lighting and security systems. These systems are becoming more embedded into the built environment and its buildings. Today, BACS technology and its connectivity extends beyond just the large high rise commercial building, adopted by small commercial and some domestic buildings. The applications of BACS are driven by the cumulative commercial need for increasing functionality and the seamless flow of information across an organisation, with the aim to reduce enterprise operating costs and provide a more time responsive building. Increased application of BACS can be shown through a market that has an expected compound annual growth of between 15 to 34 percent, to an estimated value of US$104 billion by 2020 (Marketsandmarkets, 2017; Technavio, 2016; TMR Analysis, 2017). With global rises in energy costs and greater government sanctions, BACS are likely to be at the forefront of future buildings (Brooks, Coole, Haskell-Dowland, Griffith & Lockhart, 2018b, p. i).

BACS, as building infrastructure, are generally owned and operated by facility professionals or building owners/operators. Building owners/operators primary foci are the drivers of cost efficacy and functionality that a modern BACS offers (Frost & Sullivan, 2008); however, BACS are also used by many other organisational departments. For example, the technology of BACS lies across multiple departments, including Information Technology and Communications (ITC) on which the corporate network facilitates the flow of BACS information and security (Brooks, et al., 2018b), where security systems such as access control and surveillance often converge.

The technology spread of BACS throughout all parts of a building, with multiple owners and users, leaves these systems open to associated security risks (Brooks, et al., 2018a). BACS are designed predominately from a commercial perspective and primarily operated by facility engineering professionals, who may have a limited focus on the security of the business and its built environment. Yet it can be argued that the security of such technologies is a significant business concern and therefore, the security strategies to mitigate risks against breaches of confidentiality, integrity and availability within the BACS context should be embedded in the organisational culture. If a BACS threat is realized, it can have a significant impact on the organisation, resulting in consequences such as loss of information to extended loss of occupancy.

Nevertheless, the level of awareness and understanding of the various professionals responsible for protecting BACS is not well known. With the increasing use, functionality and connectivity of BACS and their exploitable vulnerabilities in the built environment, the security and facility professionals require greater understanding to support sound risk mitigation strategies. Therefore, this article puts forward the following Research Question:

> What are the security and facility professionals' knowledge of BACS, their vulnerabilities and criticalities, and resulting security mitigation practices?

SECURITY OF BUILDING AUTOMATION

BACS are not just a convergence of a building's plant and equipment; rather, they are an information system. BACS are usually spread throughout a facility and across all levels of its communication networks, with the objective of cross-system connectivity. Consequently, many groups within an organization have, or should have, some level of BACS responsibility, but that is not always understood. Furthermore, these systems are becoming more interconnected and integrated with additional services and business applications. For example, the function of security and its associated technology is currently and will be more so, subsumed into BACS.

Issues such as the legacy of BACS technologies, remote access and interconnectivity raise the security considerations of BACS. For example, King (2016) points out that early generations of BACS were developed using discrete devices/protocols, and subsequently built upon and added to, rather than re-engineered with security as an underlying design principle (Sinopoli, 2012). Since "these service-based systems were not initially interconnected, they were not designed with logical security as a paramount concern or requirement" (King, 2016). Isolating BACS from external networks may mitigate remote attacks, but does not address the security vulnerabilities resulting from physical access to the automation network. As Sinopoli (2012) suggests, a localised attack is potentially much more dangerous and difficult to deal with. Vulnerabilities of BACS may also be public knowledge through hacker-run searchable websites such as www.shodan.io, which publicises known BACS vulnerabilities.

BACS are comprised of an architectural structure incorporating various levels of equipment and devices, which may be prone to nefarious exploitation. Such vulnerabilities expose the organisation to risks that may ripple throughout the whole organisation, resulting in substantial and far reaching impacts. Although in many cases the protection of BACS is not in the domain of most security management professionals, excluding cybersecurity, as their roles are heavily focused towards administrative duties and responding to incidents, they are arguably becoming more invested as their security systems and functions are becoming embedded in BACS. Furthermore, the ability of the organisation to occupy and operate in their

building are becoming more tied to BACS. Therefore, security professionals must demonstrate a sound understanding of the security concerns such a technological shift brings.

Nevertheless, technical security professionals are generally aware of the vulnerabilities associated with intruder alarms, access control systems, surveillance systems and other security technologies, and the various technical and procedural methodologies for countering these threats. However, cognizance must now transfer to their organisation's BACS. Currently, there is limited literature investigating the security management professionals understanding of BACS or providing specific BACS guidance aimed at this group. In contrast, there is a plethora of cybersecurity literature, aimed at professionals who have a high level of computing and networking technical knowledge. Therefore, contemporary security and facility management professionals need to have a comparative awareness and understanding of BACS, their vulnerabilities and appropriate mitigation strategies.

DEFINING BUILDING AUTOMATION

The concept of BACS developed to mean "the execution by a machine agent (usually a computer) of a function that was previously carried out by a human" (Parasuraman & Riley, 1997). Automation may be defined as the "use or introduction of automatic equipment in a manufacturing or other process or facility" (Simpson & Weiner, 1989). Automation provides the drive for ever more cost effective, efficient and reliable solutions through the gradual removal of the human. It is acknowledged that with repetitive processes, the automated alternative to human labour is cheaper, more responsive, consistent and less prone to error (Sall, 2017).

BACS integrates building services, such as utilities, with each other to exchange digital, analogue or other forms of information, potentially to a central control point for monitoring and action. Building services are utilities that are supplied and distributed within a building that may include electricity, gas, heating, ventilation, cooling (HVAC), water and communications (ISO, 2004, p. 6). To facilitate such control, computers and controllers in BACS are networked for peer to peer control. In addition, the BACS controllers have their own internal processors, supporting autonomous operations (High Performance HVAC, 2017).

Today, BACS may be known by many terms such as a Building Automation System, Facilities Management System, Energy Management System, Building Management System, Intelligent Building, and more recently, Smart Buildings. A more precise term is *Building Automation and Control System* (BACS), supported by the literature such as the International Organization for Standardization (ISO, 2007a). However, the core principles of BACS remain the same, regardless of its name. Given that the building automation industry in which BACS operate in is dynamic, these terms are often used interchangeably, and there is no single consensus that defines BACS.

Building Automation Fundamentals

BACS are modular in nature, formed from the integration of a number of devices connected and communicating on a common platform. The system's architecture contains three distinct levels (CIBSE, 2000), considered *Management*, *Automation* and *Field Device* levels (Figure 1).

