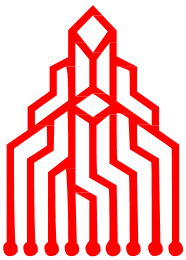
CABA Intelligent & Integrated Buildings Council (IIBC)

CABA White Paper

Cybersecurity in Smart Buildings: Preventing Vulnerability While Increasing Connectivity

Pramod E.F. Dribble, Frost & Sullivan
Raphael Imhof, Siemens Building Technologies
Udo Drafz, Siemens Building Technologies



CABA

www.caba.org

WORKING GROUP

Frost & Sullivan, Pramod E.F. Dribble

Siemens Building Technologies, Raphael Imhof

Siemens Building Technologies, Udo Drafz

ABOUT CABA

The Continental Automated Buildings Association (CABA) is an international not-for-profit industry association, founded in 1988, and dedicated to the advancement of intelligent home and intelligent 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 "Internet of Things, M2M, home automation and intelligent buildings". 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. CABA's collaborative research scope evolved and expanded into the CABA Research Program, which is directed by the CABA Board of Directors. The CABA Research Program's scope includes white papers and multi-client market research in both the Intelligent Buildings and Connected Home sectors. (http://www.CABA.org).

CABA Intelligent & Integrated Buildings Council

ABOUT CABA'S INTELLIGENT & INTEGRATED BUILDINGS COUNCIL (IIBC)

The CABA Intelligent & Integrated Buildings Council works to strengthen the large building automation industry through innovative technology-driven research projects. The Council was established in 2001 by CABA to specifically review opportunities, take strategic action and monitor initiatives that relate to integrated systems and automation in the large building sector. The Council's projects promote the next generation of intelligent building technologies and incorporates a holistic approach that optimizes building performance and savings. (http://www.CABA.org/iibc)

DISCLAIMER

This white paper was developed and published by CABA for the industry with permission from the authors. CABA expresses its appreciation to the authors and contributors for making this white paper available to be included as part of CABA's Members Library and CABA's Public Library. CABA, nor any other person acting on their behalf of CABA assumes any liability with respect to: the use of, or for damages resulting from the use of, any information, equipment, product, method or process disclosed in this white paper.

This CABA White Paper and other industry research reports can be found in CABA's Members Library and CABA's Public Library at: http://www.caba.org. This information is also keyword searchable. Contact the CABA office if you do not have the passwords to access this material by email caba@caba.org or phone 888.798.CABA [2222] or 613.686.1814 (x228). CABA encourages you to share this white paper with others in your organization and the industry. Permission is not required from CABA to share this white paper, as long as proper acknowledgment is provided to CABA.

PUBLICATION DATE: February 2015

Table of Contents

1. Why is Cybersecurity Necessary for Building Automation Systems/Smart Buildings?

What makes a building "smart" is also what makes it vulnerable. Sophisticated monitoring and control systems can deliver huge value to users; they make the building more efficient and keep occupants safe and comfortable. Current systems are a natural evolution from simple mechanical, pneumatic, and electrical controls —replacing traditional, siloed control with truly integrated data acquisition and analysis IT systems.

Until 2010, the terms "cybersecurity" and "hacking" mostly brought to mind breaches of credit card data or personal information. Industry and building management professionals thought it would never happen to them. After all, what could someone possibly accomplish by hacking into a building? [For the purposes of this paper, "hacking" includes only actions having nefarious or illegal intent.]

When the Stuxnet virus was discovered in 2010, the implications were immediately clear: industrial control systems (ICS) were no longer secure from hacking — protection through obscurity vanished.

Critical infrastructures such as power generation and distribution systems, refineries, and manufacturing systems have been successfully hacked —fortunately with little impact, though post-event analysis shows this is not for lack of effort.

The sophistication of hacking is evolving at an incredible pace, and cybersecurity developers are working to keep pace. Protective measures are becoming more efficient and effective, while hackers are becoming more sophisticated and creative. Although corporations have invested heavily in protecting critical infrastructure and securing their networks against espionage and theft of intellectual property, credit card, and personal data; the majority of IT personnel still believe they are vulnerable to hacking.

