CABA™ Continental Automated Buildings Association

Intelligent Building and Cybersecurity 2016

Landmark Research – Executive Summary

Connect to what's next™

www.caba.org

Presentation Contents

1. About CABA, Compass Intelligence & This Research
2. Research Funders
3. Methodology
4. Executive Summary

Intelligent Building and Cybersecurity: 2016 Landmark Research

This report was prepared for CABA by Compass Intelligence, LLC

About Compass Intelligence

Compass Intelligence is one of the leading market analytics and consulting firms specializing in metrics-driven market intelligence and consulting focused on the mobile, Internet of Things/M2M, green technology, and emerging technology markets. Compass Intelligence provides a number of key services including strategic advisory, market sizing/modeling, competitive benchmarking, executive-level consulting, and turn-key survey services. Providing quality services over 10 years, many of the top technology vendors rely on Compass Intelligence's expertise and insights to make better and more informed planning, strategy, and development decisions. Visit us at http://www.compassintelligence.com to learn more.

About CABA

The Continental Automated Buildings Association (CABA) is an international not-for-profit industry association, founded in 1988, dedicated to the advancement of connected home and building technologies. The organization is supported by an international membership of over 300 organizations involved in the design, manufacture, installation and retailing of products relating to home automation and building automation. Public organizations, including utilities and government are also members. CABA's mandate includes providing its members with networking and market research opportunities. CABA also encourages the development of industry standards and protocols, and leads cross-industry initiatives.

Intelligent Building and Cybersecurity Study Funders

Project Methodology & Survey Details

This project included a detailed review of the Intelligent Building and the impact specific to cybersecurity and cyber-attacks. This research included interviews, briefings, and secondary/primary research with vendors and organizations in the IB and Cybersecurity ecosystem. This project also include a survey of 500+ end-users and decision-makers.

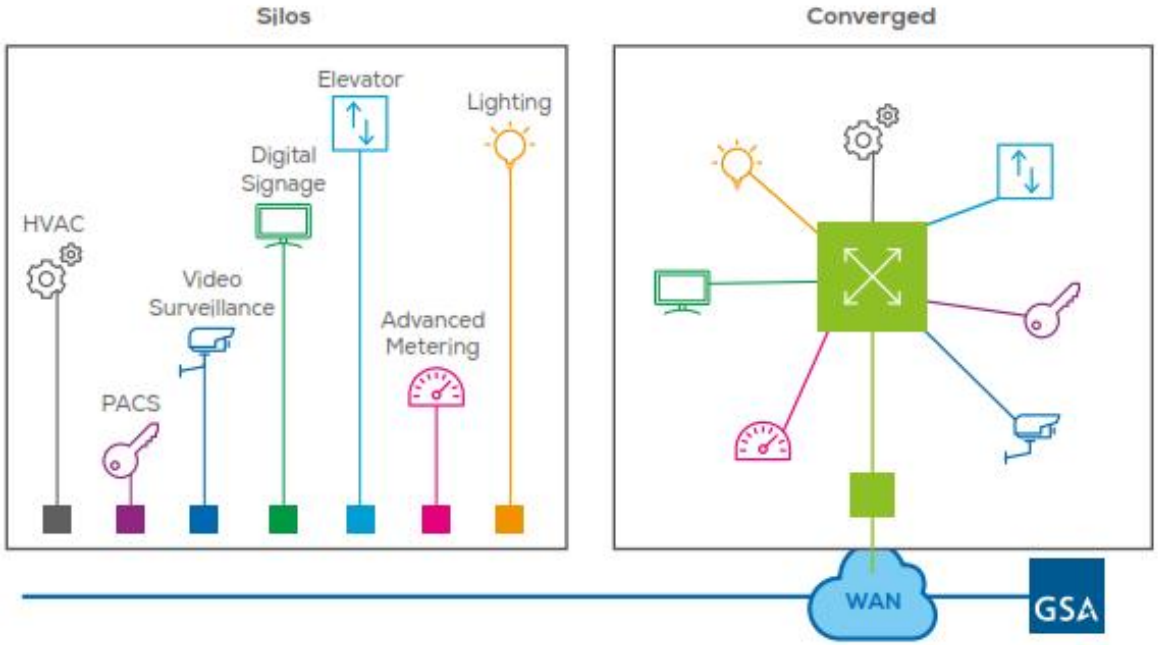
The survey research was conducted online using opt-in email lists from a well-regarded Internet research panel vendor and Compass Intelligence Thought Leaders Panel.