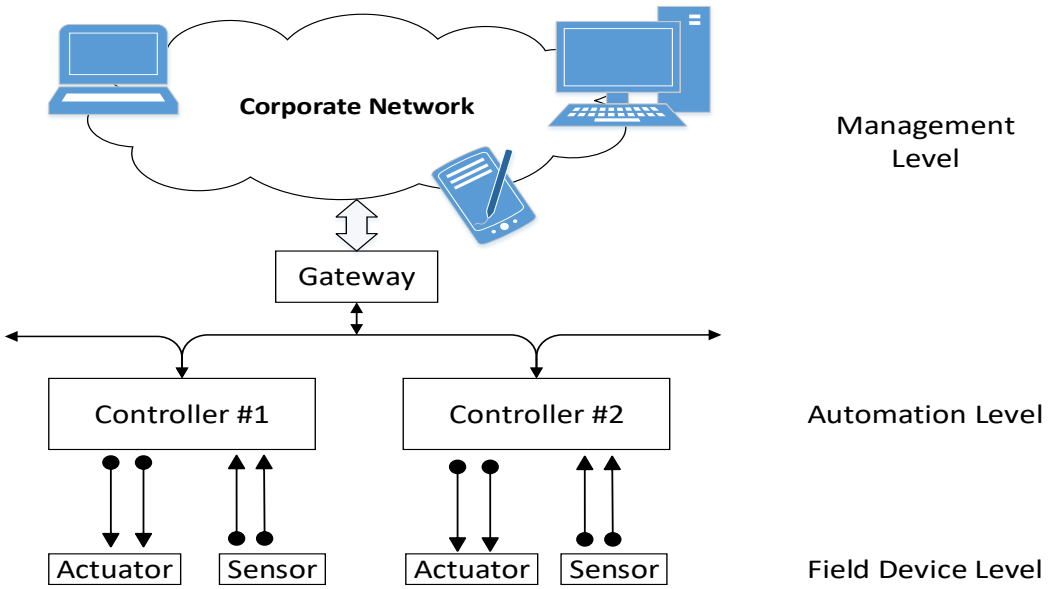

Figure 1. BACS Architecture (Brooks, et al., 2018b, p. 200)

In general, the Management level consists of the Information Technology and Communications (ITC) network, with connected "operator stations, monitoring and operator units, programming units and other peripheral computer devices connected to a data processing device i.e., a server" (ISO, 2004, p. 53). In addition, one or a number of data and information processing (software) packages enables a human system interface. Software packages range from simple information processing systems that control a single room via the internet to complex whole of building services, running not only the building plant and equipment, but also security, energy management, lighting and other services.

The Automation level is generally a dedicated communications network for the sole purpose of equipment and device connectivity, communication and control. The Automation level is comprised of "control devices and monitoring and operator units, programming units, operator stations or panels as well as programming units connected to a data processing device i.e., a server" (ISO, 2004, p. 53). This level is associated with Controllers that serve primary plant and equipment, including air handling units, chillers, boiler units and other plant and equipment.

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

Finally, for BACS to function there is a requirement for common language connectivity, achieved through standardised communication protocols at each or across its three architectural network levels. Currently, no particular protocol exists for all BACS; however, common protocols include BACnet, LonWorks, Modbus, KNX, Internet Protocol (IP), Hypertext Transfer Protocol (HTTP), to name a few (Schneider Electric, 2015; Sharples, Callaghan, & Clarke, 1999).

Building Automation Vulnerabilities

The high level of connectivity and the spread of devices throughout a building that is typical of a contemporary BACS results in a degree of embedded vulnerability that can be exploited by adversaries. The most significant vulnerabilities are considered to be physical access to the Automation level devices

and its communications network (Brooks, 2013; Sinopoli, 2012). The consequences of realized threats for BACS can be divided into three categories (Figure 2) of loss, denial or manipulation (Assante & Lee, 2015, p. 11) to control and monitoring (Brooks, et al., 2018b, p. 199). These consequences pose a significant risk to the confidentiality, integrity and availability of the organisation's information, buildings and other business elements.

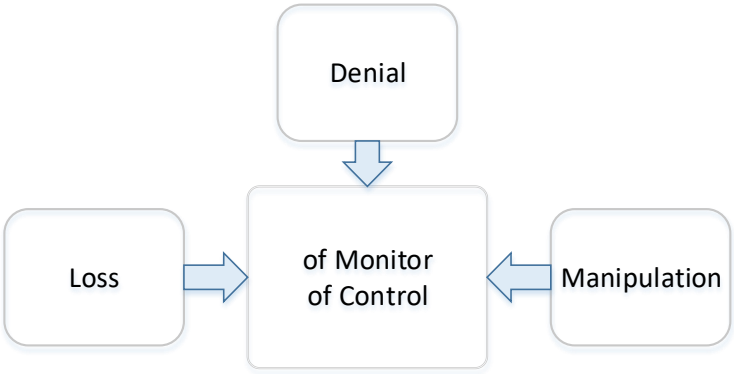

Figure 2. BACS Consequences to Realized Threats

(Brooks, et al., 2018b, p. 125; Assante & Lee, 2015, p. 11)

The BACS Automation level provides the necessary connectivity and communications between the many field devices and equipment (for example, a light) to the Management level (for example, how and when the light is used). The Automation level typically applies an open industry communications protocol (Shang et al., 2014, p. 51) between devices and gateways. In practice, the Automation level is an industrial control network, designed, installed and maintained by facility engineers and installers or integrators. Data generated at this level is normally distributed across its entire system network.

The automation communications network is the core of a BACS, providing facility and device-wide connectivity. However such connectivity, including embedded data entry access points, results in a degree of vulnerability that can be exploited. The Automation level vulnerabilities range from physical access to devices (Controllers) to highly technical remote cyber-attack (*Brooks,* et al., 2018a; Wyman, 2017).

Unlike the Automation level, both the Management and Field Device levels are less prone to exploitable vulnerabilities. At the Management level, an assumption exists that in part, the Information Technology professionals provides a commensurate level of cybersecurity protection. At the Field level, devices are isolated and realized threats generally result in restricted and somewhat isolated impacts. Management level vulnerabilities range from physical access to workstations to remote hacking via the corporate network. Whereas, the Field level vulnerabilities range from device destruction to remote control.

Generic risks to BACS can be presented at the architectural levels, which provide oversight of the more significant and critical risks. According to Brooks, et al., (2018b), the most significant critical and high risks (red and orange) lie within the Automation level, followed by moderate risks (yellow) at the Management level, and low (green) risks at the Field Device level.

Table 1 Generic BACS Risks

	BACS Architectural levels		
	Field Device	**Automation**	**Management**

Device	Low Risk	Critical Risk	Moderate Risk
Network	Low Risk	High Risk	Moderate Risk
Software (Application)	Very Low Risk	High Risk	Moderate Risk

(Brooks, et al., 2018b, p. 125)

MATERIALS AND METHOD

To uncover practitioner comprehension and practice relating to BACS security vulnerabilities and mitigations, this project applied a critical literature critique followed by an online survey. The online survey was sent to 13,803 randomly selected security and building owner/operator professionals from ASIS International, Building Owners and Operators Association (BOMA), and the Security Industry Association (SIA) memberships (see Table 2). The total response rate was 2.4 percent (n = 331).

