GlobalData.

Through the Front or Back Door, Digital Transformation and the Smart Building Are Unavoidable

B. Washburn

September 9, 2016

GlobalData.

Through the Front or Back Door, Digital Transformation and the Smart Building Are Unavoidable

Perspective

Current Perspective

Australia's business sector has some leading practices when it comes to efficient use of building resources such as energy and water. That might not seem evident based on a 2016 GlobalData survey, which found enterprise respondents in Australia mostly unenthusiastic about adoption of new types of digital services that can streamline operations, increase efficiency and lower costs. Digital security (in the form of remote surveillance, motion detectors and other digital technology) did garner the interest of about half of respondents. But, most new digital capabilities, from energy management to waste management to predictive maintenance, only caught the interest of 13%-20% of respondents, and digital technology for asset tracking barely registered interest, at just 4% of businesses.

That may sound like lacklustre interest, but there is more going on here than meets the eye, as suppliers are bringing in their own digital transformation when they install expensive building systems such as heating/cooling and people movers. A smart facilities manager should be taking stock of these new types of systems as they come through the door, and at least start to document, assess and map these new incoming communications against interface and security policies they would prefer for in-building systems. Even if digital communications choices do not seem important to the business today, they are likely to become important in the future.

Key Takeways

Direct enterprise interest in smart buildings seems mediocre, but suppliers are already taking advantage of digital transformation to improve on their products and services.

The proliferation of facilities-related Internet of Things (IoT) calls for administrators to be proactive and plan an in-building communications strategy.

Like it or not, digital transformation is infiltrating facilities everywhere. No one will be completely spared from the smart building trend: office buildings, factory floors, classrooms, showrooms, trading floors, restaurants, laboratories, entertainment halls, warehouses. In fact, it makes sense to embrace the new intelligence, but with caution. The effects are, for the most part, positive. What are some key hallmarks of a smart building? Building management systems and building automation systems today handle the following types of tasks:

Efficient energy use, including heat, ventilation and air conditioning, and lighting.

Effective water usage and waste management.

Optimised internal transport (e.g., escalators and elevators).

Asset tracking, and possibly employee tracking to locate resources when needed.

Safety and security systems.

Communications infrastructure including structured cabling and wireless coverage.

Use-case enhancements such as collaboration and workflow.

Large building owners and office space facilities managers will already be familiar with Green Star certification from the Green Building Council of Australia (GBCA) and its obvious benefits, such as lower energy costs and reduced waste expenses. There is also the National Australian Built Environment Rating System (NABERS), which measures ongoing operational efficiency. A study by the Australian Property Institute notes indirect benefits too: for example, that these buildings can be healthier for their workers and they can improve workers' overall productivity levels. A lot of what goes into a green building is about proper design and use of eco-friendly materials. But, many elements that make a smart building also fit into existing locations and can help improve efficiency and lower facilities costs.

1. Big Systems Infiltrate the Intelligent Building

How pervasive are smart building practices to date? Overtly, not too big yet, as GlobalData discovered in a 2016 IoT investment survey. For Australia-based company respondents, only 15% to 20% of respondents are currently evaluating or deploying digital solutions to address topics such as energy management or waste management. While about half of respondents were looking into broader building security such as surveillance, going digital with predictive maintenance only garnered interest from 16% of respondents, and asset tracking a mere 4%.

But, don't be fooled by enterprise interest in these technologies seeming mediocre. These types of intelligent systems are already widely infiltrating buildings, with or without your permission. Large, expensive systems such as heating, ventilation and air conditioning (HVAC) are natural candidates to include sensors that monitor the system's health and other factors, such as air quality and system pressure, and to send this telemetry data back to the manufacturer. Elevators can monitor lift and door motors, and can alert to anomalous events, for rapid response when something goes wrong. Besides real-time response, these systems can analyse collected information and instruct technicians to perform the right preventative maintenance, meaning fewer service issues. Over the longer term, the manufacturer can pool and investigate all its collected product information, and use this information to correlate what is and isn't working out in the field. The result should be faster product iterations of better performing, more reliable systems.

Moving over to utilities, these companies likely already have deployed connected meters in or to the building, which can measure energy and water usage, and even compare the results to similar types of buildings in the same geographic area. As these utilities gather more (and more granular) data in real time, they might offer services that set alarm triggers and alert building managers to investigate when they detect an unanticipated surge (or slack) in consumption from the normal time-of-day and day-of-week pattern.

Other premium equipment on premises might want to 'phone home' regularly as well, to report on system health and alert their vendors of any issues. These might include large-scale printers, copiers or scanners, bulk mailers, or specialised machinery used on a manufacturing floor or in a hospital. As above, vendors benefit from real-time information about their platforms in the field, both to provide better service and to improve their products.

2. Building Connectivity, Security Issues

There are several wrinkles to all this intelligence that is finding its way into building operations. Smart systems are connected systems, and they need to communicate back to the manufacturer. Everyone might agree that connectivity is key to digital transformation, but beyond that vendors are scattering in all technology directions.

Many devices will support a physical cable (e.g., an RJ-45 Ethernet port); some will ship with an on-board SIM card and some form of cellular data connection. Still others may default to short-range communications such as WiFi, or possibly even Bluetooth or ZigBee. Some systems might start with near-field communications/RFID tag readers and then feed the data into a wireless or wireline connection. SigFox and LoRa are emerging wireless standards specific for IoT, and cellular intends to respond with its own 5G/NB-IoT specification. What this alphabet soup of standards ultimately means is that building owners can end up with a scattered mess of communications, with each machine trying to pass its own information in its own way into and out of the building.