So what about the information and control systems that make a building smart? Have they been included in the protection envelope, or have they become the low-hanging fruit for a motivated hacker? Particularly vulnerable is the integration portion of smart building software, in which building automation is connected to fire and security, energy management, and other systems, and from which a skilled hacker could access nearly any system in a corporate network. Frost & Sullivan believes that the system of a smart building is moving into the sight of cyber attackers; this paper will show system vulnerabilities and potential damage, and help those responsible for smart building management.

2. Who is in Charge?

The role of a facilities manager, who generally is in charge of running a building, has evolved. While a building automation system (BAS) historically contained mechanical, pneumatic, or electromechanical controls, complex control systems have become the norm. Systems now contain more IT-based hardware for ever-increasing data exchange, and complex software to handle increased BAS functionality. Has the training for facility managers kept up with technological progress?

There is no evidence to suggest that a preponderance of facilities managers have access to the training necessary to effectively manage cybersecurity in smart buildings.

As smart buildings become more common, the BAS moves from the facilities and operations side into the IT realm. Is a facilities manager in the position to oversee the IT portion (including cybersecurity), or is that in better hands with an IT expert? And is an IT manager sufficiently skilled in cybersecurity specifically designed for smart buildings?

The conclusion of this white paper is that facilities managers should work with IT personnel to manage the high-tech aspects of BAS and the cybersecurity concerns that threaten them and, by extension, the rest of the organization. The correct approach is to use a combination of both professions to safeguard the BAS.

3. Cybersecurity Overview

The initial consideration for cybersecurity, like any type of security, is what must be protected and how an intruder would be able to gain access. It could be something as simple as accessing HVAC controls in an office space, where a hacker can change conditions to interfere with occupants' work. In this simple example, the measurable monetary damage is work interruption.

> It could be in a church, where an intruder uses the HVAC network to connect to the office network to gain access to parishioners' personal data.
>
> It could be a research laboratory in which a stable environment is critical; if compromised, years of research could be destroyed.
>
> It could be the cooling system to servers in an IT room.
>
> It could be the energy data of a building to indicate whether it is occupied.

Cybersecurity would prevent:

- Access to a fire system (allowing a false alarm triggering building evacuation).
- Access to a security system (allowing unauthorized access).
- Hijacking the BAS for blackmail (ransomware).
- Hijacking the BAS to damage property (increasing the temperature in a server room).
- Hijacking the BAS to destroy or steal sensitive laboratory research data.
- Hijacking the BAS to destroy environmentally sensitive products.

It is the system owners' responsibility to identify their critical assets.

The next step is to identify system vulnerabilities, including:

- Users
- Remote access
- Physical access
- Integration
- Wireless access
- Bring-your-own-device (BYOD) access

Finally, the system setup and the functionality must be clearly defined. What does the system need to perform as required? Considering these concerns will allow an asset manager to balance security, usability, and cost.

The safest system is one that is turned off. However, that is also the system that is least useful, making this a poor solution for the vast majority of applications. On the other end of the spectrum is a system with universal accessibility that is available to everyone from everywhere, providing and the greatest access to data. This system is obviously extremely insecure, and highly unadvisable.

The best system is somewhere in the middle, and depends on an organization's specific needs for security, accessibility, and use.

4. Considerations for Cyber Defense

A cybersecurity system can be visualized in layers — each requiring a different method to prevent the system from being compromised. The integration of these layers allows the system to be as secure as possible. Of course, cybersecurity is a moving target. The sophistication and frequency of cyberattacks is increasing, and no network can be truly hack-proof. A system operator's goal must be to implement protections that make the system prohibitively difficult to compromise, such that it does not justify the hacker's time and energy.

Cyber defense layers include:

- Identity validation
- Endpoint device security
- Network security
- Data security

5. Identity Validation

User access control is the most easily recognized aspect of cybersecurity. It involves user login credential verification and can include biometric checks, token cards, and personal identification numbers (PINs) in addition to the user login name and password. This area lends itself to inexpensive, highly effective improvement in an organization's overall cybersecurity level. It is typically the first line of defense for the network itself, and acts as a perimeter for sensitive, protected applications.

Simple steps that can greatly enhance system security include:

- Training: What is cybersecurity, and why is it important for your organization?
- Password standards: Strength requirements (some passwords are much harder for computers to "guess"), and individual, user-generated passwords that must be regularly changed.
- User lockout: If user credentials are entered incorrectly three times, the account automatically locks and sends a message to the system administrator.
- Default deletion: Automatic removal of all default account information.
- User account management: Ensure that only those who need access have it, and only at a certain level (least access rights management).