- The survey was conducted in August 2015.
- The survey involved 939 people who started the survey, 543 of these qualified for the survey and a total of 502 completed it in it's entirety.
- The survey ran for one week.
- Qualified respondents were over the age of 18, employed, involved in company's IT or facility management and currently have or plan to purchase Cybersecurity solutions.

Executive Summary

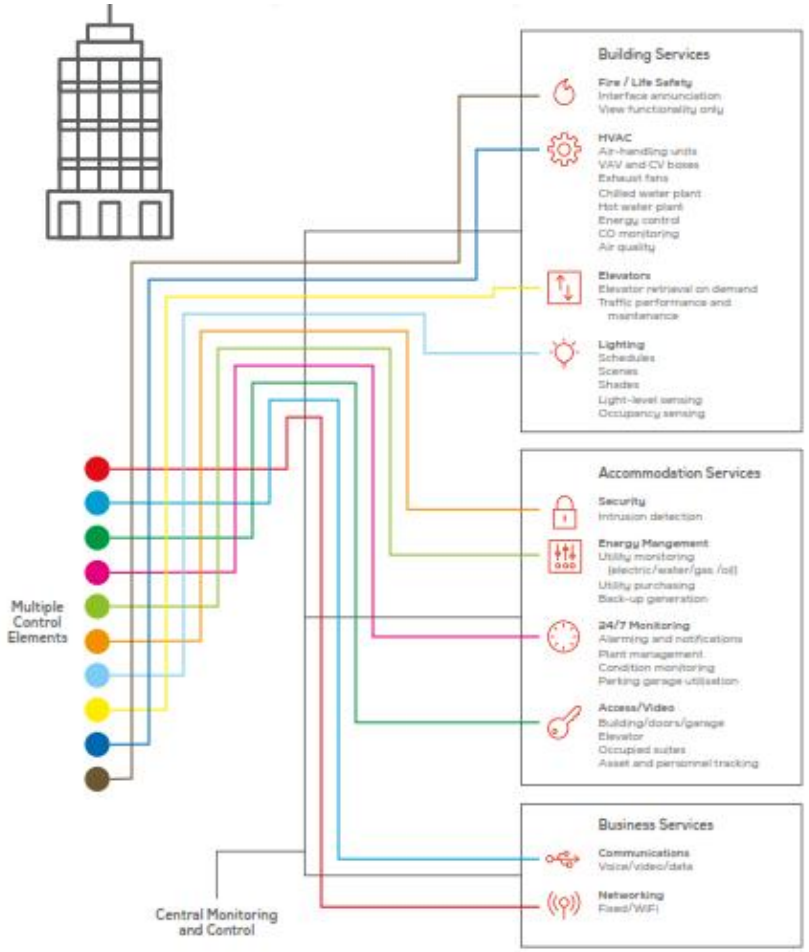
- Focus on improving operational efficiency and safety
  - Implementation in monitoring, automation, management of buildings
  - Enter BMA/BAS…
    - Building Management
    - Building Automation
- Advancement of IoT and M2M in BMA/BAS
  - Integration of IT and OT?
- Introduction of growing threats and potential for cyber-attacks
- Cost savings and reducing energy consumption, drivers for investment
- Cybersecurity becomes high priority as incidents and threat activity on the rise
  - Examples include Target breach through HVAC, Ukraine BlackEnergy malware incident, Hollywood Presbyterian Medical Center in LA crypto-ransomware cyber-attack

