Five Best Practices to Improve Building Management Systems (BMS) Cybersecurity

By Gregory Strass, CISSP, CEH
Jon Williamson

Executive summary

Data breaches and other cyber crime cost companies billions each year worldwide, and the damage to brand reputation can be incalculable. Since hackers look for weakly defended systems to attack, this paper presents 5 cybersecurity “best practices” to mitigate system vulnerabilities. Some are commonsense measures like effective password management; others involve securing open ports and other access points, software upgrades, user management, and vulnerability plans.

998-2095-07-29-14AR0

Schneider Electric

Introduction

Cybersecurity threats and attacks have become a common occurrence and pose a global problem. Cyber criminals are targeting individuals and corporations with more frequent, more sophisticated, and more coordinated assaults. Cyber attacks in the United States alone increased 17-fold between 2009 and 2011.[1] The European Cybercrime Centre at Europol has identified the top 20 countries for cyber crime (**Figure 1**), and no region of the world is immune. Unsurprisingly, countries with more advanced Internet infrastructure and that have incorporated more online digital technologies into their day-to-day business operations experience more incidents of cyber attacks.

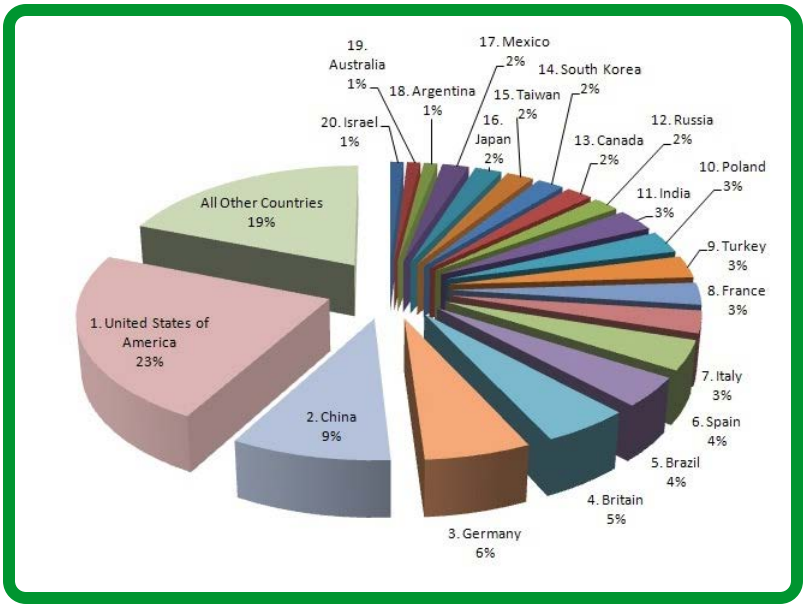

Figure 1
Top 20 counties experiencing cyber crime

"Cyber crime is a $400 billion criminal enterprise worldwide — making it bigger than global drug trafficking."

Cyber crime costs companies literally 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] 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 (**Figure 2**) and among sectors, but the one common feature is that cyber attacks are costing companies more money every year (**Figure 3**).[4]

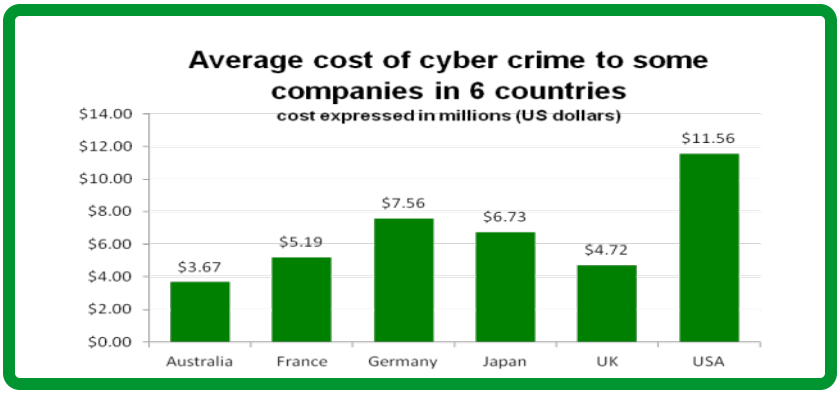

Figure 2
Average cost of cyber crime based on a survey of 234 companies in six countries.[4]

[1] "The Economic Benefits from Improved Cyber Security Infrastructure", Gary Anderson and Gregory Tassey. NIST Economic Analysis Office Economic & Policy Analysis Brief 13-3

[2] "Cybercrime: A growing global problem," European Cybercrime Centre.

