Life Is On | Schneider Electric

Defending Against Cyber Threats to Building Management Systems

by Daniel Paillet, CISSP, CEH

Executive summary

Until recently, monitoring of building management systems (BMS) security was never an issue. With the threat of cyber attacks looming large, more attention must be paid to the integrity of the BMS. While well understood protocols exist for monitoring and protecting computers and data centers, BMS systems are often ignored. This paper describes the threats that exist and recommends approaches for deploying a "Defense in Depth" methodology specific to BMS.

Introduction

The threat of cyber attacks against Building Management Systems (BMS) is a growing concern both inside and outside of the buildings industry. One recent event, the much publicized attack against retail giant Target (nearly 1800 department stores across the US), resulted in the theft of 40 million payment card numbers over a 19 day period. This breach occurred because Target had provided an outside heating, ventilation and air conditioning (HVAC) supply company external network access. This then allowed hackers a path from which to launch an attack against more critical systems within the Target network.[1]

Building and access control systems are computers that monitor and control building operations, such as air conditioning, electrical power, electronic card reading, elevators, fire alarms and fire suppression, heating, lighting, ventilation and video surveillance. These systems are increasingly connected to other information systems and to the Internet. While this advancement in technology improves automation and enables remote operations, it also exposes these systems to possible cyber attacks. Until very recently, no one was addressing the potential cyber risks to these types of systems within the US government network of nearly 9,000 federal facilities. Cyber threats to these systems were still considered "an emerging issue," and a cyber expert informed government agencies such as the General Accounting Office (GAO) that such systems were not designed with cyber security in mind.

Now these threats have attracted the attention from the U.S. Department of Homeland Security (DHS). From fiscal year 2011 to fiscal year 2014, the number of cyber incidents involving industrial control systems, including building and access control systems, rose from 140 incidents to 243 incidents, a 74% jump. The financial costs of these types of incursions run into the hundreds of billions of dollars each year. One international law enforcement agency estimates that victims lose about $400 billion each year worldwide — making it a bigger criminal enterprise than the global trade in marijuana, cocaine, and heroin combined.[2]

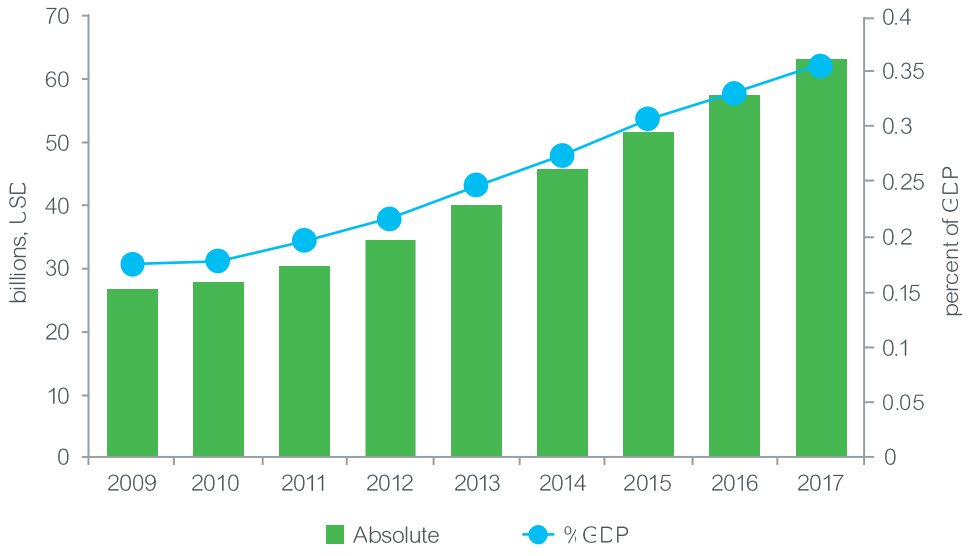

Figure 1
Growth in cyber security spending in the US (courtesy of the Telecommunications Industry Association).

