Cybersecurity Best Practices

A summary of NEII's guideline for the industry to mitigate and counter increasingly pertinent cyberattacks

by Kevin L. Brinkman and Barry Blackaby

The National Elevator Industry, Inc. (NEII) released *Elevator & Escalator Industry Cybersecurity Best Practices*, a guideline for the industry developed by cybersecurity and codes experts from NEII member companies and international industry partners, in 2019. Developing *Best Practices* was critical, since building transportation systems with multiple controllers and processers, monitoring systems accessing the internet and Wi-Fi-capable communication systems have become an integral part of complex, modern buildings.

Best Practices provides a path to help elevator and escalator manufacturers design systems that provide measured protection and manage against network-based cyberattacks. *Best Practices* focuses on the interfaces between the elevator or escalator system and the internet, building-area networks and untrusted systems. Maintenance and service tools used by technicians are included and treated as untrusted systems.

Best Practices was developed with experienced cybersecurity professionals from Europe, the Pacific Asia Lift and Escalator Association (PALEA) and the China Elevator Association (CEA). During an 18-month collaborative effort, these experts developed models based on various building networks and elevator equipment designs.

Best Practices outlines the risk-assessment process, documentation, training, requirements, design, implementation, verification, release and operations of a sound cybersecurity program. It provides a baseline for development of a cybersecurity standard by the International Organization for Standardization (ISO).

The fundamental recommendation of *Best Practices* is a strong cybersecurity process lifecycle. This lifecycle needs to include a commitment to adequate training, tools, resources and processes to strengthen and protect elevator and escalator systems from cyberattacks. The lifecycle approach is also a fundamental premise of best practices for all cybersecurity standards and approaches.

Introduction

Cybersecurity protection for elevators and escalators has become a necessity. These systems — at one time isolated building conveyances — have become an integral part of complex modern building systems. Vertical-transportation (VT) systems have multiple controllers and processors, monitoring systems accessing the internet, Wi-Fi-capable communication with personal computers and mobile device-based service tools. Elevators have also become a key component in emergency situations with voice, real-time, in-car video displays and complex interaction with fire- and life-safety systems during building evacuation. The ability to deliver real-time data electronically to service personnel, as well as software updates on demand, is the norm. While connectivity takes elevators and escalators to new levels of availability, efficiency and general building safety, it also presents exposure to cyberthreats such as denial of service. The concern of jurisdictions, as well as customers, has been growing, to the point that states and customers are enforcing their own VT system cybersecurity requirements and restrictions.

The initial meeting for cybersecurity was planned to consist of representatives of NEII North American companies. It ended up with major manufacturers' cybersecurity experts from Finland, Germany and North America. Later, PALEA and CEA joined the team, making it a truly international effort. Due to the criticality of time, it was agreed to complete a fast-tracked guideline of best practices in time for the spring 2019 ISO Plenary Meeting, where it could serve as a starting document for initiating an international, consensus-based standard.

Continued

Learning Objectives

After reading this article, you should have learned about:

- Why and how the guideline was created
- What the guideline includes
- What is considered trusted or untrusted in a network
- The lifecycle of the cybersecurity process
- Security levels and measures
- The security concerns relating to tools used to service elevators and escalators

ELEVATOR WORLD EW ONLINE CONTINUING EDUCATION

Value: 1 contact hour (0.1 CEU)

This article is approved for Continuing Education by NAEC for CET® and CAT®.

EW Continuing Education is currently approved in the following states: AL, AR, FL, GA, IL, IN, KY, MD, MO, MS, MT, OK, PA, VA, VT, WV and WI. Please check for specific course verification of approval at www.elevatorbooks.com.