[3] "The Economic Impact of Cybercrime and Cyber Espionage," McAfee and the Center for Strategic and International Studies, July 2013.

[4] "2013 Cost of Cyber Crime: Global Report," Ponemon Institute, October 2013.

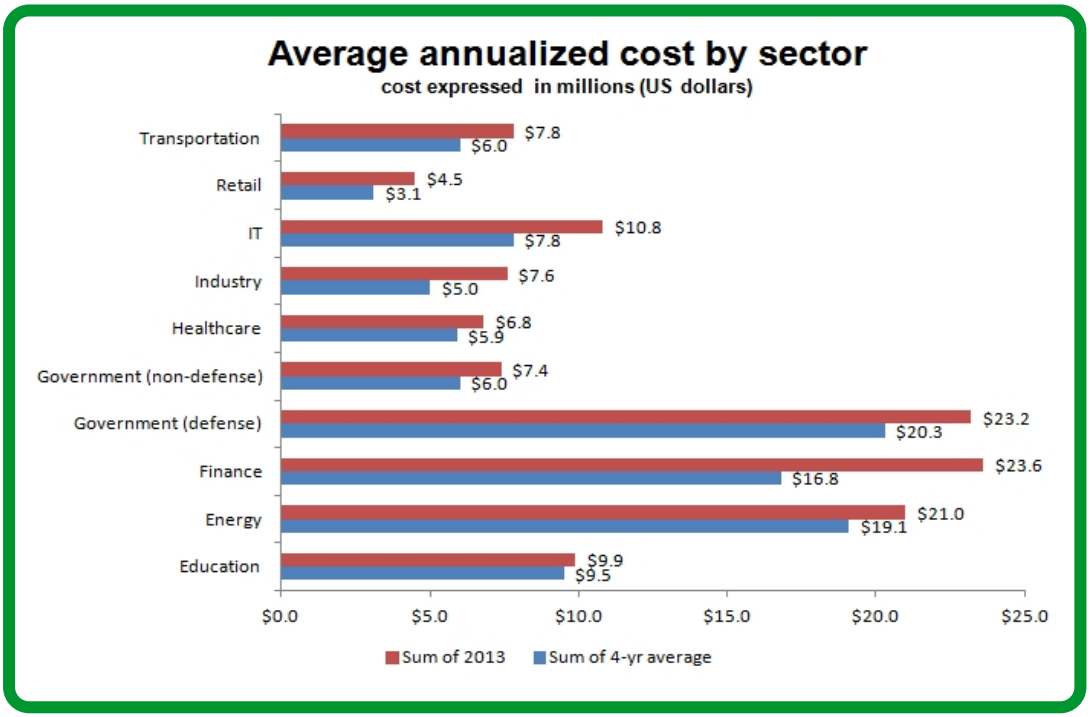

Figure 3
Average 2013 cost of cyber crime by industry, vs. previous 4-year average

The financial consequences of a cybersecurity attack include direct costs — forensic investigation into the breach, technical support, lost revenue, upgrading cybersecurity technologies and activities — and indirect costs such as loss of productivity, regulatory noncompliance, loss of intellectual property, service or product quality degradations, and, harder to quantify but perhaps most costly of all, the damage to the company's reputation and/or customer desertion (**Figure 4**)[5].