There are several dimensions to possible security concerns, too. No one wants an expensive machine to have open ports that can be compromised, to have systems taken over and/or vandalised; no one wants unencrypted and unsecured data intercepted. If a partner cloud vendor does not have a rigorous security policy and IT is not following a robust security policy, data could be compromised. A breach into a building management system could be a back door into accessing corporate data. It is important that that security is holistic and considers the different types of vulnerabilities from external hackers to the carless, targeted or malicious insider. Building connectivity and security needs to be holistic.

3. Proactive Response

Fortunately, a facilities manager doesn't have to deal with all the challenges of going digital all at once, but it is important to set a digital policy framework. Many expensive devices will have more than one connectivity option. It makes sense to use wireline where it is available and require wireless to be shut off by default; and to ensure wireless is locked down if it is the only option (e.g., by specifying the device may only connect through cellular VPN, or only connect through an assigned secure WiFi hotspot, and never public WiFi). The idea is to foster an environment that is friendly to these new digital devices, but also identifies them and helps manage how they connect with the outside world.

Recommended Actions

Vendor Actions

First, a facilities manager needs to be receptive about real-time communications interfaces to expensive machinery on site. That can provide real-time status reports and alarms, and offer remote management. A dedicated small screen physically attached to the machine, or a dedicated proprietary console that ships with the equipment, is inadequate for truly remote monitoring, troubleshooting and management.

Start-up company Tile shows what is possible with relatively inexpensive, WiFi-based device location tags. That application focuses on finding devices when they are lost or stolen across town, or in another country, but the technology can apply just as well for finding expensive lab or medical machinery that could be anywhere in a large building or campus covered with managed WiFi. Technologies that support asset management and location-based services and can apply security policy to support geo-fencing, for example, will be important for facilities management.

A facilities manager should work with the rest of IT to set some sort of company-wide digital policy framework, in terms of what sorts of connectivity interfaces are preferred, which are acceptable and which are not acceptable for the device automation. These should include security policies that are checked and enforced, to prevent possible hijacking of equipment controls or unauthorised access to machine data.

If nothing else, a facilities manager should be aware of the digital communications that purchased or upgraded equipment can deliver. Even if the digital capabilities are remotely administered by a third-party management and maintenance contract, or even if the facilities manager keeps the communications components turned off, the administrator should keep a record of available capabilities. At some point in the future, that could be extremely helpful when the business decides to kick-start an intelligent building strategy.

Basingstoke

4th Floor, Northern Cross
Basing View, Basingstoke,
Hampshire, RG21 4EB,
UK
+44 (0) 1256 394224

Beijing

Room 2301 Building 4
Wanda Plaza, No 93 Jianguo Road
Chaoyang District
Bejing 100026, PR China
+86 10 6581 1794
+86 10 5820 4077

Boston

179 South St, Suite 200,
Boston, MA 02111
USA
+1 617 747 4100

Buenos Aires

Basavibaso 1328, 2nd Floor
Off 206, Buenos Aires, 1006
Argentina
+54 11 4311 5874

Dubai

Dubai Media City
Building 7, Floor 3, Office 308
PO Box 502635
Dubai
United Arab Emirates
+971 (0) 4391 3049

Hong Kong

1008 Shalin Galleria
18-24 Shan Mei Street
Fo Tan, New Territories
Hong Kong S.A.R
+852 2690 5200
+852 2690 5230

Hull

GlobalData PLC
Shirethorn House
37-43 Prospect Street
Hull
HU2 8PX

Hyderabad

2nd Floor, NSL Centrum,
Plot No-S1, Phase 1 & 2
KPHB Colony, Near: BSNL Office
Hyderabad-500072
Andhra Pradesh
+91-40-30706700

London

John Carpenter House
7 Carmelite Street
London
EC4Y 0BS
+44 (0) 207 936 6400

Madrid

C/Jesusa Lara, 29 – Atico J,
28250 Torrelodones Madrid,
Spain
+34 91 859 4886

Melbourne

Suite 1608
Exchange Tower
Business Centre
530 Little Collins Street
Melbourne
3000, Victoria, Australia
+61 (0)3 9909 7757
+61 (0)3 9909 7759

New York

441 Lexington Avenue,
New York, NY 10017
USA
+1 646 395 5460

San Francisco

Progressive Digital Media Inc
425 California Street
Suite 1300
San Francisco
CA
94104
USA
+1 415 800 0336

Seoul

Global Intelligence & Media Korea Limited
11th Floor, West Wing,
POSCO Center Building,
892, Daechi-4Dong,
Gangnam-Gu, Seoul 135-777
Republic Of Korea (South)
+82 2 559 0635
+82 2 559 0637

Shanghai

Room 408, Jing'an China
Tower No: 1701,
West Bejing Road
Jing'an District, 200040,
Shanghai, PR China
+86 (0)21 5157 2275(6)

Singapore

1 Finlayson Green
#09-10
049246
Singapore
+65 6383 4688
+65 6383 5433USA
+1 415 800 0336

Sydney

Level 2
63 York Street
Sydney
NSW 2000
Australia
+61 (0)2 8076 8800

Tokyo

Global Intelligence & Media Japan Tokoyo
Level 3,
Sanno Park Tower,
2-11-1 Nagata-cho,Chiyoda-ku,
Tokyo, 100-6162
Japan
+81 3 6205 3511
+81-3-6205-3521

Toronto

229 Yonge Street
Suite 400
Toronto
Ontario
M55B 1N9
Canada

Washington

21335 Signal Hill Plaza,
Suite 200, Sterling,
VA, 20164
+1 703 404 9200
877 787 8947 (Toll Free)