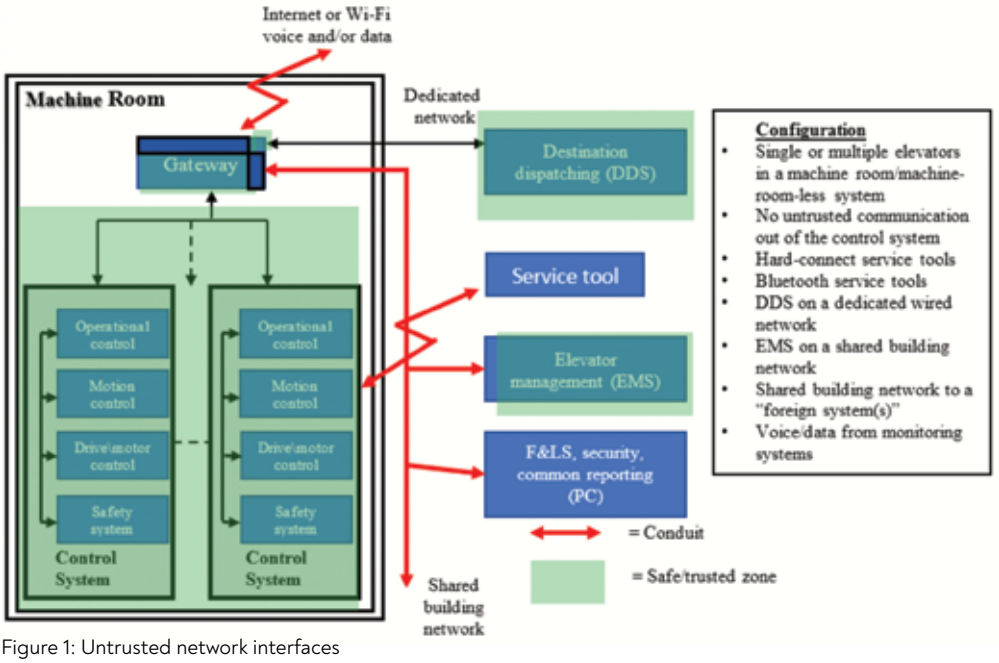

Figure 1: Untrusted network interfaces

At the first meeting, it was concluded that:

- Cybersecurity is a safety issue.
- There is a need for a worldwide standard for the elevating industry.
- The need is immediate, due to pressure from jurisdictions and customers.
- Until a standard becomes available, a guideline of best practices is needed.

Best Practices was completed in time, and a new work item was initiated by ISO to generate a cybersecurity standard for the VT industry. Care was taken with *Best Practices* to omit requirements that may constrain an ISO standard.

Due to length and time constraints, this article provides a condensed description of *Best Practices*. For further detail, readers are advised to review the guideline on the public portion of the NEII website (nationalelevatorindustry.org). *Best Practices* is loosely based on the ISA/IEC 62443 standard for worldwide applicability.

Scope

The guideline provides a path to aid elevator and escalator manufacturers in designing systems that provide measured protection from and management against network-based cyberattacks. The guideline focuses on the interfaces between the elevator or escalator system and the internet, building-area networks and untrusted systems. Maintenance and service tools used by technicians are included and treated as untrusted systems. The approach was to use industry best practices as guidance until such time a comprehensive cybersecurity standard for elevators and escalators becomes available.

Architectures Considered

The guideline is primarily targeted to interface points where the elevator or escalator system has communication with untrusted entities. While the guideline is focused on interfaces with other systems and networks, service tools — whether wired or wireless — are covered. Figure 1 depicts an elevator system's architecture and parts of the system at risk. This example applies equally to escalator control systems.

Since it is an example, actual implementations will vary. The guide depicts several examples. For brevity, only one is shown in this article. The interfaces included in the scope are:

- Connection points that interface with the internet either physically or wirelessly
- Connection points that interface with a physical or wireless building network
- Serial communication interface with a fire- and life-safety system (physically isolated wire interfaces are exempt.)
- Connection to intelligent service tools, wired or wireless
- Intelligent service tools (e.g., PCs)
- Trapped-passenger alarm systems, if they can accept downloaded software or elevator interaction
- Communication links that connect outside the elevator and escalator system/spaces

The safe/trusted portions of the systems are not considered in the guideline; they are covered by the semitransparent green areas in Figure 1. While a cybersecurity architecture best practice should consider a layered approach in the safe/trusted zones, this topic was deferred to a more comprehensive standard. It should also be noted that most systems will contain multiple trusted zones. Figure 1 depicts a complex installation in which the destination and management systems communicate over a network via a gateway that interacts with a cloud.