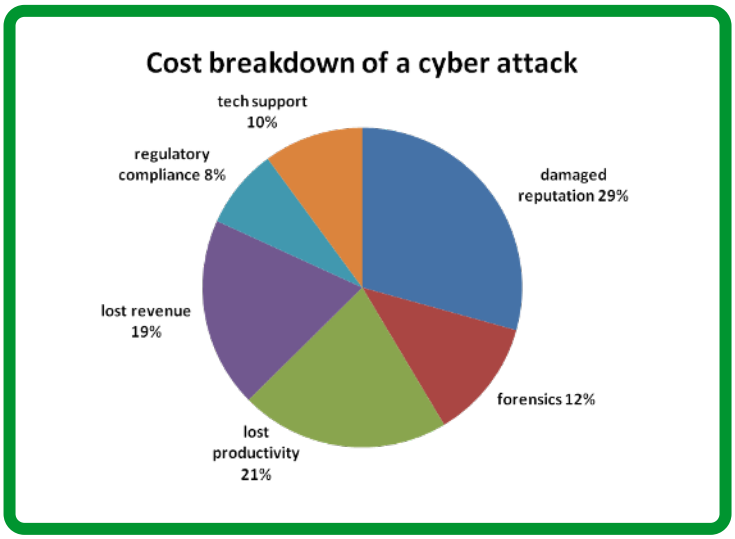

Figure 4
Financial consequences of a cyber attack, broken down across 6 categories.

Building management systems (BMS) that were once proprietary and stand-alone now are integrated with other systems. Today's intelligent building management systems (iBMS) are networked with IT data centers, remote access servers, and utilities through open protocols. While these iBMS provide significant benefits, they also open companies up to greater cybersecurity vulnerabilities.

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

This paper discusses practices and procedures that will lead to more secure iBMS in the field. Although many steps may sound familiar and commonsense, additional rationale is offered for why these steps are so important. These best practices revolve around the following 5 aspects of cybersecurity as well as other activities that should be considered:

1. Password management
2. Network management
3. User management
4. Software management
5. Vulnerability management

Making improvements in these 5 areas will pay great dividends and lead to better-hardened, resilient systems that are less vulnerable to attack.

Password Management

Properly managing users and passwords is critical to securing any building management system (BMS). Most attacks on BMS devices are successful because a password has been compromised. There are many password-related subjects that could be covered. This paper addresses the two most important:

- Change default passwords
- Password complexity

Credentials and credentialing

When referring to a user's name and password as a single element, the term "credential" is often used. The process of managing users' names and passwords can be referred to as "credentialing."

Change default passwords

The importance of changing default passwords for every installation cannot be understated. **This should always be the first thing done when a new device is initialized.**

Products ship with minimal credentials to allow for system initialization. From a security standpoint, the longer a device sits with default credentials once it's been removed from its sealed shipping materials, the greater the risk it will be compromised.

Many think that changing default credentials is unnecessary because no one would ever be interested in their device, let alone be able to find it on the Internet. Unfortunately, the opposite is true. Devices retaining default credentials make hacking into a BMS mere child's play.

Even if the manufacturer does not intend them to, a device's default-credential values find their way into publicly available documents or onto the Web. Obtaining them is usually a simple Google query. There are search engines that routinely scan for all accessible devices connected to the Internet, including BMS devices. A substantial amount of information about the devices is stored on the service's database. That data is then available to all of the site's subscribers — legitimate users as well as hackers.

"The longer a device sits with default credentials, the greater the risk it will be compromised."

This information about devices is valuable to a hacker. Once hackers are armed with the network information, it is a simple process for them to access the device and determine if it is using default, or easily guessed, credentials. Once accessed, the device's information is harvested and stored for later use. It is also possible the hacker will just sell the information to others in the hacker trade. This is a process that happens continuously, and no Internet-facing devices are exempt.

At a minimum, a device's default credentials should be changed before it is ever connected to the Internet. A "best practice" would be to change the default credentials when the device is first unpacked.

Table 1
4 best practices for password management

Vulnerability	Reason	Best Practice
Default credentials	Available in online databases	Change defaults before connecting
Simple passwords	Easily cracked	10- to 15-character multi-type passwords
Demonstration systems	Hard-coded credentials	Change defaults before connecting
Same credentials for all sites	All sites at risk if credentials hacked	Unique credentials for each site
Credentials shared among a group of users	Lack of traceability and accountability	Require unique credentials per user

Another common practice is connecting a "demo unit" to the Internet while it still contains default credentials. While there may be no useful information in the device's database, there is still real risk. Just having access to the device provides a hacker with a wealth of information.