[1]http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[2]https://news.clearancejobs/01/26/dhs-eyes-cybersecurity-issues-building-control-systems/

Another report reaches the same conclusion, estimating that the cost of malicious cyber activity worldwide is anywhere from $300 billion to $1 trillion.[3] The financial impact on companies varies from country to country and among sectors, but the one common feature is that cyber attacks are costing companies more money every year.[4]

"Defense in Depth" applied to operations

Defense in Depth is an information security strategy which integrates people, technology, and operations in order to establish penetration barriers across multiple protection layers in support of the critical missions of an organization.[5]

Though normally associated with information technology (IT) security, Defense in Depth should also be applied to Operations Technology (OT) systems such as Building Management Systems (BMS). There is a difference in how this approach is applied to OT vs. IT. IT systems are focused on the core security triad of confidentiality, integrity and availability of ***information*** (in that order of priority). In the case of a BMS system, however, the security triad consists of availability of operational assets as the first priority, integrity/reliability of the operational process as second priority, and confidentiality of operational information as a third priority.

The deployment of such a multi-disciplinary defense approach across system levels requires a cost-benefit balanced focus on the three primary levels of people, technology and operations.[6] **Table 1** illustrates the major steps that need to be accomplished at each of these levels.

Table 1
Key steps within the three pillars of the security triad.

People	Technology	Operations
Support is forthcoming from senior leadership	The right technologies are procured and deployed	Create and implement the activities necessary to sustain the security position of operations on a day- to-day basis[7]
Building management personnel (or anyone who else can access the system.) are trained and aware of cyber security issues	Defense is provided at multiple points	
Security responsibilities are agreed to and roles are assigned across the IT and building management organizations	Defenses are deployed in layers, access to the BMS via the IT network is isolated/limited	
Security policies and procedures are established	Detection intrusion technologies are deployed	

[3] http://oreo.schneider-electric.com/flipFlop/695962877/files/docs/all.pdf

[4] "Understanding the economics of IT risk and reputation," IBM, November 2013.

[5] http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf

[6] https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

[7] https://www.nsa.gov/ia/_files/support/defenseindepth.pdf

The sources of threats are not only invisible hackers that are patrolling the internet in search of soft targets. The category of people threats can include both internal employees and outsiders. Techniques that people use to threaten systems include the following:

- **Phishing** – In this case, the act of defrauding an online account of financial information is executed by the scammer appearing to be a legitimate company, or website.
- **Spear Phishing** – This is an email that appears to be from a legitimate business or person. The email is in fact from some criminal enterprise who wants to retrieve a credit card number, password, or financial information from your personal computer.
- **Advance Persistent Threats (APT)** – These are network attacks where an unauthorized person gains access to a targeted network and stays on the network undetected for a long period of time. APT attacks are intended to steal information from organizations.

More technologically-oriented threats include the following:

- **Malware** – This is malicious code or software designed to damage or perform unauthorized actions on a computer system.
- **Key Loggers** – These are programs that record keystrokes on a computer and creates a log of those details. Those logs can be sent remotely over the internet for further review by the malevolent agent that installed the software.
- **USB key drop** – These are USB keys that are intentionally left in parking lots or garages in hopes that someone will pick the key up and plug it into an office computer. The key can have malicious software, load viruses and even send information from the infected PC across the internet.
- **Pwnie Plug** – This is a small squarish white device that looks like a power adapter that plugs into a wall and that is actually used to hack into nearby networks.
- **Pineapple** – This is a battery powered wireless hacking device that can be used against wireless networks or devices.