Cybersecurity Process Lifecycle

The fundamental basis of *Best Practices* is a strong cybersecurity process lifecycle. This lifecycle requires adequate training, tools, resources and processes to harden and protect the elevator and escalator system from cyberattacks. The lifecycle approach is also a fundamental premise of best

Continued

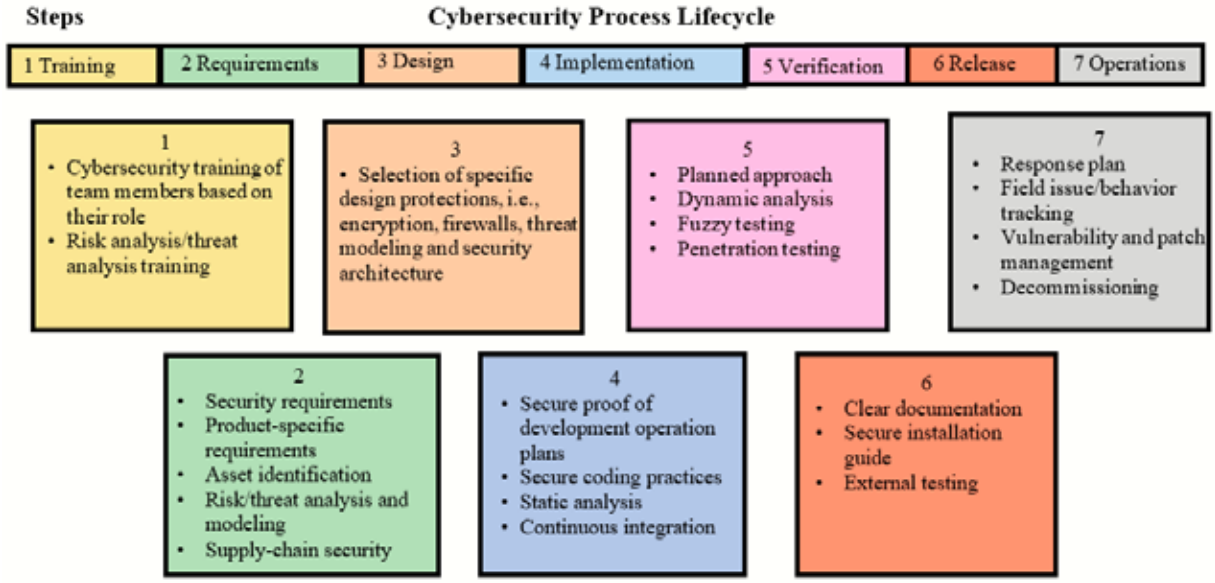

Figure 2

practices utilized for most cybersecurity standards and approaches.

The lifecycle approach recommended contains seven distinct functions, which are further described in the following sections. The important point is the functions described are considered the basis of a cybersecurity plan, no matter how many steps an organization has overall.

Training

To ensure an appropriate level of security for an elevator or escalator installation, each employee participating in the cybersecurity lifecycle requires adequate training tailored to his or her particular role. This includes, but is not limited to, developers, line and upper management, maintenance staff and procurement specialists. All employees participating in the cybersecurity lifecycle need to generally understand what cybersecurity is about, the current best practices and how to apply them, the system to be secured, and the risks induced by cybersecurity threats. It is recommended that the training team include cybersecurity specialists. In addition to general cybersecurity training, it is essential that the team performing the risk or threat analysis has up-to-date knowledge about relevant standards like ISO 14798 and can work according to relevant best practices.

Requirements

The process of managing cybersecurity requirements of an elevator or escalator system is effectively a process of managing risk. To achieve a product with an acceptable level of security, it is necessary to create a set of meaningful measures and controls that mitigate the various risk events threatening the system. Since identifying assets and gathering possible security risks is a creative and cooperative process, seeking professional external support (e.g., to moderate workshops) might be a valuable addition when no internal expertise is available.

Process

The following process should be followed for determining security requirements:

- Identify assets and level of tolerable risk.
- Conduct an initial risk assessment: identify threats and risks to the assets, determine likelihood and impact of risk events, determine unmitigated cybersecurity risk and define security-level target for the system.
- Create security requirements.
- Further iteration of risk assessment: evaluate existing countermeasures, reevaluate likelihood and impact of risk events and determine residual risk.
- Document cybersecurity requirements, assumptions and constraints.

The risk assessment should be based on test results and updated every time changes are made to the system or when the threat landscape changes significantly (e.g., new software vulnerabilities are published).

Requirement Process Guidelines

Asset and System Under Consideration Identification

To date, the major safety requirements of VT systems have been physical safety of people and, secondarily, equipment. To address these requirements, ASME A17.1 has relied on physical devices and safety-chain components. Since most systems did not communicate outside machine rooms, data protection was never a major consideration. Data concerns have been mostly where the software for safety-related functions (fire service) has been changed/updated and now behaves differently, without traceability. Due to the introduction of internet connections, Wi-Fi and software-based (Safety Integrity Level) safety systems, data may now be an integral part of a safety function and require codified protection. The guideline provides a detailed process for the requirements, risk tolerance and levels of mitigation.