Once hackers are "into" a demo device, they scan it for weaknesses. They may uncover hard-coded credentials that would allow all such devices to be compromised — even if the default credentials were changed. For example, many older BMS devices have hard-coded credentials burnt into the code. The reason for doing this was to enable factory support teams to reset lost or forgotten passwords. Manufacturers always intended to keep this information confidential. But if these credentials are in the code, it is generally straightforward for a hacker to find them and leverage that information to compromise all similar devices.

Another best practice is to have unique credentials for each site. Employing a single set of credentials for all sites makes device management easier, but it means that all sites would become vulnerable if those credentials were compromised.

Best practices dictate that each site have its own, unique credentials.

Password complexity

"Machines today can test up to 348 billion passwords per second."

The days of simple passwords with only 6–8 alphabetic characters are gone. Today, there are inexpensive machines that can easily test up to *348 billion passwords per second*. To provide any real level of protection, only complex passwords of sufficient length should be used.

Creating a complex password is a straightforward process. Increasing the number of character types used (alphabetic, uppercase and lowercase, numbers, and special characters) exponentially increases the length of time it takes to crack a password.

Considering the powerful software available to crack passwords, it is important that they not be easily guessed and that they are created with sufficient complexity. The following rules, summarized in **Figure 5,** are the minimum requirements for creating secure passwords:

- A minimum length of 10 characters
- At least one numeric, one lowercase alphabetic, and one uppercase alphabetic character in each password

What makes a password secure?

Length	**At least 10 characters** **15 characters for infrequently accessed systems**
Character set	**Include mixture of numbers, uppercase and lowercase letters, and special characters**

Figure 5
"Rules" for creating a complex, secure password.

In theory, passwords need to be changed within a period of time not to exceed the time it takes to crack them. Since many BMS devices are in the field for 15 to 30 years and may not be accessed often, making the password more complex is the only good way to adequately protect these systems. When the interval between access times might be years, password lengths of 15 characters or more are recommended.

"Remembering a long phrase tends to be easier than remembering a long, complex password."

As passwords increase in length, it is often better to employ the concept of a "passphrase." Instead of attempting to modify (or "decorate") existing passwords with special characters and a mixture of uppercase and lowercase, consider creating a secret phrase. These can be quite effective because they usually run more than 15 characters. Remembering a long phrase tends to be easier than remembering a long, complex password.

A Word of Caution

Historically, BMS devices have had minimal password-handling capabilities. Attempting to use sufficiently complex passwords or passphrases may create operational issues, up to and including system crashes. It is strongly recommended that before making the existing passwords for devices more complex, consult the operator's manual to check what constitutes valid password length and character sets. Alternatively, test complex new passwords on non-production devices first, to see what password characteristics are allowed by the device.

Network Management

Once all devices have adequately secure credentials, the next step is to safeguard other places and ways a hacker could get into the system. Such other "points of entry" include the Web interface, USB ports, open IP ports, and building automation devices communicating over open protocols.

Secure the Web interface

"SQL injection was responsible for 83% of successful hacking-related data breaches from 2005–2011."

Source: Privacyrights.org

Devices containing Web interfaces require special consideration. Any Web interface that is accessible from the Internet is the first, most susceptible point of attack. There are various cyber attacks that can easily defeat improperly coded Web-based authorization. One is called "SQL Injection," which could allow an attacker to change all passwords in the device with a single "properly formatted" value entered into the "Name" field.

It can be difficult to determine the types of vulnerabilities present in a device's Web interface. A best practice is to access the BMS manufacturer's website to locate information about Web interface security. Devices with vulnerable Web interfaces should never be placed directly onto the Internet. If Internet access is required, one best practice to mitigate the risk is to insert a firewall between the device and the Internet and block port 80 and port 443 and any other port supporting the HTTP/HTTPS protocols. (8080 is a common alternate HTTP port.)

Secure all points of access

BMS devices often have many non-IP-based communication channels. Beyond the RJ-45 Internet connector, they often have RS-232 and/or RS-485 connections as well as current loops. All such interfaces need to be evaluated for weaknesses that may threaten secure device operation. Interfaces that are not being used should be disabled if possible.