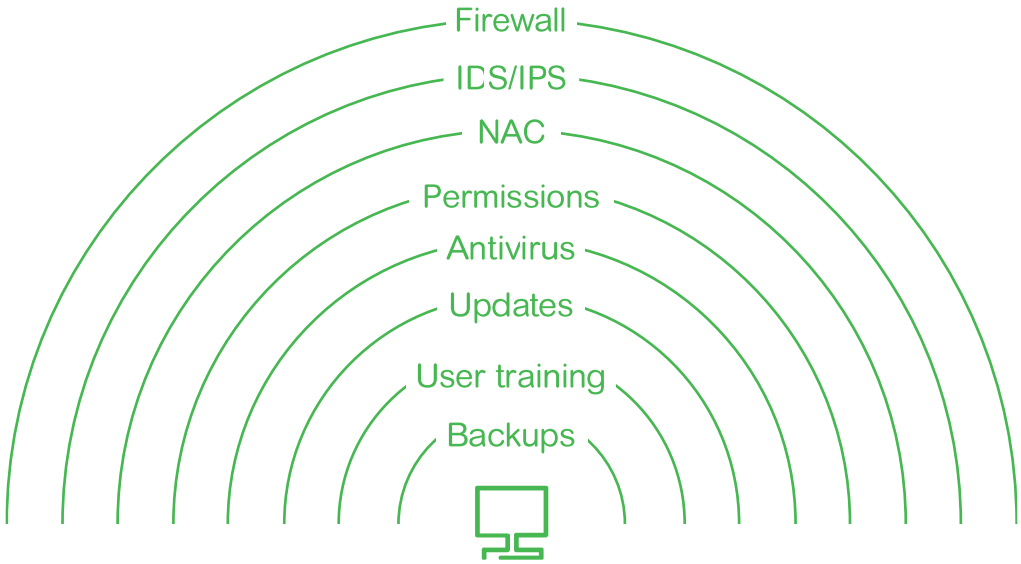

Figure 2
Example of a layered approach to defense.

The layered protection approach depicted in **Figure 2** was developed by the United States Control Systems Security Program (CSSP). This example of a Defense in Depth security implementation manages risk with diverse strategies. If one layer of defense turns out be inadequate, another layer of defense is in place to prevent a full breach.[8]

Defense in Breadth

Defense in Breadth which is a supplement to Defense in Depth is defined as follows: A planned, systematic set of multi-disciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or sub-component lifecycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).[9] In short, Defense in Breadth uses of multiple types of security devices within each security layer."[10]

In order to understand the differences between Defense in Breadth and Defense in Depth, consider the following anti-virus example: Defense in Depth uses anti-malware as one type of defense. Defense in Breadth may employ multiple anti-malware applications. It is prudent to deploy both approaches because one anti-virus software-package may detect a virus that another will miss. Use of one vendor's antivirus software on an email server and use of a different vendor's software on PCs, workstations, and servers potentially casts a broader net of protection (in this case against viruses).

The realm of BMS, Defense in Depth/Breadth includes security of gateways, meters, and controllers. Construction of such defense architecture begins when the manufacturers of these components pursue a Secure Development Lifecycle at the manufacturing level for BMS-related devices and software (see **Figure 3**). This process allows for the development of hardened devices and software that can be resilient against attacks. **Figure 3** illustrates the different layers and processes that enable the hardening of BMS that are secured by design, secured by default, and secured in deployment.

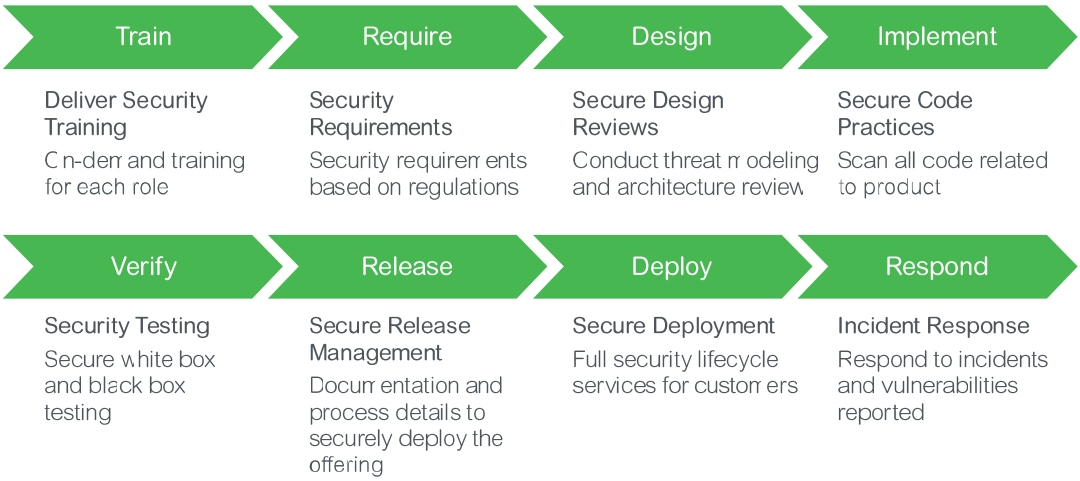

Figure 3
Secure Development Lifecycle.