Table 2. Survey Response Rates and Distribution

Association	Distributed	Population[2]	Response	Rate (%)
ASIS International	5379	35,000	240[1]	3.06%
Security Industry Association (SIA)	2469	1,000		
Building Owners & Operators Association (BOMA)	5955	10,000	91	1.53%
Overall	13,803	46,000	331	2.40%

Note: 1. Respondents noted their professional practice area, resulting in not being to identify their security association membership. Therefore, the security associations are a combined data set. 2. BOMA and SIA are based on organisational membership, resulting in an estimation of members.

The survey consisted of 18 questions and gathered data on respondents' role, understanding, and knowledge of BACS vulnerabilities and mitigation practices. The survey contained mixed response questions, including yes/no, Likert and self-response open questions. Data were collected as both quantitative measures and qualitative self-directed text. The survey followed a logic path, which at certain points removed respondents from having to address certain questions that they felt they did not understand. This approach provided a number of benefits, such as removing respondents whose poor understanding of a particular question might result in random responses, as well as reducing completion time.

Respondents were first asked their job function, including Security, Building Owner/Operator, Consultant or Other. Depending upon the response, a selection of job roles related to the selected job function was displayed. Respondents were then asked whether they were aware of the different levels of BACS architecture. Those who responded *yes* were asked to rate their level of understanding of each of the three architecture levels on a Likert scale from very low to very high. Respondents who indicated that they did not have an understanding of BACS architecture were directed to later questions.

All respondents were asked whether or not BACS vulnerabilities featured in their group risk register. They also rated, on a Likert scale (strongly agree to strongly disagree, with a further 'don't know' option), the positive impact of BACS with a free text field for positive and negative impacts. Respondents were also asked whether or not they were responsible for a BACS. Those that indicated *yes* were asked about their role in relation to BACS security. All respondents were asked whether security systems were integrated

with BACS, and which systems these were. Finally, respondents rated the level of criticality of 23 BACS vulnerabilities on a 7-point Likert scale; the levels at which they applied different mitigation strategies; and which stakeholder groups they engaged with.

RESULTS

The collected survey data was analysed using a variety of statistical techniques to gain an understanding of professional awareness of BACS security. Respondents came from 38 nation states, with the majority from the Unites States (73%), followed by the United Kingdom (5%) and Canada (4%). The assumption was that BOMA and SIA respondents, given their geographical membership, had a higher proportion of United States respondents. However, ASIS gained respondents from a wider geographic sample. The majority of respondents undertook a security function (72%), with building owners and operators accounting for the remainder (28%).

Security & Building Professionals Awareness

Two-thirds (75%) of respondents believed that they had an awareness of the various hardware and logical levels of BACS architecture. Such awareness was further supported by the overall median understanding of the three BACS architecture levels, which was reported as being "somewhat high". Furthermore, 45 percent of the respondents stated that BACS vulnerabilities are included in their group risk register. The inclusion of BACS into a risk register was reported by 27 percent of building owner/operators and 41 percent of security professionals.

Nevertheless, such a *high* level of confidence in awareness and an almost 50 percent inclusion of BACS vulnerabilities in risk registers was contradicted by the assessed criticality of BACS vulnerabilities across all 23 assessed BACS vulnerabilities. The BACS vulnerabilities were viewed as being of relatively equal criticality. In addition, that there was little or no difference ($M = 5.82$, $SD = 1.75$ to $M = 4.81$, $SD = 1.76$) between vulnerabilities. In other words, physical access to the controller or manipulation of a sensor or actuator were of an equal criticality as a cyber-attack on a Management level device. Despite 75 percent of respondents reporting they had an awareness of BACS architecture, the neutral (and arguably inappropriate) responses suggest that many respondents did not understand the criticality of the BACS vulnerabilities.

The lack of differentiation between the criticality of BACS vulnerabilities also persisted within the job function groups, although some differences were found in the significance weighting *between* these groups. For example, building owners or operators indicated 59 percent of BACS vulnerabilities were critical, as opposed to 33 percent of security professionals. Such variance suggested culturally defined differences in the perception of BACS between the various professional groups.

Greater accuracy in the perception of the BACS vulnerabilities were found to be held by the more technical practitioners ($M = 5.14$, $SD = 1.73$ to $M = 2.57$, $SD = 1.76$). This group included integrators and cybersecurity professionals, making up an expert group ($n = 10$) who demonstrated an awareness of the different criticalities of BACS vulnerabilities. The group's mean perceptions of the criticality of the different BACS vulnerabilities aligned with the findings from the literature, which concluded that the greater risks lie in the Automation level with the BACS Controller.

Level of Professional Responsibilities

When respondents were asked whether they are responsible for a BACS, the overall level of responsibility was found to be low (15%). Among those indicating that they are responsible for a BACS were 36 percent of building owner or operators and 10 percent of security professionals. These results indicated that there was little direct responsibility for BACS and given that 75 percent of participants claimed *some* awareness of BACS architecture, this suggested greater use than responsibility among the professionals.

BACS responsibility within each job function group was supported by the additional finding that 33 percent of all building owners or operators, and 7 percent of all security professionals surveyed, indicated that they:

1. Regularly discuss potential vulnerabilities within their BACS with other managers;
2. Regularly work with, manage, oversee, or make recommendations relating to a BACS; and
3. Regularly provide protective advice in regard to BACS vulnerabilities.

Together, these findings indicated that responsibility for BACS was largely outside the security professionals' responsibilities; rather, with a relatively small group of building owners or operators.

Security Integration into BACS

When the degree of security system integration into BACS was examined, the results indicated that half (51%) had some security system integration. Although this suggested that there is currently a reasonable level of security system integration into BACS, the data provided limited understating of the level and type of security integration. Of concern was the difference in the level of security system integration between the security professionals (52% reporting integration) and building owners or operators (19% reporting integration). These differences further support the suggestion of culturally defined differences arising from occupational perspectives of BACS.

Respondents who reported BACS security systems integration were also asked about the types of security systems. The systems reported as being integrated were found to differ between the job function groups, further suggesting a culturally defined focus on different aspects of either BACS or security systems. For example, security professionals primarily reported duress (62%), intruder alarm (60%), CCTV (51%) and electronic access control (51%) as being the most common integrated security systems. In contrast, building owners or operator professionals primarily selected *other* (60%), and reported non-security related systems such as HVAC, fire systems and lift control (Table 3).

Table 3. Security System Reported Integration with BACS by Function

Systems	Building Owner/Operator	Security	Total
Electronic access control	19%	51%	**26%**
CCTV	14%	51%	**19%**
Intruder alarm	11%	60%	**13%**
Security lighting	19%	39%	**15%**
Duress	8%	63%	**9%**
Incident reporting	7%	40%	**6%**
Intercom	24%	29%	**8%**
Radios	17%	33%	**2%**
Other[1]	60%	0%	**2%**

Note: 1. Other systems reported: HVAC, fire systems and lift control

The security systems of duress (8% to 63%; n = 52), intruder alarm (11% to 60%; n =49), CCTV (14% to 51%; n = 37) and electronic access control (19% to 51%; n = 32) had a diverse response to BACS "integration" between the professional groups. Such variation in the understanding indicates that *integration* means different things to different professionals. For example, is the "once only" entry of staff employment information that subsequently propagates through the enterprise system into the security access card considered integration? In contrast, is a hard-wired connection between systems integration? This outcome highlights definitional and semantic issues that results in the ability to define BACS and integration as problematic. As such, the data provides a limited understating of the level of security integration into BACS.