Standalone vs. Converged Building Systems



Source: https://www.wbdg.org/resources/cybersecurity.php

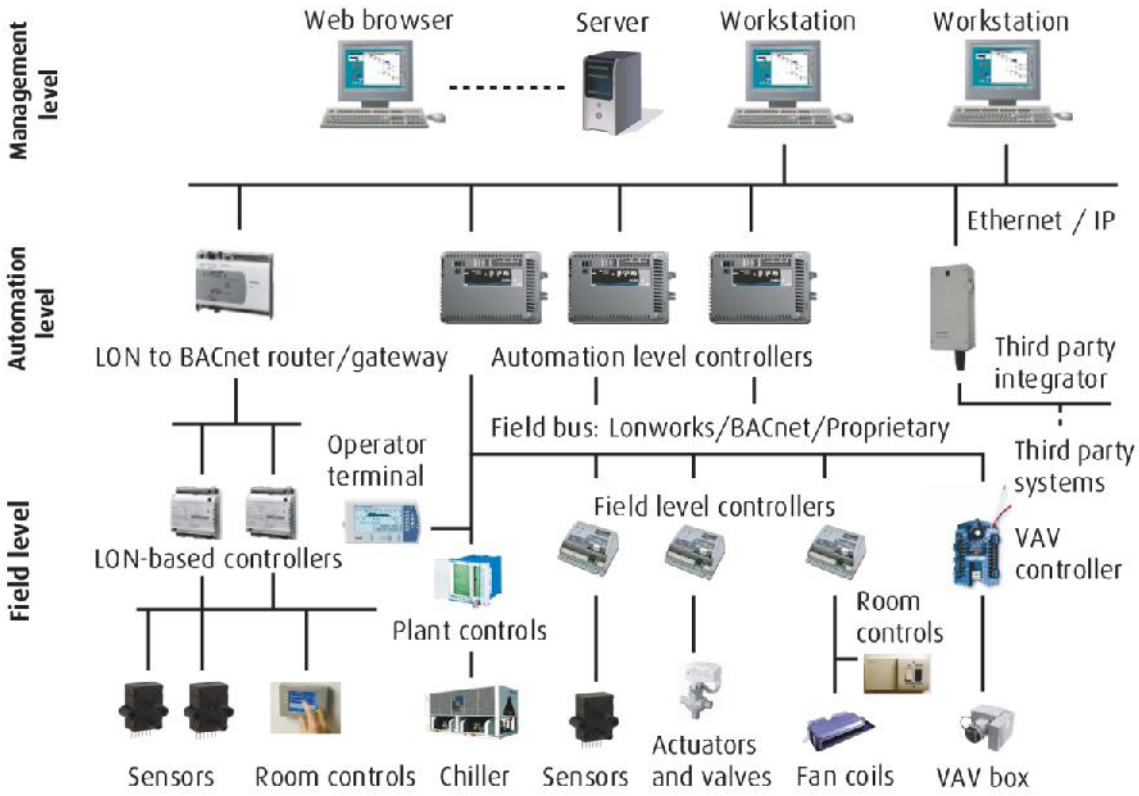
Intelligent Building Integrated Systems, Primary Touchpoints



- **Building Services**
  - *Fire safety*
  - *HVAC*
  - *Elevators*
  - *Lighting*
- **Accommodation Services**
  - *Physical security*
  - *Energy management*
  - *Monitoring*
  - *Access/video*
- **Business Services**
  - *Communications*
  - *Networking*

Source: The IET – The Institution of Engineering and Technology.

Building Management System (BMS)



Source: CABA's 2011 Smart Grid Impact on Intelligent Buildings & BSRIA.