Initial Risk Assessment

The initial risk assessment identifies the events/risks that threaten the system. Threats range from software-based viruses, worms, malware and ransomware to physical, unauthorized access, unintended actions and sabotage. To assess the

Continued

probability of threats occurring, the assessment should consider the adversary capability (sophistication and resources), as well as the vulnerabilities and access to the system. This form of security risk assessment is more complex than safety risk assessments. Assessing the motivation for an attack on an elevator, versus the sophistication and resources of the attacker, is difficult. The ability to assess an elevator car running at high speed into a terminal is easier to quantify.

The risk assessment system focuses on ISO 14798:2009, a specifically tailored risk-assessment standard for the elevator industry. It shows how this method can be adapted to deal with cyberthreats and attacks. Other risk-assessment standards are IEC 62443-3-2, ISO 27005 and *NIST SP 800-30 Guide for Conducting Risk Assessment*. *Best Practices* does not prohibit any risk-assessment standards, since all are viable and any restriction of a standard has been deferred to ISO to determine. Additional input about possible threats is given, for example, in NIST SP800-30, BSI Group (formerly the Engineering Standards Committee) Top 10, Open Web Application Security Project (OWASP) Top 10, Common Attack Pattern Enumeration and Classification (CAPEC) or other threat catalogs, which are kept up-to-date and distributed by several relevant organizations.

Selection of Security Requirements

Following the initial risk assessment, meaningful countermeasures must be chosen to mitigate assessed risks exceeding the previously defined acceptable risk level. The best practice when creating/choosing countermeasures is the "defense in depth" approach. Countermeasures should not rely on a single line of defense, but utilize multiple layers of protection. If one line of defense breaks, the asset is still defended by at least another layer. Compensating countermeasures, such as physical access control or detective controls, may also be used to satisfy one or more security requirements.

In parallel to the development of the system's architecture and the assignment of its functionality, it is good practice to review and update base-threat modeling. Several approaches are practicable, such as Microsoft's STRIDE. This methodology answers the question, "What can go wrong with my system?" by systematically screening each component of your system for the possibility of spoofing (using a false identity), tampering (unauthorized modification of data or a system), repudiation (obfuscating responsibility for an action), information disclosure (unauthorized disclosure of valuable data), denial of service (reducing the availability of a service to possibly zero) and elevation of privileges (gaining higher privileges than intended by exploiting a design flaw or vulnerability).

If the threat model is kept up-to-date with the evolving architecture of the system, a comprehensive catalog of possible threats will be available. These threats can then be mitigated by choosing appropriate countermeasures, which can be incorporated into the next iteration of the system's architecture.

Documentation of Cybersecurity Requirements, Assumptions and Constraints

As with all requirements, cybersecurity requirements and assumptions need to be documented, sent down through the design process and included in the system test plan.

Externally Developed Component Security

The methods described above should be extended to components developed by external sources, whether commercial, off-the-shelf software, open-source software or developed specifically for the company. No matter how thorough the risk assessment (which includes selection of countermeasures and the security concept), it can be jeopardized by insecure elements among externally developed components.

Best Practices includes audits of suppliers, guidance for only buying from reliable suppliers and only outsourcing to trustworthy service providers and demanding contractual assurance of processes be adhered to. Further information can be found in ISO/IEC 27036-3 and IEC 62443-2-4. The guideline provides ideas about what you could demand from a security perspective from your suppliers/service providers.

Design

The goal of the design phase is development of the system's architecture. In this phase, all decisions are made regarding high-level design choices and which key components are used. Furthermore, during architecture development, the product's complete functionality should be outlined to the degree necessary to achieve an architecture that fits the required functionality. This outline could, for example, consist of the involved entities, resulting data flow and important security or non-security properties already assignable.

Due to the far-reaching effects of choices made during the design phase, this phase is especially prone to the introduction of security vulnerabilities. Flaws in the developed architecture might lead directly or indirectly to vulnerabilities that could be hard to identify at this high-level stage, since they might be very specific or only recognizable on a much lower level. Fixing these security issues is most efficient if they are identified as early as possible, preferably during the design phase. If security flaws are discovered only in later phases, such as during testing or operations, it becomes increasingly complex and expensive to deal with them. Therefore, it is very important to try to detect vulnerabilities during the design phase and use industry standard best practices to reduce the exposure.