Most Critical BACS Vulnerabilities

When respondents were asked to rate the criticality of 23 BACS vulnerabilities, the mean criticality rating of each vulnerability was relatively equal. Although two-thirds of respondents indicated an awareness of BACS architecture, this contradicted the overall mean responses to the criticality of different vulnerabilities across the BACS Automation, Management and Field device levels. The results indicated a perception of equivalence of criticality for all BACS vulnerabilities (Figures 3 and 4), which also persisted when each job function group was examined individually. For example, approximately 60 percent of building owners or operators in a simplified 2-scale analysis rated all vulnerabilities as significant, followed by 30 percent of security professionals. Equivalence of responses to all vulnerabilities are displayed with trend lines.

These results display how each professional group provided a homogenous rating to the BACS vulnerabilities. The perception of equality of vulnerabilities demonstrated a lack of robust understanding of which BACS hardware or software is likely to be more or less vulnerable than other parts. Importantly, it indicates a lack of understanding of which parts of the BACS architecture are more critical to maintain operations, and may therefore require greater protection.

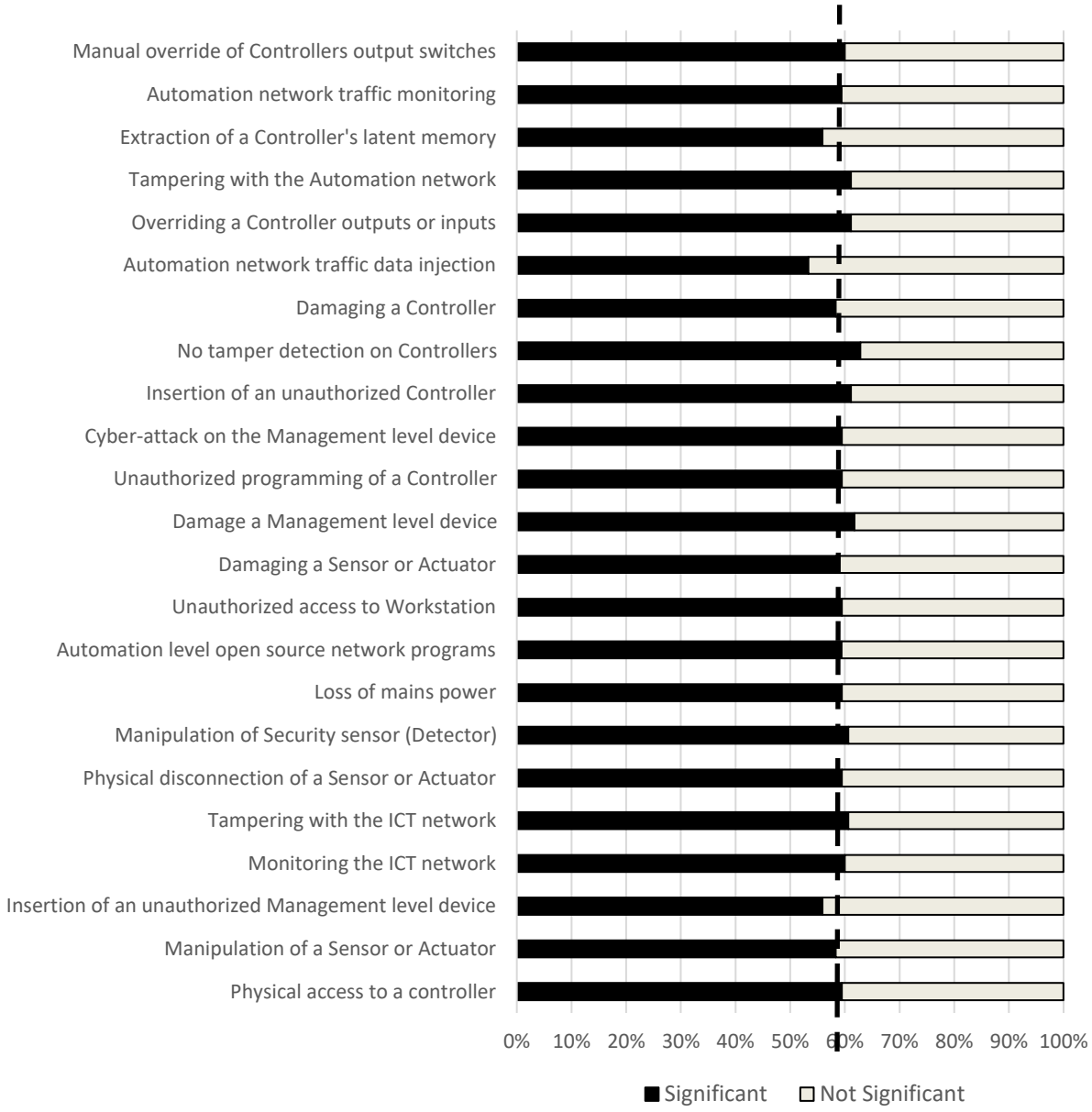

Figure 3. Perceived Criticality Significance of BACS Vulnerabilities by Building Owner or Operators