A system should be able to generate a user account report. This tool allows the system administrator to see everyone who has access to the system and decide whether they need that specific level of access (e.g., removing accounts of users who have left a company).

Group accounts are generally a bad idea — If 10 staff members use the same login credentials, how can individual actions be identified to determine accountability? Most systems provide reports about user activity. Managing user accounts is necessary to safeguard system operations.

6. Endpoint Device Security

Endpoint security is designed to provide security for all devices on the network, which include: mobile phones, tablets, laptops, printers, and personal computers. This area of cybersecurity is important, as hot-desking, hoteling, and bring-your-own-device (BYOD) are becoming increasingly cost-effective and popular. Endpoint security is important in smart buildings because adding nodes to the network increases both the number and variety of endpoints that could be targeted for unauthorized access. In the case of smart building systems that are linked to business processes, endpoint security is critical; maintaining a robust endpoint cybersecurity strategy is vital to extracting the maximum value of a smart building application.

Most malware is still distributed through Web sites and email phishing attacks; therefore, connecting an end device that can be used to browse the Internet and receive email attachments is a big security risk. The best strategy is to disallow BAS access from any device that has Internet and email capability.

Device ports also must be considered. If a BAS server has a USB port, it can be infected via a detachable storage device, this is the likely approach taken in the Stuxnet virus incident in 2010. A business system

can be infected by something the user brings from home, BYOM (bring your own malware). If there is a need to retrieve data from a personal endpoint device, secure methods include:

- Strictly managing its Internet and email capabilities.
- Disabling all ports, or allowing only use of company-certified devices (USB sticks).
- Using a data diode, which is a server that the BAS can send data to, but cannot be accessed.

Physical access security is the prevention of physical access to the network and its infrastructure by unauthorized persons. BAS network security includes sequestering server hardware in a location only accessible by maintenance personnel and the building operator, a strategy that can be employed for most critical hardware. If some of the network infrastructure is unprotected, multiple security strategies can be used:

- Device authentication
- Port authentication

With device authentication, the system has a list of devices that are permitted to connect to the network. If a device that is not on the list connects to the network, the router will not direct any data to or from it.

Port authentication locks or dedicates ports. If an 8-port router has only three ports in use, an intruder could plug a device into one of the remaining ports to access the system. Port authentication blocks data from being transmitted to or from those ports.

Sophisticated device security can not only prevent unauthorized devices and unauthorized ports to access the system, but can also detect unauthorized access attempts and send warning messages to the system operator.

7. Network Security

Network security prevents access to the system via the network itself. It is the practice of restricting access to a private network at its entry points. This involves firewalls, anti-virus programs, intrusion detection and prevention systems, and security information and event management programs. This security is generally concerned with access from outside the system. If a BAS network is not connected and does not share any network infrastructure hardware, then the system is protected by the air gap (isolation from unsecured networks). This means that an intruder must physically access the system to connect to it. This is a very-high security approach, but is not all that practical. A smart building does

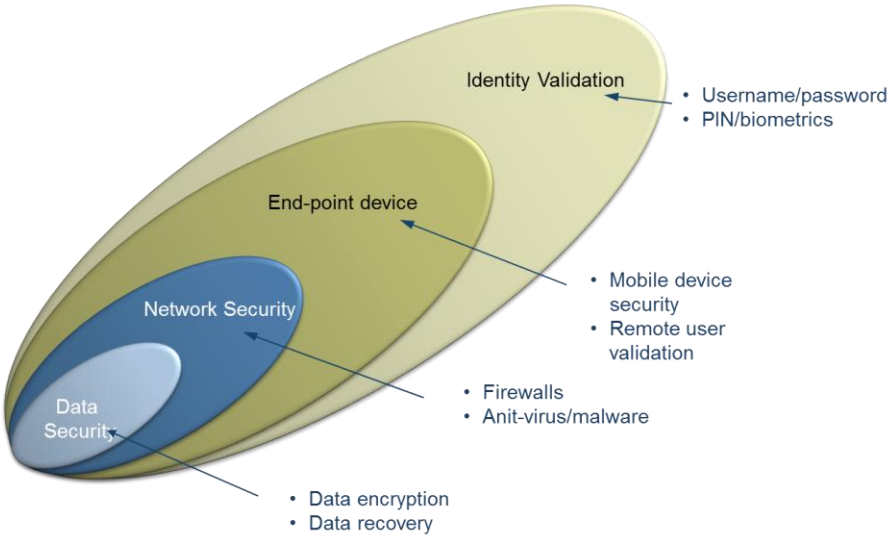
benefit from connections to other systems; a connection just for performance analyses or a remote login tool for building managers does not truly extract value.