[8]Viega and McGraw [Viega 02] in Chapter 5, "Guiding Principles for Software Security," in "Principle 2: Practice Defense in Depth" from pages 96-97_

[9]http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf

[10]Official (ISC2) Guide to CISSP-ISSMP CBK, Second Edition, page 198

BMS security

Within the realm of Building Management Systems (BMS) cyber security needs to address more than the commonly recognized deliberate attacks from disgruntled employees, industrial espionage and/or terrorists. In some cases user error, equipment failure or natural disasters can make the system vulnerable. These can create weaknesses in the system defense perimeter that can allow an attacker to penetrate the network, gain access to control software and alter load conditions to destabilize the system in unpredictable ways.[11]

Table 2 illustrates how BMS networks can be made more threat resistant through targeted management of security system process and procedures.

Table 2
Best practices for strengthening BMS network security.

Processes	Procedures	Benefits
• Follow standards and regulations • Credential management • System administration • Patch management • Incident response	• Personnel training • Regular assessments	• Prevent inadvertent mal-ware introduction • Avoid social engineering breaches • Compliance with norms

Details regarding the points listed in **Table 2** can be accessed via the link provided in the footnote at the bottom of this page.[12]

For maximum protection, conventional IT security solutions should be incorporated into Building Management System networks. Listed below are some areas to consider in the overall security scheme:

Access controls

- Physical Access Controls: Fences, security locks, card readers, video cameras
- Network Boundary Controls: Firewalls, VPN, unidirectional gateways

Network hardening

- Installation processes and procedures for software and embedded devices covering such elements as changing default credentials and disabling unused services from operating systems
- Implement Host intrusion prevention systems on endpoints, application “white listing” (the use of anti-spam filtering software to allow only specified e-mail addresses to get through) to prevent Trojans and malicious software from executing in servers/workstations

[11]NIST Smart Interoperability Panel: Cyber Security Group

[12]http://iom.invensys.com/EN/pdfLibrary/NERCCIPComplianceChecklist.pdf

Authentication and authorization

- Centralized account management for user authorization and authentication
- Role-based access control for end user rights and privileges
- Monitoring and auditing of system events
- Centralized security event logging of network and system access
- Intrusion detection prevention systems to detect anomalous traffic on the network
- Security incident event manager with real time alerting and 24/7 monitoring

Enhancing availability and reliability of the network helps to build customer confidence in the cyber security characteristics of the BMS.

The National Institute of Standards and Technology (NIST) has provided guidance in developing a framework for improving cyber security applicable to BMS. One such document *"Framework for Improving Critical Infrastructure Cyber Security,"* outlines basics on how to deploy a framework. According to NIST, a framework enables organizations – regardless of size, degree of cyber security risk, or cyber security sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The framework provides organization and structure to the various cyber security approaches by assembling standards, guidelines, and practices that have proven to work effectively. The framework should embrace globally recognized standards for cyber security. It can be used by organizations globally and can serve as a model for international cooperation on strengthening critical infrastructure cyber security.[13]

The weakest links in any IT or Building Management System are the people who administer and use the systems. Their actions, either intentional or unintentional, can increase the security risk to systems. Unintentional actions include unsecured laptops, workstations, work areas, and not following proper process and procedures (like password management including not revoking credentials and access when an employee leaves the company). Intentional actions include insider threats such as sabotage, fraud, theft or leaking of intellectual property or classified/confidential information.