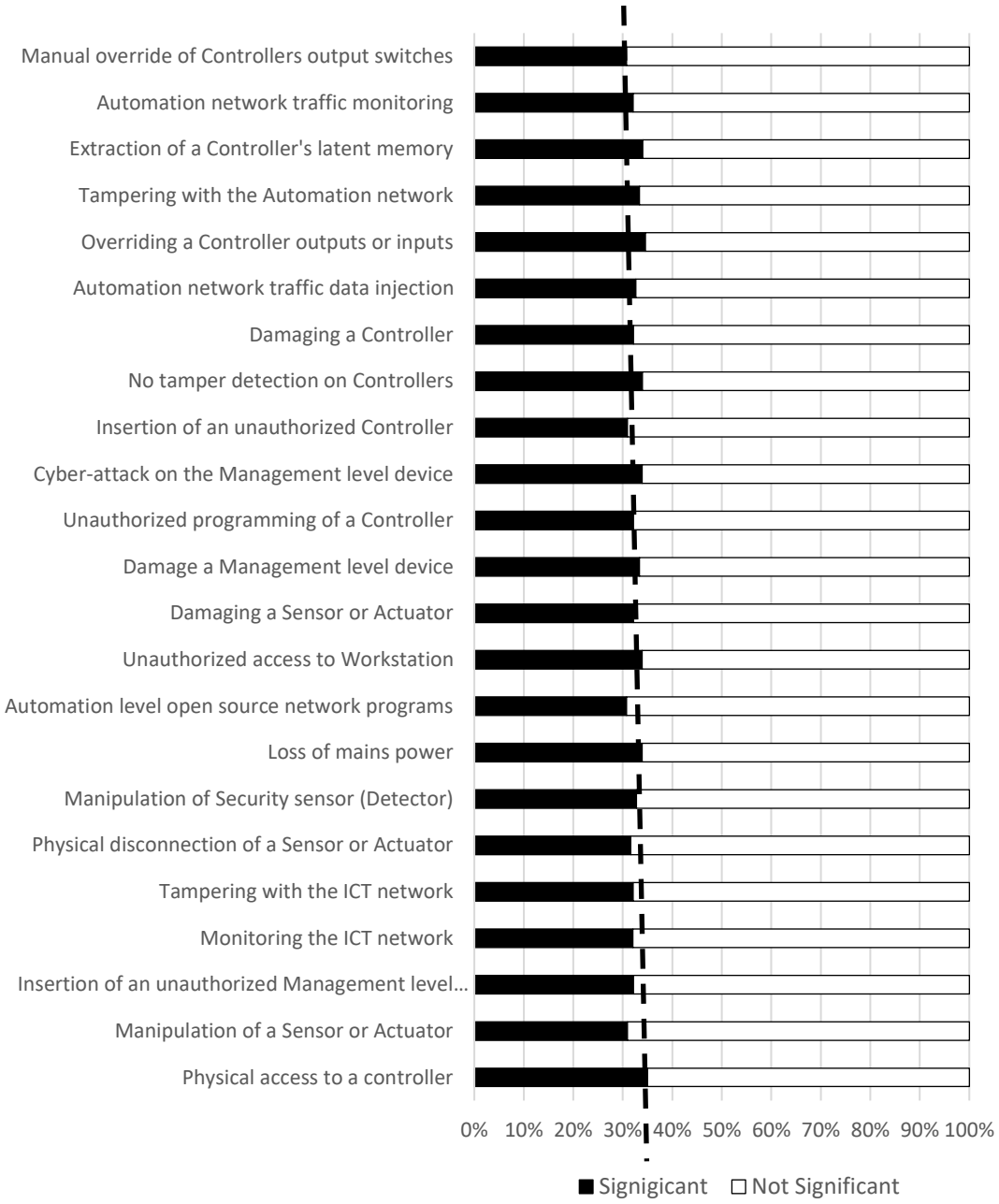

Figure 4. Perceived Criticality Significance of BACS Vulnerabilities by Security

Expert BACS Group

The expert group, consisting of cybersecurity and technical security professionals such as integrators or security engineering design specialists, provided criticality ratings of the 23 BACS vulnerabilities and displayed a greater awareness in variation (Figure 5). As Figure 5 indicates with a trend line, unlike the other job function group figures (see Figures 3 and 4) there is a distinct difference between the most significant and least significant critical vulnerability.

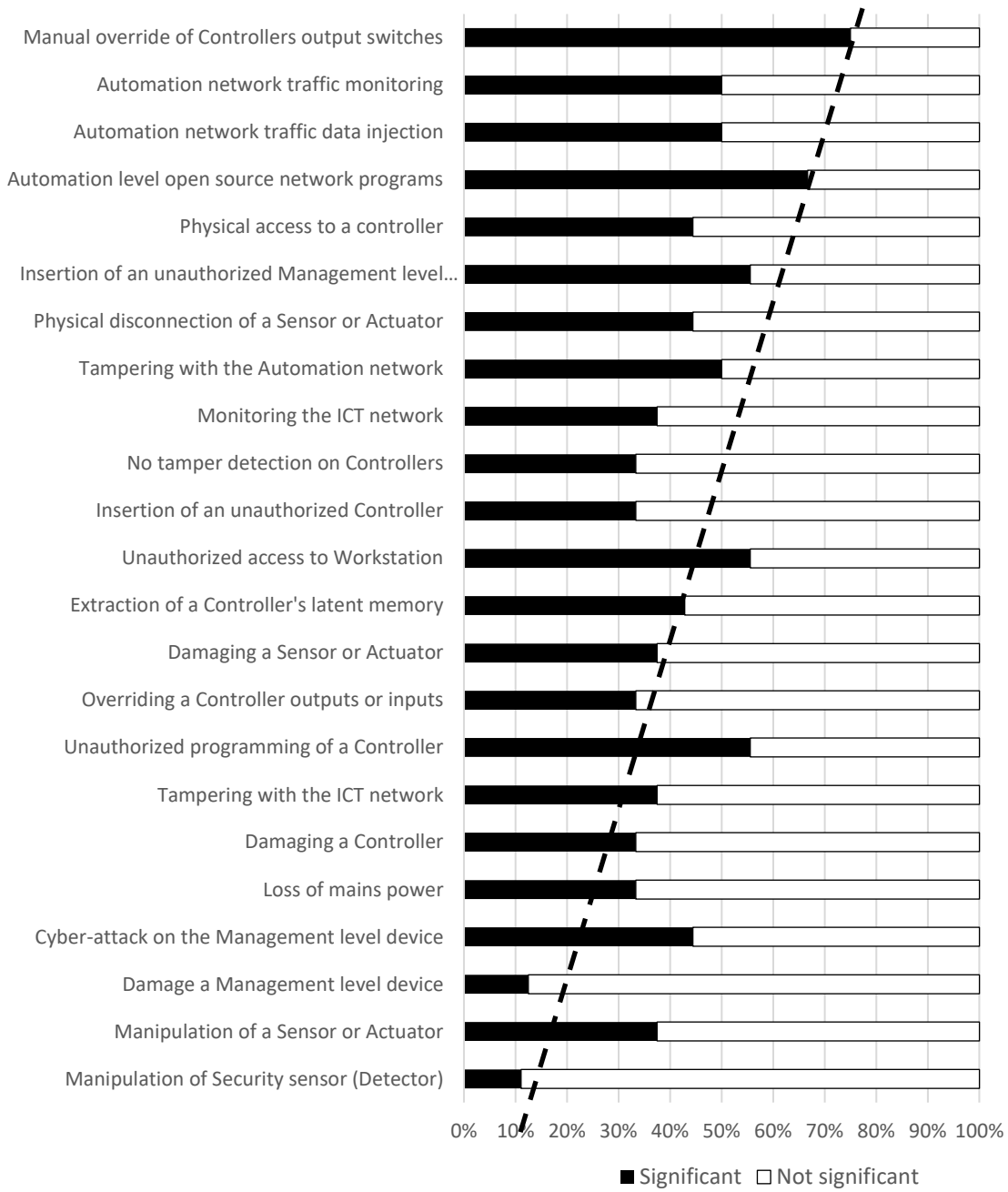

Figure 5. Perceived Criticality Significance of BACS Vulnerabilities by the Expert Group

Examination of the mean and median criticality of each vulnerability (see Table 4) revealed that the expert group demonstrated the greatest level of awareness of BACS vulnerabilities, rating manual override of Controller output switches as the most critical vulnerability. In contrast, security professionals cited cyber-attack on the Management level device as the most critical BACS vulnerability, while building owners or operators cited tampering with the Automation network.