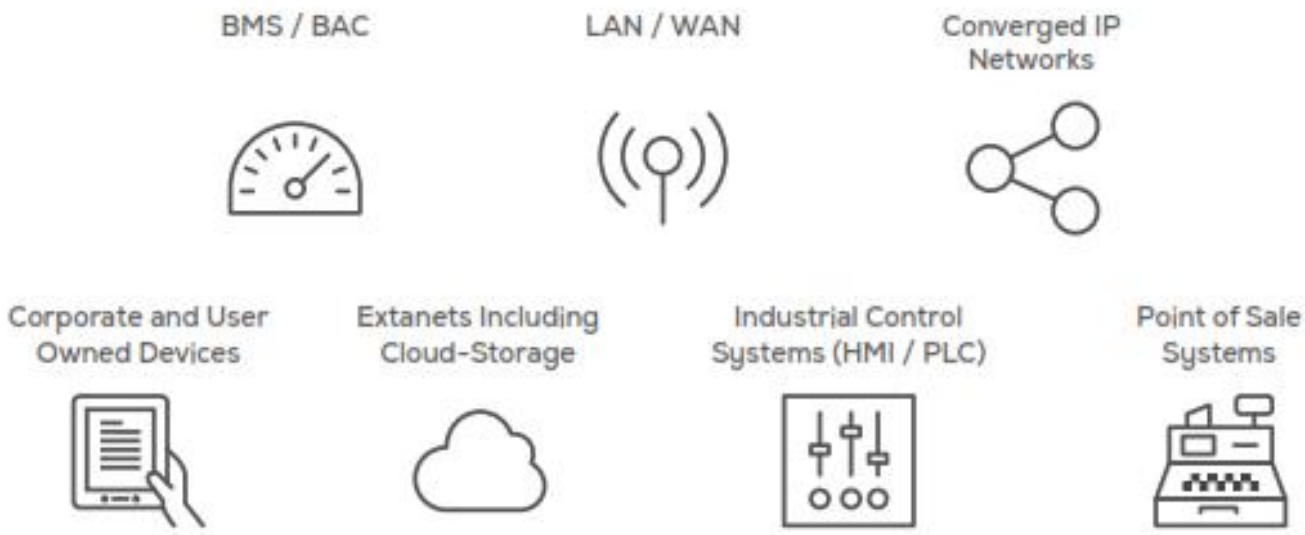
Other Background based on CABA previous studies

- Commercial and larger buildings more likely to implement and use BMS/BAS
- Industrial and Commercial buildings more likely to utilize BMS/BAS (primarily non-residential)
- Integration of Security and Other Building Systems including Access Control, CCTV, and Intruder Alarms (What's Next?)
- Cost savings and reducing energy consumption, drivers for investment

The Cybersecurity Ecosystem, 2016

Source: Compass Intelligence.

Selected Access Points for Cyber-Attacks – Where is the Risk?



Source: Compass Intelligence.

Protection Requirements

Full Assessment

- Processes, Systems, Tech

ID Types & Risk

- Network, Security, Spam, DoS

ID & Evaluate Threats

- Sources of Vulnerability
- Inside and External

Stakeholder Roles

- Priorities, Escalation
- Responsibilities

Coordination Across

- Stakeholders

Structured Audits

- Accountability and Review
- Adaptation

Source: Compass Intelligence.

Framework Core which includes a set of cybersecurity activities that are deemed common across various infrastructure sectors:

- Identify - Develop an organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
- Protect - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Recover - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event."

Source: National Institute of Standards and Technology, NIST

Key Recommendations & Final Thoughts

- Building owners and operators
  - Understand both intra and inter-system integration (IT and OT systems), including understanding the differences among industries and building types.
  - Understand and identify the preparedness level that is needed to protect against the risk of BMS/BAS-related cybersecurity.
- Strong collaboration and coordination is required among all building stakeholders, including building control systems' vendors and cybersecurity vendors.
- Stringent policies and procedures to guard both IT and OT against cybersecurity threats must be implemented. Cybersecurity is not just a technology issue; it is also a "people" issue.
  - A comprehensive cybersecurity plan is critical and must include all threats, including employees, tenants, and even ex-employees.
- Education of building owners and facility managers about cybersecurity issues.
- IP and cloud-enabled buildings - Need to protect and secure both the IT and OT networks
  - Security starts with the building systems companies and products, and it ends with the customer. Again, focus on securing endpoints, connectivity, applications/data, and implementing threat management solutions.

Action Items to implement today!

Policy Steps	
	VPN connections
	Unidirectional gateways
	Standards based security hardware and software
	Complex and routinely changing passwords
	Independent 3rd party audits
	Data encryption to ensure privacy and protection against data thefts
	Network monitoring and analysis tools that focus on network connections and traffic specifically related to OT
	NIST Framework and recommended whitelisting techniques that only provide access to approved/authorized parties

Final Word

"It is important to understand that cybersecurity protective measures that aim at proactively thwarting cyber-attacks, more so than simply monitoring and reporting, are likely to offer the best defense against such incidents/events. Proactive prevention offers a range of economic and non-economic benefits such as safeguarding infrastructure as well as organizational reputation."