The threat of "social engineering"

Social engineering in the context of cyber security refers to one person who influences another individual who is in possession of a computer (and who has internal access to particular networks and/or data bases) to follow their instructions under false pre-tenses. For example a caller could pose as someone form IT support asking for credentials or other sensitive information. Additional examples of these types of attacks are detailed below:

Example 1: email for a "friend"

In some cases the user may believe that he or she is receiving an email from a recognized friend. In fact, if a criminal manages to hack or socially engineer one person's email password he, in all probability, may have access to that person's contact list. This happens because most individuals use one password everywhere, meaning that the criminal most likely has access to that individual's social networking contacts. Once the

[13] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

criminal has that email account under his control, he sends emails to all of the affected person's contacts or leave messages on all their friend's social pages, and possibly on the pages of the person's friend's friends.

The messages received from the hacker are designed the abuse trust and to peak curiosity. They may contain a link that *"you just have to check out!"*. Since the link comes from a friend and you're curious, you'll trust the link and click. This leads to malware infection that allows the criminal can take over your machine and collect your contacts info and deceive them just like you were deceived.

In other cases the email may contain a download of pictures, music, a movie, or a document that has malicious software embedded. If you download–which you are likely to do since you think it is from your friend–you become infected. Now, the criminal has access to your machine, email account, social network accounts and contacts, and the attack spreads to everyone you know.

The messages received from the hacker may depict a compelling story or pretext. For example, you may get an urgent request from your "friend" to help because he is stuck somewhere, has been robbed, and needs some emergency money to get back home. Or you may get asked to donate to a charitable fundraiser, or some other cause – with instructions on how to send the money (to the criminal).

Example 2: Phishing attempt

A hacker engaged in "phishing" sends an e-mail, instant message or text message that appears to come from a legitimate, popular company, bank, school, or institution. These messages usually present the reader with a scenario or a story. The message may explain there is a problem that requires you to "verify" of information by clicking on the displayed link and providing information in their form. The link location may look very legitimate with all the right logos, and content (in fact, the criminals may have copied the exact format and content of the legitimate site). Because everything looks legitimate, you trust the email and the phony site and provide whatever information the criminal is asking for. These types of phishing scams often include a warning of what will happen if you fail to act soon, because criminals know that if they can get you to act before you think, you're more likely to fall for their scam.

The message you receive may also notify you that you are a "winner". The email may claim to be from a lottery, or a dead relative, or the millionth person to click on their site. In order to give you your 'winnings' you have to provide information about your bank routing so they know how to send it to you, or give your address and phone number so they can send the prize, and you may also be asked to prove who you are often including your Social Security Number. These are the 'greed phishes' where even if the story pretext is thin, people want what is offered and fall for it by giving away their information, then having their bank account emptied, and identity stolen.

Example 3: Baiting scenarios

These socially engineering schemes play on people's desires for "a good deal". The "bait" may be a good price on a particular item or a hot new movie or song. These schemes are often found on peer-to-peer sites, on social networking sites, or malicious websites that come up through search results. The scheme may show up as an amazingly great deal on classified sites, or auction sites. To allay your suspicion, you can see the seller has a good rating (all planned and crafted ahead of time). People who take the bait may be infected with malicious software that can generate any number of new exploits against themselves and their contacts. They may lose their money without receiving their purchased item, and, if they were foolish enough to pay with a check, they may find their bank account empty.

Example 4: Response to a question you never had

Criminals may pretend to be responding to your "request for help" from a company while also offering more help. They pick companies that millions of people use like a software company or bank. If you don't use the product or service, you will ignore the email, phone call, or message, but if you do happen to use the service, there is a good chance you will respond because you probably do want help with a problem (like a computer problem that you may be having).

The representative, who is actually a criminal, will need to 'authenticate you', have you log into 'their system' or, have you log into your computer and either give them remote access to your computer so they can 'fix' it for you, or tell you the commands so you can fix it yourself with their help. This can enable the criminal to get back into your computer later.