Significantly, the expert group also expressed a wider range of criticality ratings to BACS vulnerabilities (34.4% difference between least and most critical) when compared with building owners or operators (18%) and security professionals (19%). These differences further supported the view that the expert group held the most accurate and nuanced understanding of BACS vulnerabilities. For example, the majority of critical concerns were located at the BACS architectural level of Automation.

Although this expert group was small (n = 10), they nevertheless held congruent views. For example, vulnerabilities such as insertion of a rogue Controller and unauthorized programming of the Controller were rated as a relatively low criticality, opposing the findings of the literature review (Table 4).

Table 4. Expert Group Ratings of Criticality of BACS Vulnerabilities in Highest Order

Level	Expert Group	Mean	Median	SD
Automation	Manual override of Controllers output switches	4.63	6	2.12
Field	Automation network traffic monitoring	4.38	4.5	2.23
Automation	Automation network traffic data injection	4.25	4.5	1.85
Automation	Automation level open source network programs	4.11	5	2.08
Automation	Physical access to a controller	3.89	4	1.91
Management	Insertion of an unauthorized Management level device	3.78	5	2.15
Field	Physical disconnection of a Sensor or Actuator	3.78	4	1.81
Automation	Tampering with the Automation network	3.75	4	2.38
Management	Monitoring the ICT network	3.75	4	2.05
Automation	No tamper detection on Controllers	3.56	4	1.95
Automation	Insertion of an unauthorized Controller	3.56	4	1.95
Management	Unauthorized access to Workstation	3.44	5	2.22
Automation	Extraction of a Controller's latent memory	3.43	4	2.19
Field	Damaging a Sensor or Actuator	3.38	3	1.93
Automation	Unauthorized programming of a Controller	3.22	4	2.04
Automation	Overriding a Controller outputs or inputs	3.22	3	2.2
Management	Tampering with the ICT network	3.13	2.5	2.2
Automation	Loss of mains power	3.11	1	2.47
Automation	Damaging a Controller	3.11	3	2.08
Management	Cyberattack on the Management level device	3	1	2.26
Management	Damage a Management level device	3	3.5	1.73
Field	Manipulation of a Sensor or Actuator	2.88	2.5	1.9
Field	Manipulation of Security sensor (Detector)	2.22	1	1.69

To assess statistically significant differences between the mean vulnerability perceptions of the security management, building owners or operator and expert groups, a one-way ANOVA between groups was undertaken. Using ANOVA enabled a comparison of the effect of role function (building owners/operators, security and expert group) on the criticality of 23 BACS vulnerabilities. Before undertaking the ANOVA, an inspection of skewness, kurtosis and Shapiro-Wilk statistics indicated that the assumption of normality was supported for each group, and Levene's statistic was non-significant, indicating homogeneity of variance was not violated. These tests indicated that no statistical assumptions related to running an ANOVA had been violated.

The results of the ANOVA indicated statistically significant differences between groups for 14 of the 23 BACS vulnerabilities, indicating that the level of criticality was influenced by role function for these vulnerabilities. Hochberg's GT2 ($\alpha = 0.05$) was selected as the post-hoc test, being more robust to the large differences between group sample sizes. The results of the Hochberg's post-hoc analysis revealed that building owners or operators and security management professionals generally perceived BACS vulnerabilities as more critical than the expert group.

The ANOVA results indicated that significant vulnerabilities with the largest magnitude of difference between the group's mean scores were those that the expert group rated as *less critical* than the other two groups, such as Manipulation of Security sensor (Detector) and Cyber-attack on the Management level device. Those vulnerabilities with no significant difference were those the expert group rated as *more* critical (and therefore closer to the consistent high ratings of the other two groups).

The difference between the groups is displayed (Table 5) by comparing the median vulnerability ratings for building owners (5.5 to 7), security professionals (5 to 6.5) and the expert group (1 to 6).

Table 5. Difference in BACS Vulnerability by Group

BACS Vulnerability	Security		Building Owner/Operator		Expert Group	
	Median	SD	Median	SD	Median	SD
Cyberattack on the Management level device	6.5	1.67	7	1.68	1	2.26
Manipulation of Security sensor (Detector)	6	1.77	7	1.75	1	1.69
Loss of mains power	5	1.97	6	1.95	1	2.47
Tampering with the ICT network	5	1.59	6	1.65	2.5	2.2
Manipulation of a Sensor or Actuator	5	1.71	6	1.8	2.5	1.9
Overriding a Controller outputs or inputs	6	1.9	6.5	1.41	3	2.2
Damaging a Controller	6	1.86	6	1.96	3	2.08
Damaging a Sensor or Actuator	6	1.78	5.5	1.95	3	1.93
Damage a Management level device	5	1.85	6	1.77	3.5	1.73
Unauthorized programming of a Controller	6	1.86	7	1.74	4	2.04
Tampering with the Automation network	6	1.98	**7**	1.53	4	2.38
No tamper detection on Controllers	6	1.89	6	1.9	4	1.95
Insertion of an unauthorized Controller	6	2.06	7	2.03	4	1.95
Physical access to a controller	6	1.91	6	2.05	4	1.91
Monitoring the ICT network	6	1.78	6	1.99	4	2.05
Extraction of a Controller's latent memory	6	1.87	6	2.08	4	2.19
Physical disconnection of a Sensor or Actuator	5	1.92	6	1.94	4	1.81
Automation network traffic monitoring	5	1.74	6	1.83	4.5	2.23
Automation network traffic data injection	5	2	6	1.84	4.5	1.85
Unauthorized access to Workstation	6	1.63	6	1.94	5	2.22
Insertion of an unauthorized Management level device	6	1.89	7	1.97	5	2.15
Automation level open source network programs	5	1.87	6	1.48	5	2.08
Manual override of Controllers output switches	6	1.75	6	1.9	6	2.12

BACS Mitigation Strategies

When asked which mitigation strategies were generally applied to BACS, respondents who identified themselves as security management professionals indicated the greatest level of practice and application of mitigation strategies (42%), followed by building owners or operators (25%). As with the BACS critical vulnerabilities, the majority of respondents generally rated the mitigation strategies as being relatively equal and with limited variance. For example, the security management professionals demonstrated a variance of 4 percent, building owners or operators a variance of 5 percent, and the expert group demonstrating the highest variance at 12 percent.

In order to determine whether there was statistical significant relationships between role function and the BACS application of each mitigation strategy, given the categorical nature of the mitigation strategy data a Pearson's chi-square test of contingencies ($\alpha = 0.05$) was selected. The chi-square test was found to be statistically significant for the application of guidelines and standards [χ^2 (4, N = 154) = 23.9, p < .001, V = 0.28], suggesting that the expert group were significantly more likely to apply guidelines and standards at the Field and Automation levels than the Management level. Likewise, this finding also suggested that security management professionals and building owner operators were significantly more likely to apply this mitigation strategy at the Management level.

The chi-square test was also statistically significant for physical security [χ^2 (4, N = 156) = 24.5, p < .001, V = 0.28], indicating that the expert group were significantly more likely to apply physical security mitigation strategies at the Automation level, whereas security management professionals and building owner operators were significantly more likely to apply this mitigation strategy at the Field and Management levels.