One common, but often ignored, access point is the USB port. From a security standpoint, the USB port presents a **high risk** to the device. The software drivers associated with USB ports were designed to automatically run programs found on them as soon as the device is inserted. If the USB device is tainted with malware, this "Auto Run" feature can result in the malware being loaded onto the device without any warning.

*"From a security standpoint, the USB port presents a **high risk**."*

Best practices call for disabling all USB ports' "Auto Run" feature. If that is not possible, at least limit physical access to the USB ports.

Another significant security risk comes from hackers distributing infected USB flash drives to people with potential access to devices of interest. The ways hackers distribute the USBs vary: they may simply drop infected memory sticks in the parking lot or give them away as "prizes" through the mail. The goal is to get an infected memory stick into the hands of someone who has access and might use it to transfer data to the device.

Once the infected stick is inserted into the unprotected USB port, the system is "auto-infected" and the hacker has unrestricted access to the compromised device.

So, when transferring data to a device, best practices mandate that only a "known secure" device from a quality vendor, removed from a sealed package, should be used.

Additional guidance

Many websites provide guidance on how to better manage cybersecurity. The basis for many is the National Institute for Standards and Technology (NIST) Generally Accepted Principles and Practices for Securing Information Technology Systems.

Enable only the minimum number of ports

Devices often ship with many TCP/IP ports open. Often some of these ports are not needed for proper system operation. Ports like FTP, SMTP, SNMP, and others may be needed for large installations, but not for smaller sites.

Review the required functionality for each network segment, and adjust port access accordingly. For devices that do not provide the ability to close unused ports, a firewall should be installed and configured to allow communications only on needed ports.

Secure segments running open BMS protocols

Most of the field bus networks running in an iBMS use protocols that are inherently insecure. In some cases these protocols have vulnerabilities that allow users to inject commands into the controlling device. While there are efforts to enhance protocols like BACnet with security features; these protocol changes have not yet made it into new devices.

Ultimately, a risk assessment should be performed to determine the relative risk of each such network. Most iBMS protocols are managed by active groups or committees and have websites that can be referenced when starting a risk analysis. For any segments determined to contain critical control elements, physically securing all aspects of that segment should be considered.

Table 2
4 best practices for network management

Vulnerability	Reason	Best Practice
Web interface	SQL injection	Install firewall
USB port	Access to entire system	Disable Auto-Run Disable / secure port
TCP/IP ports	Access to entire system	Close ports Install firewall
Open protocol networks	Allow hackers to inject commands	Perform risk assessment Physically secure segments

User Management

Once the BMS has been cybersecured from external threats, the next issue to address is safeguarding the system from within. Over the past several years, BMS have evolved from “single user – command line” systems to full-blown, multi-user GUI systems. Along with this expansion in functionality has been a significant increase in the types of operations a user can perform.

Grant users minimal authority to do their job

While it is easier to grant everyone “super user” privileges, such a practice is strongly discouraged. One of the major threats to all systems is the “disgruntled” employee. The amount of damage disgruntled employees can do will be controlled by the level of access granted. If they have simply been given “super user” privileges, the damage could be catastrophic.

Best practice is to follow the principle of least privilege and give each user only enough access privileges to allow them to do their job.

Manage user accounts

User management is an important component to maintain a device's security. Some devices have services to help automate this process, or rely on external Directory Services (Microsoft Active Directory or Linux's LDAP) for this functionality. For sites where user accounts are controlled only inside the device, the following practices need to be implemented:

"One of the major threats to all systems is the 'disgruntled' employee."

Auto-expire all accounts
For devices that provide password-aging functionality, all non-administrator accounts should be configured so their passwords expire after a certain date or a certain number of days. This means regular users will need to periodically reset their passwords. Accounts that are not accessed within a specified period of time need should be disabled automatically –— requiring the system administrator's intervention to re-enable the account.

Immediately disable accounts for employees who leave
An often overlooked but significant security risk is failing to disable accounts for employees who leave the company. This is especially important when employment is terminated; either temporarily as a layoff or permanently. Best practices call for disabling such accounts as soon as employees resign or before they are notified of their termination.

For employees who tender their resignation, it is important to evaluate the risk associated with allowing them continued device access until their departure date.

Change accounts when employees change roles
Similarly, review employees' authorizations and access when they change business roles. It is important that their access and authorizations are still at levels appropriate to their new roles.