Example 5: Creating distrust

Some social engineering is all about creating distrust, or starting conflicts. These are often carried out by people you know and who are angry with you, or by troublemakers just trying to wreak havoc. These people want to first create distrust in your mind about others so they can then present themselves in a heroic fashion and gain your trust. In some cases this may involve extortionists who want to manipulate information and then threaten you with disclosure. This form of social engineering often begins by gaining access to an email account or other communication account such as an instant messaging client, social network, or chat forum, They accomplish this either by hacking, social engineering, or simply guessing particularly weak passwords.

The malicious person may then alter sensitive or private communications (including images and audio) using basic editing techniques and forwards these to other people to create drama, distrust, or embarrassment. They may make it look like it was accidentally sent, or appear like they are letting you know what is 'really' going on. Alternatively, they may use the altered material to extort money either from the person they hacked, or from the supposed recipient.

There are literally thousands of variations to social engineering attacks. The criminal's imagination is the only limit to the number of ways he can socially engineer affected users. The criminal is also likely to sell your information to others so they too can run their exploits against you, your friends, your friends' friends, and so on.[14]

In general, social engineering is considered any act that influences a person to take an action that may or may not be in their own best interest.[15] It represents the "art and science" of one individual getting another individual to comply with their wishes. Oftentimes, the attacker in a social engineering situation will target the weakest link in the computer security chain. In fact, one could postulate that even an unplugged computer can serve as the conduit to an act of social engineering. If the attacker can persuade an unsuspecting individual to plug a computer in and switch it on that "unplugged" computer could serve as a conduit to a breach.[16]

Social engineering is the easiest path from which to gain unauthorized access into a BMS. To defend against such attacks companies must train their organizations, contractors and business partners, in order to resist such threats. This can include awareness training, as part of the on boarding process when new people or outside firms are brought into the organization.

Some organizations deploy threat modelling in order to anticipate the various series of events that could lead to a security breach. In the case of BMS, threat modelling would include identification of accessible entry points, and a clear definition of contractor and user access rights (e.g., principle of least privilege). Policies, processes and training then needs to be developed surrounding the outputs of that threat model.

Insider threats can have dire consequences when sabotage of BMS assets and process is involved. Training programs are an important means of defense under such circumstances. **Table 3** illustrates core elements that should be integrated into a BMS security training program:

Table 3
Elements for strengthening BMS cyber security.

Human resources	Organizational education	Policies and processes
• Start with the hiring process, deactivate access upon termination	• Special training for mangers and human resources	• Implement principle of least privilege, separation of duties, strict password management rules, change controls
• Log and monitor activities	• Reinforce awareness training annually	• Backup and recovery
• Look for and anticipate issues leading to malicious activity	• Train contractor and business partners	• Establish and communicate deterrents for non-compliance

[14]http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering# close

[15]Social-Engineering.org

[16]http://www.textfiles.com/russian/cyberlib.narod.ru/lib/cin/se10.html

Conclusion

Creating a security policy and network infrastructure for Building Management Systems will require the support of senior management. The work involved in maintaining robust defense in depth and breadth is ongoing. As attacks (including social engineering) become more common and more sophisticated, processes and procedures need to be developed that secure BMS networks. Training of people who manage BMS networks is a critical success factor. Vigilance and due diligence should include a disciplined maintenance of the BMS systems with the latest updates, and evolving the strategies that account for defense in-depth and breadth security architectures. Training of end users/employees and should occur on a regular basis in order to guard against social engineering malfeasance. Such investments will benefit the organization by reducing incidences that result in loss of revenue, and by safeguarding the organization's reputation with customers and partners.

About the author

Daniel Paillet is currently Cyber Security Lead Architect within the Schneider Electric, Energy Management Business Unit. His background includes working in the US Department of Defense on various security projects. He has over 15 years of security experience in Information Technology, Operational Technology, Retail, Banking and Point-of-Sale. He holds the CISSP, CEH and other agnostic and vendor specific certifications. His current role is to architect, improve, and develop secure solutions and offerings within Schneider Electric.

Note: Internet links can become obsolete over time. The referenced links were available at the time this paper was written, but may no longer be available now.

Schneider Electric USA
800 Federal Street, Andover, MA 01810 Telephone: 978-794-0800 www.schneider-electric.us

998-2095-12-08-15AR0_EN Rel. 03/19