The degree of application of each mitigation strategy was then calculated for each job function, to determine whether there were any discernible differences between the respondents within each group. Results indicated that security management professionals, as would be expected, believed they apply the greatest level of security mitigation strategies; however, given the low level of their BACS responsibilities and neutral understanding of BACS critical vulnerabilities, this finding may be unreliable. A similar assumption may be applied to building owners or operators.

When the expert group's assessment of the mitigation strategies were isolated, it identified that they produced a similar conclusion (Table 6) to that drawn from the literature. For example, the most selected mitigation strategies by the expert group were security risk assessment, threat assessment, procedures, security awareness and continuity planning. The mitigation strategy of security risk assessment and threat assessment may be assimilated under security risk management, which may also include criticality assessment. However, there was a relatively low variance between the highest (52%) to the lowest (41%) applied strategy, with a relatively consistent agreement between respondents.

Table 6. Average Mitigation Strategy Application by Expert Group

	Expert Group	
Mitigation Strategy	**Average % Strategy Applied**	**SD (between levels of application)**
Procedures	52%	0.94
Threat assessment	52%	0.94
Security risk assessment	52%	1.25
Continuity planning	52%	1.25
Security awareness	52%	1.7
ITC security	48%	0.94
Guidelines/Standards	48%	1.25
Policy	48%	1.89
Recovery planning	48%	1.89
Maintenance	44%	0.82
Emergency response	44%	1.41
Tamper detection	44%	2.16
Auditing	44%	2.16
Electronic access control	41%	1.25

Intruder alarm	41%	1.7
Personnel security	41%	1.7
Physical security	41%	2.05

BUILDING AUTOMATION SECURITY AWARENESS

The study posed the following Research Question: *What are the security and facility professionals' comprehension of BACS, their vulnerabilities and criticalities, and resulting security mitigation practices?* In response, findings indicate that security management focused professionals and building owners or operators have limited technical understanding of the vulnerabilities and resulting security strategies necessary within a risk framework to protect buildings from BACS exploitation. Findings suggest that these two groups need to take guidance from the "expert" group of cybersecurity and technical security professionals in BACS security. The expert group had a more robust understanding of the vulnerabilities and resulting security strategies. Embedding their understanding into a risk framework for decision-making provides a more effective building protection from BACS exploitation.

Expert Group Membership

There were three distinct groups identified, being the expert group which comprises of (1) cybersecurity professionals, and (2) technical physical security professionals which includes integrators and engineering and design specialists, and (3) the security management and building owners or operator professionals. As discussed, the expert group cluster displayed a robust understanding of BACS vulnerabilities and resulting mitigations strategies. It is argued that this expert group held a higher level of technical understanding than the security management and building owners or operator groups due to the cumulative results of a number of factors, commencing with their greater technical training, generally in electrical and electronics engineering, and knowledge. Such technical knowledge underpins their ability to comprehend systems, displayed with most working on systems such as BACS but also IT networks and the many security technologies. Furthermore, for the past decade or more there has been a slow but progressive convergence of technologies that are both computer controlled and operated over computer networks. The sum of technical training, and knowledge and experience on technical systems, resulted in the expert group displaying such a greater level of BACS security understanding.

BACS Vulnerabilities and Criticalities

Building owners or operator professionals were found to have a greater level of BACS responsibilities, higher than security management professionals; however, overall there was an indication of greater use of BACS than direct portfolio responsibility among the managerial professions. Regardless of the level of responsibility, security managers and building owners and operators demonstrated limited understanding of the technical significance of BACS vulnerabilities and therefore, the appropriate mitigation strategies required to protect against malicious interference. This lack of understanding is significant, as those responsible for and interacting with BACS did not appear to appreciate their deficiency of knowledge in this area.

For the awareness of threats and risks associated with BACS, the study found that security management and building owners or operator professionals demonstrated a discordant connection between their *expressed* understanding of threats and risks, and the *revealed* understanding. Although 75 percent of security management and builder owners or operator professionals *claimed* to have an awareness of

BACS architecture and 48 percent feature BACS vulnerabilities in their group risk register, the majority of these professionals displayed a limited technical understanding of the criticality of BACS vulnerabilities. For example, most security management and builder owners or operator professionals rated the criticality of each BACS vulnerability relatively equally and with limited distinction. Such ratings indicated that a blanket approach of considering all vulnerabilities to be equally critical was generally applied by these two professional groups.

In contrast, the expert group of cybersecurity and technical security professionals such as integrators or security engineering design professionals displayed a much more diverse and accurate understanding of BACS vulnerabilities. This group indicated that some vulnerabilities, particularly at the Automation level, were more critical than others. Their understanding of critical BACS vulnerabilities correctly identified the greater risks as laying in the Automation level Controller (Brooks, 2013; Brooks, et al., 2018b; Granzer, Praus, & Kastner, 2009), a view which concurs with the literature.

A lack of awareness, knowledge and understanding of BACS vulnerabilities may be attributed to definitional issues based on role functions and the type of interaction with BACS. For example, diverse views on what types of security systems integrate into BACS are directed by the professional group being asked. Security professionals cited the most common BACS integrated security system as duress, intruder alarm, CCTV, and electronic access control. However, building owners or operator professionals cited intercom, electronic access control, lighting, radios, and CCTV as the most common BACS integrated security systems. The understanding of *integration* between security and builder owners or operator professionals lacks definition, likely leading to misunderstanding. The study also found that half of all reported BACS had integrated security systems. Although such security systems integration into BACS is likely too significantly increase in the future, the ability to define BACS is problematic and may lead to differing interpretations and perceptions of the level of security system integration between different job functions.

BACS Security Mitigation Practice

Results indicated that security management and building owners or operator professionals apply the most BACS mitigation strategies; however, as with BACS vulnerabilities, these were rated relatively equally and with limited variance. Therefore, findings suggests that security management professionals believe they apply the greatest number of security mitigation strategies, although given their low level of BACS responsibility and neutral understanding of BACS critical vulnerabilities, such an assertion is invalid.

Given the lack of revealed understanding of BACS criticalities and blanket approaches to security mitigation, no clear conclusion of which mitigation strategies the professionals apply could reliably be extracted. Nevertheless mitigation strategies were elicited from the expert group, who cited the five most significant BACS mitigation strategies as procedures, security risk management (threat, security risk and criticality assessments), continuity planning, security awareness and ITC security.

LIMITATIONS

There were several limitations identified in the study, such as terminology in language, distribution of sample and understanding of practice through the survey method. The first limitations relates to semantics and definitional issues. For example, differences in the term *integration* between security and builder owner/operator professionals may stem from a lack of universal nomenclature. Even through the data achieved a statically valid random population sample across the three associations, they were limited

even distribution across job function and the expert group was limited (n 10). In addition, survey logic resulted in different sample sizes for different questions. Such a sampling limitation should be noted when generalising findings.