Best practices include:

- The principle of least privilege, meaning a process or a user should, by design, not have higher privileges than necessary for the fulfillment of their task
- Attack surface identification and minimization
- Modular design methodology to reduce the impact of security threats
- Defense in depth, meaning no risk should be mitigated by a single measure, but by a set of layered measures still effective if one of the individual measures fails (also described in the requirements phase)

Continued

- Restricting the access of a user, interfacing system or task to adjust the data required for the respective functionality
- Preferring simple, proven, in-use concepts or components over unnecessarily complex, proprietary or inadequately tested ones
- Performing security design reviews on a regular basis to detect security requirements not yet addressed by the present design and checking whether the system's current architecture is in conformity with the best practices

Additional information regarding security best practices in the design phase can be found in IEC 62443-4-1 Practice 3, NIST SP 800-82, Chapter 5 and BSI ICS Security Compendium Chapter 5.6.

Implementation

At a minimum, the following main attributes associated with secure implementation should be followed:

- Use of secure coding guidelines
- Use of static analysis tools
- Unit testing of critical functions
- Analysis of third-party and open-source software
- The use of secure coding guidelines

Secure coding guidelines should list potentially exploitable coding constructs or designs that should not be used. These should be from real-world examples. Typically, they should also include a list of banned/deprecated functions. A best practice is to carry out continuous source code analysis during development. When developers check in the code, the code should automatically be analyzed for any possible security issues.

Verification, a Planned Approach

In addition to the normal testing and validation processes that are a part of product development, cybersecurity verification and test plans should be parts of a formalized process in the system verification phase. The following key activities related to security are important.

Dynamic Analysis

Dynamic analysis identifies memory corruption, race conditions, user-privilege issues and other critical security problems.

Fuzz Testing

Fuzz testing should be performed on all components that process data originating outside the security zone or component. A fuzz-testing plan should be created documenting testing that will be done. The plan should include a list of all components that will be fuzzed, a description of how the fuzzing will be done, whether smart fuzzing or dumb fuzzing will be done and the pass/fail criteria for the tests.

Penetration Testing

In addition to the use of fuzz-testing tools, various penetration-testing tools are recommended during testing. The test plan should have specific line items relating to the use of penetration-testing tools. Independent (third-party) risk analysis and penetration testing should be considered periodically.

Release

The documentation listed below and risk acceptance are suggested to be completed before product release.

Documentation

- Threat modeling and risk assessment (threat model with residual risks identified)
- Security requirement and secure design
- Security test plan
- Analysis reports
- Test reports
- Fuzz-testing report
- Internal penetration-testing report
- External penetration-testing report

User Manual

Administrator guidance should include all administrator responsibilities necessary for secure operation of the product, procedures for reporting security vulnerabilities and any security protocols that are mandatory or optional.

Installation Guidelines for a Secure System

Installation guidelines should list and explain all security configuration options present in the system and make note of their default and optional settings. The default configuration should be secure. Additionally, the installation manual should contain all field/external testing requirements to be performed before commissioning to create a secure installation.

Incident Response Plan

Documented procedures should be prepared for a structured reaction in case of an incident, including a responsible, accountable, consulted and informed matrix with contact details.

Operations

Where service is maintained, an inventory (including version control of hardware/software) needs to be recorded. If a vulnerability in hardware or software assets is detected, it is necessary to analyze and determine if the vulnerability has any impact on the asset.

Response Plan

Written procedures should be available to execute the necessary next steps in case of an incident (incident response plan). The response plan should contain the necessary information to deal with all kinds of conceivable incidents and is highly dependent on specific assets.

The company should also consider how to handle the decommissioning of an elevator or escalator system, since sensitive information might be stored on some components (IDs, credentials, parameter sets, etc.), which, if disclosed, might be used maliciously or provide insight into the asset and other linked assets. Erasing the information or physically destroying the asset might be necessary. Decommissioning of an asset should be reflected in asset inventory.

Continued

Levels of Security

As described in Section 4.2 of the guideline, the security-level target of the system or component (zone) should be defined during risk assessment, and the achieved security level of the system or component (zone) should be verified through testing.