Using the security layers discussed earlier, together with VLANs and VPNs, remote access can be secure. VPN firewalls can offer a simple, secure connection between two points: a communication tunnel is opened between two pieces of hardware that can identify themselves to each other. High-security VPN firewalls include functionality such as user and device authentication, multiple VPNs to secure access to the system by allowing only a dedicated connection.

After the connection is secure, data in transit (data transferred between two points) and data at rest (stored data) must be examined. The data in transit is vulnerable to a man-in-the-middle attack, when an attacker hacks into the Ethernet connection and copies data while it is being transferred between two end devices on the network. Encryption can offer protection, information encrypted by the sender and decrypted by the receiver, would make it difficult for a hacker to understand the data. Additionally, the man-in-the-middle attack is based on the intruder having access to the system in the first place. Several network security layers would make this type of attack more difficult.

Encryption is also a protection for data at rest, requiring an encryption key to make sense of the data. However, intruders can also use this to their advantage. Ransomware called Cryptolocker will encrypt all data until it becomes useless and demand ransom to obtain an encryption key. Post-event analyses of such malware attacks show that companies have paid ransoms in the range of hundreds of thousands of dollars to get the key.

Ideally, standard backup protection at set intervals should be used for important stored data. One copy should be kept off-site and disconnected from the system.



Source: Frost & Sullivan

A comprehensive and robust cybersecurity platform requires all of these features, but few programs perform all of the functions well. Owners, operators, and users of these systems in smart buildings typically do not have expertise in software, IT, or cybersecurity, and cannot adequately distinguish high-quality solutions from low-quality ones. This has given rise to companies that offer cybersecurity as a service, and present managed security to their clients. This approach can greatly simplify a building owner's effort and provide a figurative insurance policy in the event of a breach.

Most cybersecurity solutions are single-aspect applications. They protect from a single type of cyber threat, but do not provide a comprehensive defense. This creates a worst-case scenario of a company believing it is protected from cyber threats while remaining vulnerable to a variety of methods, and a best-case scenario of running a number of cybersecurity programs simultaneously, which is extremely inefficient.

The different layers of cybersecurity strategy are in response to a varied array of cyber threats. Generic terms for these threats are malware and hacking. Malware is an unauthorized program that degrades the network or prevents or alters its intended use. It may not be designed to steal information, but it can have that function. Hacking is the attempt to access secure networks or information without the permission of the owner/user.

Three main groups of cyber threats are defined based on the way they interact with data:

- Infiltration is the practice of gaining unauthorized access to the network, and damaging it, or stealing information, or a combination of the two. By far the greatest proportion of infiltration attempts involve remote-access applications that bypass or fool login credentials verification, endpoint security features, and network security applications. Other infiltration methods include using SQL injection, admin interfaces, remote file inclusion, authorization flaws, directory traversal, and insecure X.25 interfaces.

- Aggregation (man-in-the-middle attack) is when information is intercepted in transit by an unauthorized user. This type of hacking is called data harvesting.

- Exfiltration involves removing proprietary data from networks.

Infiltration, aggregation, and exfiltration further break down based on the methods used to interact with data.

Phishing is a simple form of infiltration, and relies on the naivety or ignorance of the user. It typically takes the form of an electronic communication or fake computer notification, leading the user to execute a malicious task on his or her system that then goes on to infect the network. Proper education on how to approach communication from unknown or questionable sources as well as procedures for software updates can completely negate this threat.