Software Management

Always apply software security patches

When attacking a device, hackers first determine if all security patches have been installed. When security features are not up-to-date, there are usually areas that can be exploited to compromise devices. A best practice is to regularly apply all security patches to all devices.

Ensure only authorized users can deploy software

Only highly trusted users should be granted privileges allowing them to deploy software. Often deployment requires running a host system in an administrator mode. In other cases, the tools used to install software open the device to increased risk of attacks. Best practices limit this role to a very few, highly trusted employees.

Install only authorized software

An increasingly common cyber attack is the distribution of doctored software deployment packages that may contain modified applications or additional applications that compromise the device's integrity.

Different devices provide different methodologies for ensuring a deployment package is valid prior to installation. Some packages provide verification codes to authenticate the integrity of the software. Many installers verify these codes automatically; others require manual verification (which is a straightforward process of comparing two strings). Other installers use cyber certificates, and still others employ secured communications channels between trusted hosts.

Be fully familiar with the deployment system's security features and implement procedures to ensure that software package authentication processes are followed prior to deployment.

Vulnerability Management

Patching devices with vulnerabilities requires planning. Different companies have different policies for performing BMS updates. It is important to understand these requirements as well as to determine any operational impact caused by the temporary service outage needed to complete the update process. A Vulnerability Management Plan takes into consideration all aspects of the vulnerability update.

A vulnerabilities severity rating helps determine how quickly vulnerabilities need to be addressed. Each known vulnerability is assigned a qualitative rating. Some rating systems use “Critical,” “High,” “Medium,” and “Low”; others use a numeric system ranging from 1 to 10. Generally speaking, vulnerabilities rated Critical (9-10) and High (7-8) need to be addressed as soon as possible. Less severe vulnerabilities can usually be addressed during regular maintenance.

Issues to consider when creating a vulnerability management plan include:

- How does a given vulnerability impact a particular installation?
- What is the process to quickly access and update the device?
- Are there factors that will affect the ability to access or update the device?
- Are there risks associated with the update?

It is a best practice to have a formal vulnerability management document for each installation.

Conclusion

Over the past few years, data breaches have become headline news around the world. Various actors, from nation-state governments to advanced hacker networks, have made finding and exploiting vulnerabilities both weapons of the state and a lucrative business.

Cyber attacks cost companies billions each year in lost revenue, security upgrades, lost productivity, and damaged reputation. Any company with infrastructure connected to the Internet is vulnerable. Today's computerized building management systems, with their integrated IP-based communications networks, are no exception. A hacker can use a single BMS device as an entry point to access the entire system.

"Effective and regular cybersecurity training makes everyone aware of vulnerabilities."

It is an established fact that hackers are more likely to attack weakly defended systems, ignoring systems that require too much effort to crack. But there are common "best practices" to thwart such attacks, or at least make things significantly more difficult for hackers. Some are simple, commonsense tactics such as changing the factory-set default credentials, making passwords more complex, and changing them on a regular basis. Other measures include shutting off external access: securing Web interfaces, disabling USB and IP ports, or installing firewalls. Some practices focus on internal access vulnerabilities, such as defining more strictly the level of authorization for each employee, disabling inactive accounts, ensuring that security patches are installed, and limiting who can deploy software upgrades.

While not every employee needs to be an expert in all fields, certain practices apply to all employees. Effective and regular cybersecurity training makes everyone aware of vulnerabilities. Ultimately, the level of cybersecurity is directly related to the effort expended in making it difficult for hackers to access valuable systems.

About the authors

Gregory Strass is the Building Systems IT Cyber Security Lead at Schneider Electric. He holds degrees in Electrical Engineering and Computer Science from the University of Illinois in Urbana. Additionally he holds CISSP and CEH certifications. He has worked in the embedded field for over 35 years.

Jon Williamson is the Schneider Electric Building Systems Communication Officer. He holds a degree in Mechanical Engineering from the University of New Hampshire in Durham. Active in the BMS market for over 19 years, he has practical and product management experience in system deployment, networking and protocols. In his current role as Communication Officer, he is responsible for system architecture, communication protocols and cybersecurity requirements.