A review to verify the security level should also be redone during the lifecycle of the system when any of the following occur:

- Changes are made to the system
- New vulnerabilities relevant to the system are detected
- New security patches to system components are published by vendors or the open source community
- Periodically, as determined by the organization's policy

SL 0

Security levels (SLs) can be described as the skill level and motivation of the attacker. In SL 0, no specific requirements or security protection are necessary. Through risk assessment, it has been determined that the system does not require specific security requirements, for example, because consequences of misuse are determined to be negligible. When assessing if a security level has been achieved, SL 0 can indicate that a subset of countermeasures for SL 1 have been implemented, but full SL 1 is not met.

SL 1

Protection from casual or coincidental violation is needed. The system should be protected against casual attackers with low skills or unintentional misuse. Protection requires a basic level of security controls to ensure confidentiality, integrity and availability of data, and to enforce authentication, authorization and accounting of access. For example, security controls according to SL 1 do not require unique authentication of users and devices. A recommended set of controls for SL 1 is provided in the ISA/IEC 62443-3-3 standard referenced in the guideline.

SL 2

Protection from intentional violation using simple means with low resources, generic skills and low motivation is needed. The system should be protected against attackers who have the tools and skills to misuse generic information technology systems, such as web-based applications, but lack specific knowledge on elevator and escalator systems and are not specifically targeting these systems. The motivation of the attackers can be monetary gain (through ransomware) or reputation gain, for example. In contrast to SL 1, protection according to SL 2 requires security controls implemented in a more granular manner. For example, users and devices should be authenticated uniquely.

SL 3

Protection against intentional violation using sophisticated means with moderate resources, elevator and escalator system-specific skills and moderate motivation is likely. The system should be protected from highly skilled attackers knowledgeable about security and elevator or escalator systems and who are specifically targeting those systems. An attacker going after an SL 3 system will likely use attack vectors that have been customized for the specific, targeted system. The motivation of the attackers may include blackmail, revenge (disgruntled former employee) or sabotage (industrial competitor). Controls for SL 3 are outside the scope of the guideline.

SL 4

Protection from intentional violation using sophisticated means with extended resources, elevator and escalator system-specific skills and high motivation is likely. The system should be protected against highly skilled attackers knowledgeable about security and elevator or escalator systems and that are specifically targeting those systems with extended resources and high motivation. This is similar to SL 3, but with SL 4, the attacker is even more motivated and prepared to spend extended periods of time and resources to plan and execute the attack. Controls for SL 4 are outside the scope of this guideline. A more detailed description of the SL process can be found in IEC 62443-3-3.

Security Measures

This section recommends the use of security measures for SL 1 and 2 based on the systems requirements defined in Table 6 (a) of the ISA/IEC 62443-3-3 standard. A detailed description of the requirements can be found in that standard.

Security of Service Tools

Tools used for servicing elevators or escalators should employ effective security measures. Service tools can be broadly put into three categories:

1) Those that can communicate with the elevator and escalator remotely from anywhere on the internet
2) Those based on low-/moderate-range proximity wireless technologies such as Wi-Fi and Bluetooth
3) Those that require physical proximity to the equipment and that a cable/wire be plugged in, such as USB or serial cable

Good cybersecurity practices involve an in-depth strategy that implements multiple security measures based on the level of accessibility to the device and impact to the system if compromised. In this regard, accessibility in the above three cases would require different types of security controls, depending on the extent of system control capable through the service tools. For example, if the service tool is capable of writing configuration changes remotely from the internet, then a multifactor authentication is recommended. This could include a combination of device authentication using certificates or pre-shared unique keys, passwords and whitelisting. At minimum, a unique password-based scheme is required, even when physical access is required.

PC Hardening

In addition to security controls for authentication and encryption, an important requirement for service tools is to ensure the machine (PC/mobile device) on which the tool is running is sufficiently hardened, and proper access control is employed. Using strong passwords for all user accounts,

Continued

maintaining good antivirus and anti-spyware software, applying patches on a timely basis, turning on software firewall options and restricting use of the machine to the function intended are some of the key elements in a hardening guide. Such hardening guidelines are published by National Institute of Standards and Technology (NIST) and other organizations and are recommended for any third party involved in using service tools or servicing the elevator.

Summary

Best Practices was a cooperative effort under the NEII banner among major manufacturers with participation from various design centers around the world. The initial meeting set the goal of a fast-track effort to generate a guideline in approximately one year, in time for the ISO Plenary Meeting to initiate a working item to address cybersecurity concerns facing the elevator/escalator/moving-walk industry. Due to the criticality, the Plenary Committee voted to initiate a two-year work item to address cybersecurity.