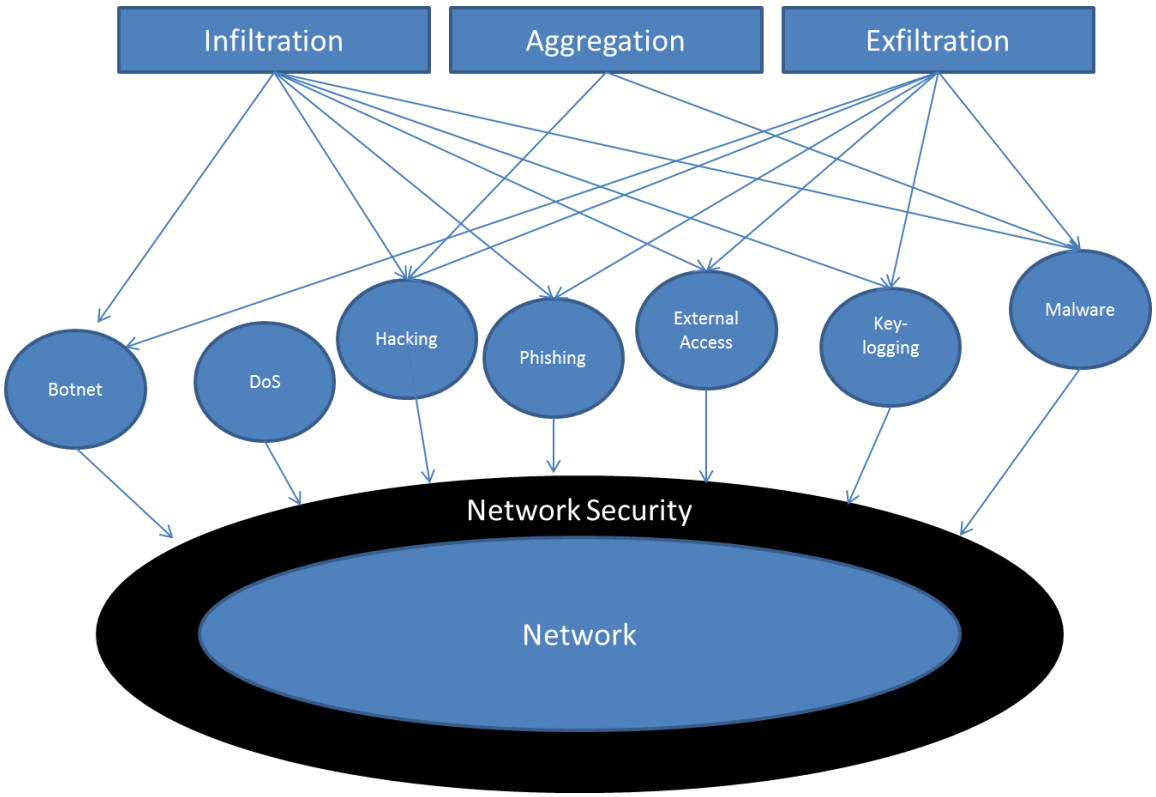
External access is another simple form of cyberattack, and can be either through infiltration, exfiltration, or a combination of the two. This method is when the unauthorized user gains physical access to network hardware and uploads or downloads proprietary information. This barely qualifies as a cyber threat because the physical security of a location must be lax or compromised to be a serious concern. This threat can be negated by restricting access to network hardware through a series of security checkpoints, and requiring identity verification and screening of possessions before access is granted.

Keystroke logging, or key-logging, is a more sophisticated form of cyber threat. It involves the recording of a user's keystroke history to extract username/password combinations and other sensitive information such as credit card or bank account numbers. This requires that a program called a key-logger be running on the target device, or that a piece of hardware be connected to the target device from which the key-logger can run. A key-logger allows a hacker to record login credentials and fully access the network once that barrier is overcome.

Denial-of-service (DoS) attacks are designed not to infiltrate a network, but rather to cause it to fail for a short period of time. Every network has a maximum number of requests it can process per second, and a DoS attack links many computers together until it can bombard the network with more requests than it can process, causing the network to slow down, fail, and shut down. The frequency of these attacks has increased in recent years, particularly against politically polarizing organizations. While these attacks are

less destructive than others, they can be coupled with infiltration tactics to target the network while some or all of its security features are compromised.

Some malicious programs set up a botnet system once they have breached the network. This creates a command-and-control architecture to direct and spread the infection within the network, making cleanup considerably more difficult, and damage potentially much greater.



Source: Frost & Sullivan

Some solutions to these attacks are low-cost and easily implemented.