No clear conclusion of what security mitigation strategies professionals apply could be extracted from the data, nor was the study able to determine the ideal security measures used by security and building owners or operator professionals. These issues were largely due to the homogenous rating of mitigation strategies, which may have been facilitated by the design of the survey mitigation question. The question asked participants whether they apply a particular mitigation strategy, which allowed them to select one or more BACS architecture levels (or alternately, select 'Don't know', although no respondent did this). Such an approach may have given the impression that the question was asking the participants to list the levels at which they believed the mitigation strategy *should* be applied. Although this may be a limitation of the study that influenced more homogeneous ratings of mitigation strategies, it is also interesting that no respondent used the 'Don't know' option.

CONCLUSION

Intelligent Buildings or Building Automation and Control Systems (BACS) are becoming more common in all parts of the built environment and its buildings. Increasing use of these systems are driven by the cumulative commercial need for increased functionality and flow of information throughout the building, to reduce operating costs, gain greater sustainability and have a more time responsive building. In general, the building operator has portfolio responsibility for BACS; however, their focus or knowledge is generally not the security of BACS. Therefore, there are potential significant security threats and risks from BACS to the organisation through loss, denial or manipulation of information or services.

This study applied an online survey to a sample of the professional memberships of security and building owners or operators associations to gather professionals' understanding and knowledge of BACS vulnerabilities and mitigation practices. The aim was to gain an understanding of both security and building owners or operator's comprehension and practice with BACS security.

The study found that the majority of the security management and building owners or operators had an awareness of and included BACS in their risk registers, although both groups lacked robust technical understanding. Professional understanding of a broad spectrum of BACS vulnerabilities were that they were of equal criticality, with limited variance. There was a blanket or generic approach to all BACS vulnerabilities, which resulted in strategies that were poorly targeted or provided limited risk mitigation. As with BACS vulnerabilities, mitigation strategies were considered with limited variance.

In contrast, there emerged a group of technical professionals who demonstrated a robust understanding of BACS vulnerabilities and resulting mitigation strategies, comprising of cybersecurity and technically focused security participants such as integrators and engineering design professionals. For example, this group rated BACS vulnerabilities with significant diversity (see Figure 5) across the BACS architectural levels. Consequently, there needs to be a greater awareness from security management and building owners or operators of BACS vulnerabilities and mitigation strategies that are risk based. In addition, security management and facility professionals need to better use the knowledge that technical professionals hold when considering BACS security at the design stage and ongoing management of built environment security.

Acknowledgement

This article was made possible by research funding and membership participation from: ASIS Foundation, Security Industry Association (SIA), and the Building Owners and Managers Association (BOMA). The research Report: Brooks, D. J., Coole, M., Haskell-Dowland, P., Griffith, M., & Lockhart, N. (2018b). *Building automation & control systems: An investigation into vulnerabilities, current practice & security management best practice*.

REFERENCES

Assante, M. J., & Lee, R. L. (2015). *The industrial control system cyber kill chain*. Singapore: SANS Institute. Retrieved from https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

Brooks, D. J. (2013). Security threats and risks of intelligent building systems: Protecting facilities from current and emerging vulnerabilities. In Christopher Laing, Atta Badii and Paul Vickers (Eds.). *Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection* (pp. 1-16). IGI Global. ISBN 978-14-66626-59-1

Brooks, D. J., Coole, M., Haskell-Dowland, P. (2018a). *Intelligent building management systems: Guidance for protecting organizations*. Alexandria, VA: ASIS Foundation.

Brooks, D. J., Coole, M., Haskell-Dowland, P., Griffith, M., & Lockhart, N. (2018b). *Building automation & control systems: An investigation into vulnerabilities, current practice & security management best practice*. Alexandria, VA: ASIS Foundation.

CIBSE. (2000). *Building control systems: CIBSE guide H*. Oxford: Butterworth-Heinemann.

Frost & Sullivan. (2008). *Bright green buildings: Convergence of green and intelligent buildings*. Retrieved from https://www.caba.org/CABA/DocumentLibrary/Public/Bright_Green_Buildings.aspx

Granzer, W., Praus, F., & Kastner, W. (2009). Security in building automation systems. IEEE *Transactions on Industrial Electronics*, *57*(11), 3622-3630.

High Performance HVAC. (2017). *Building automation systems*. Retrieved from http://highperformancehvac.com/building-automation-systems-hvac-control/

ISO. (2004). ISO 16484-2 *Building automation and control systems (BACS): Part 2 hardware*. Geneva: International Organization for Standardization.

ISO. (2007). ISO/IEC 14908-1 *Open data communication in building automation, controls and building management - control network protocol: Part 1 protocol stack*. Geneva: International Organization for Standardization.

King, R. O. N. (2016). Cyber security for intelligent buildings. *Engineering and Technology Reference*, 1-6, ISSN 2056-4007. DOI 10.1049/etr.2015.0115

Langston, C., & Lauge-Kristensen, R. (2002). *Strategic management of built facilities*. Boston: Butterworth-Heinemann. ISBN 978-07-50654-40-1

Marketsandmarkets. (2017). *Building automation system market by communication technology (wired, and wireless), offering (facilities management systems, security & access control systems, and*

fire protection systems), application, and region - global forecast to 2022 (SE2966). Retrieved from http://www.marketsandmarkets.com/Market-Reports/building-automation-control-systems-market-408.html

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *39*(2), 230-253. DOI 10.1518/001872097778543886

Sall, I. (2017). *Does IoT mean the death of the BMS?* Retrieved from http://www.facilitiesshow.com/does-iot-signal-death-bms

Schneider Electric TAC. (2004). *Product catalogue*. Schneider Electric.

Schneider Electric. (2015). *Guide to open protocols in building automation*. Andover, MA: Schneider Electric. Retrieved from https://blog.schneider-electric.com/wp-content/uploads/2015/11/SE-Protocols-Guide_A4_v21.pdf

Shang, W., Ding, Q., Marianantoni, A., Burke, J., & Zhang, L. (2014). Securing building management systems using named data networking. *IEEE Network*, *28*(3), 50-56. DOI 10.1109/MNET.2014.6843232

Sharples, S., Callaghan, V., & Clarke, G. (1999). A multi-agent architecture for intelligent building sensing and control. *Sensor Review*, *19*(2), 135-140. DOI 10.1108/02602289910266278

Simpson, J. A., & Weiner, E. S. C. (Eds.). (1989). *The Oxford English Dictionary* (2nd ed.). Oxford: Oxford University Press.

Sinopoli, J. (2012). *Security issues with integrated smart buildings*. Retrieved from http://www.automatedbuildings.com/news/dec12/articles/sinopoli/121119103101sinopoli.html

Technavio. (2016). *Global integrated building management systems market 2017-2021*. Retrieved from https://www.technavio.com/report/global-automation-global-integrated-building-management-systems-market-2017-2021?

TMR Analysis. (2017). *Commercial building automation market 2016-2024*. Retrieved from http://www.transparencymarketresearch.com/commercial-building-automation.html

Wyman, R. (2017). Consider the consequences: A powerful approach for reducing ICS cyber risk. *Cyber Security: A Peer Reviewed Journal*, *1*(1), 1-17.