Care was taken in developing the guideline to create a document that has worldwide applicability with enough guidance and references to allow all vendors to create a cybersecurity program, no matter their present level of maturity on the topic. Since it is reasonably assured that the ISO team will include many of the same personnel who participated in the guideline, there is a probability that the guideline and any standard generated will align.

While timely generation of a standard is critical, there are several difficult considerations that will need to be addressed in the standard that are not addressed in *Best Practices*:

- Determine if an industry-specific standard is required.
- Establish a classification of cyberthreats to lift systems, devices and networks.
- Define security levels by lift functions.
- Address the limited selection of applicable cyberrisk analysis tools.
- Determine which parts of the cybersecurity lifecycle are required, versus recommended.
- Establish a cybersecurity testing/certification process.
- Determine how often field upgrades and maintenance are required.

While time pressure concerns from jurisdictions and customers are understood, solving these issues on a worldwide basis will be challenging.

References

[1] Federal Office for Information Security. *BSI ICS Security Compendium*, V1.23, Bonn, Germany.

[2] BSI. "BSI Analyses About Cybersecurity," BSI Top 10

[3] International Society of Automation (ISA)/International Electrotechnical Commission (IEC). CAPEC V 3.0 Common Attack Pattern Enumeration and MITRE Corp. "Security for Industrial Automation and Control Systems, Parts 2-4: Security Program Requirements for IACS Service Providers."

[4] *ISA/IEC 62443-2-4 2017*. "Security for Industrial Automation and Control Systems, Parts 2-4: Security Program Requirements for IACS Service Providers"

[5] *ISA/IEC 62433-3-3: 2013*. "Industrial Communication Networks – Network and System Security - Part 3.3: System Security Requirements and Security Levels."

[6] *ISA/IEC 62443-4-1:2018*. "Security for Industrial Automation and Control Systems - Part 4 - Secure Product Development Lifecycle Requirements."

[7] *ISO/IEC 27036-3:2013 Information Technology – Security Techniques – Information Security for Supplier Relationships* – Part 3: Guidelines for Information and Communication Technology Supply Chain Security.

[8] *ISO 14798:2009 Lifts (Elevators), Escalators and Moving Walks – Risk Assessment and Reduction Methodology*

[9] *ISO 27005:2018 Information Technology – Security Techniques – Information Security Risk Management*

[10] U.S. Department of Commerce. *NIST SP800-30 Rev .1 Guide for Conducting Risk Assessments National Institute of Standards and Technology*.

[11] U.S. Department of Commerce. *NIST SP800-82 Rev .2 Guide to Industrial Control Systems (ICS) Security National Institute of Standards and Technology*.

[12] The OWASP™ Foundation. "OWASP ASVS Testing Guide Open Web Application Security Project."

Kevin L. Brinkman has more than 28 years of elevator- and lift- industry experience. He has been responsible for codes and safety at NEII since 2015. In his role as vice president, codes and safety, he focuses on code development and adoption, along with safety of elevator workers and the riding public. Brinkman serves on a number of influential code-development committees. He is a member of the ASME A17 Standards Committee for the ASME *A17.1 Safety Code for Elevators and Escalators* and is chair of the ASME A17 Code Coordination and Editorial Committee, as well as a member of several other A17 working committees. Brinkman also serves on the International Code Council/ANSI A117.1 Committee, NFPA 5000 and 101 technical committees, and is involved in the International Building Code process.

Barry Blackaby has more than 35 years of elevator experience in the industry. He recently retired from Otis, where he was associate director of worldwide electrical code. He is now managing director of B. Blackaby and Associates LLC. Blackaby served two terms as chair of the A17.1 Electrical Committee and two terms as chair of the Earthquake Committee. He is currently a member of the A17 Standards, Electrical and Earthquake committees and a contributing member of the International Standards Committee. He is also task group leader for Elevator and Escalator Industry Cybersecurity Best Practices.

Learning-Reinforcement Questions

Use the below learning-reinforcement questions to study for the Continuing Education Assessment Exam available online at www.elevatorbooks.com or on p. 127 of this issue.

- Why is a strong cybersecurity process lifecycle a fundamental basis of *Best Practices*?
- What should be included in product documentation?
- What should an incident response plan include?
- What are the *Best Practices* recommendations for the use of security measures for SLs 1 and 2?
- How can service tools be categorized?