Some hackers try to use “brute force” to access networks. This is essentially the high-tech version of trying every password combination within the parameters of the organization to thwart login credential verification. This threat can be easily negated by requiring that a user input the correct password within a set number of attempts, and locking the account after that number of incorrect attempts. Even if the attempt threshold is quite high, at 5 attempts for example, it severely restricts the effectiveness of a brute force approach.

Several measures can be implemented to secure current BAS installations. Many best practices are independent of BAS protocol and vendors. BAS systems need protection to avoid unauthorized use of the systems or use as a gateway to bridge into other customer systems, such as enterprise resource planning (ERP) or file servers. BAS systems are probably most vulnerable from attacks via the Internet. However, vulnerabilities from within the building must be considered as well.

Simple best practices can be applied for protection from Internet attacks. For example, BAS access can be restricted to VPN connections only. Use of a Web server-based human-machine interface (HMI) is recommended because it relies on IT technologies to secure access, and it restricts ports that need to be opened on a firewall. One common way to protect BAS systems from internal attacks is to segregate the BAS network from the IT backbone using VLAN IT technologies. However, common operational and behavioral procedures can help protect BAS systems as well. For example, good password etiquette, providing each user with an individual account, and keeping BAS software and firmware up to date can help to prevent attacks. Good password practices seem obvious, but an astonishing number of digital security breaches involve a user who did not change a password from “password.” Related to this, providing unique user accounts and implementing password standards (not allowing common selections such as “password”, “123456” or “secret”) can go a long way toward securing an organization’s data. Encrypting the data at rest can further protect an organization. If a network is compromised and data stolen, encryption will prevent the hacker from accessing or using that information. This is particularly effective if data has been backed up to a separate system, so an organization can still access data and operate normally during and immediately after a data breach.

Security audits to validate security measures will help to avoid complacency. Educating database users, owners, and operators on the need for, and methodology of, cybersecurity is often the difference between success and failure. Explaining what behaviors will lead to a more- or less-secure network can be all the protection an organization needs to prevent data breaches.

8. The IT Guy

The IT professional does not necessarily have much expertise in ICS. The IT profession has been focused on servers, PCs, data networks, and PC networks, personal information, public information, and company data. ICS information comes from serial communication over ARCnet and many proprietary systems and application-specific hardware and protocols. The technologies have developed differently, making the ICS IT systems alien to many IT professionals.

Do IT professionals understand what a BAS is and what its components do? Their responsibility is to ensure that the IT system is reliable and secure; surely a BAS will benefit from a reliable and secure IT infrastructure. They use IT-based tools and work flows that may not work on an ICS.

So again, an analysis of the system is required:

- How many IP-based controllers are part of the system? What IT functionality do they have?
- How much bandwidth are they going to use?
- Do they use broadcast as a method of communication?
- How can they be configured?
- How can they be recovered if they fail?

Does the IT professional appreciate that a building automation controller cannot be easily turned off and on, that there is a consequence to occupants if a controller is turned off, and that there are sometimes lengthy sequences for turning them off and on? Do they appreciate that the BAS is not designed to be easily modified? Do they understand that it is designed to be installed once, and to be left unchanged for the rest of its life?

What operating system do IP-connected components have, and how can they be upgraded or patched?

How often do they need to be upgraded or patched, and what is the process?

The answers to all these questions will help IT professionals gain a better understanding of a BAS and help them manage IT as well as IT security.

9. References

[1] Frost & Sullivan (2014) Big Data as an Enabler for Smart Buildings - Convergence of Building Technologies and the ICT Industry Drives More Investments through Partnerships. London, UK. Frost & Sullivan

[2] Frost & Sullivan (2014) The Smart Building Systems Market in North America - Merging Physical and Virtual Environments though Connectivity. San Antonio, Texas, USA. Frost & Sullivan

[3] Frost & Sullivan (2015) Cybersecurity in the US Power Industry - Regulatory Compliance is the Main Investment Driver. San Antonio, Texas, USA. Frost & Sullivan

[4] Frost & Sullivan (2014) The Role of ICT in Building Smart Cities Infrastructure - Connectivity, Cloud-based Analytics, and Open Data to be Key Enablers of Future Urban Growth. Warsaw, Poland. Frost & Sullivan