ELEVATOR WORLD

ONLINE
CONTINUING EDUCATION

ELEVATOR WORLD Continuing Education Assessment Examination Questions

- Read the article **"Cybersecurity Best Practices"** (p. 95) and study the learning-reinforcement questions at the end of the article.
- To receive **one hour (0.1 CEU)** of continuing-education credit, answer the assessment examination questions found below online at www.elevatorbooks.com or fill out the ELEVATOR WORLD Continuing Education reporting form found overleaf and submit by mail with payment.
- Approved for Continuing Education by **NAEC for CET® and CAT®.**

1. On which of these items is *Best Practices* **not** focused?
   a. The interfaces between the elevator or escalator system and the Internet.
   b. Cybersecurity certification.
   c. Building area networks.
   d. Untrusted systems.

2. Which of these is included in the scope of *Best Practices*?
   a. Maintenance and service tools used by elevator/escalator technicians.
   b. The definition of SLs by lift functions.
   c. Which parts of the cybersecurity lifecycle are required versus recommended.
   d. When upgrades should be required in the field.

3. Which of the following parts of elevator system architecture are **not** addressed?
   a. Building area networks.
   b. Service tools.
   c. Internet or Wi-Fi voice and/or data.
   d. Internal communication buses.

4. Which is **not** a part of the initial risk assessment?
   a. Creating security requirements.
   b. Identifying threats and asset risks.
   c. Determining the likelihood and impact of risk events.
   d. Defining an SL target for the system.

5. Best practices do **not** include:
   a. The principle of least privilege.
   b. Modular design methodology.
   c. Defense in detail.
   d. A preference for simple, proven concepts over complex or proprietary ones.

6. On which components should fuzz testing be performed?
   a. All that process data originating outside the security zone or component.
   b. All that receive data originating outside the security zone or component.
   c. Only on those considered primary lines of communication.
   d. All those considered lines of communication.

7. Which is (are) considered best practice to be included in documentation?
   a. Threat modeling and risk assessment.
   b. A security test plan.
   c. Analysis and test reports.
   d. All of the above.

8. When should the SL target of the system or component (zone) be defined?
   a. During product brainstorming.
   b. During risk assessment.
   c. During the first installation.
   d. After each installation.

9. Which of the following type of authentication is recommended if the service tool is capable of writing configuration changes remotely from the internet?
   a. Multifactor.
   b. Individual.
   c. Selective.
   d. Specific.

10. Which is **not** an example of PC hardening?
    a. Maintaining antivirus software.
    b. Applying update patches.
    c. Using the machine for general purpose.
    d. Turning on software firewall options.

Continued

ELEVATOR WORLD Continuing Education Reporting Form

Article title: **"Cybersecurity Best Practices"** (EW, April 2020, p. 95).

Continuing-education credit: This article will earn you one contact hour (0.1 CEU) of elevator-industry continuing-education credit.

Directions: Select one answer for each question in the exam. Completely circle the appropriate letter. A minimum score of 80% is required to earn credit. You can also take this test online at www.elevatorbooks.com.

Last name: _____

First name: _____ Middle initial:_____

CET®, CAT® or QEI number:_____

State License number:_____

Company name:_____

Address:_____ City:_____

State: _____ ZIP code:_____

Telephone:_____ Fax:_____

E-mail:_____

– – – – – – – – – – – – – – – – – –

This article is rated for one contact hour of continuing-education credit. Certification regulations require that we verify actual study time with all program participants. Please answer the below question.

How many hours did you spend reading the article and studying the learning-reinforcement questions?

hours: _____ minutes: _____

Circle correct answer.

1.	a	b	c	d	7.	a	b	c	d
2.	a	b	c	d	8.	a	b	c	d
3.	a	b	c	d	9.	a	b	c	d
4.	a	b	c	d	10.	a	b	c	d
5.	a	b	c	d					
6.	a	b	c	d					

Signature: _____

Payment options:

Check one:
- ❑ $35.00 – Course fee
- ❑ Payment enclosed (check payable to Elevator World, Inc.)

Charge to my:
- ❑ VISA
- ❑ MasterCard
- ❑ American Express

Card number: _____

Expiration date: _____

Signature: _____

To receive your certificate of completion using the mail-in option, send the completed form with questions answered and payment information included to: Elevator World, Inc., P.O. Box 6507, Mobile, AL 36660.

To receive your certificate of completion online, visit www.elevatorbooks.com and follow the instructions provided for online testing.