International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Vulnerabilities in Cyber Security

Josh Pappachan John[1], Om Ashok Jadhav[2], Gaurav Vitawkar[3]

Department of MCA In ASM IMCOST, Thane, Mumbai University
jjoh6418@gmail.com[1], omjadhav39@gmail.com[2], gaurav.vitawkar17@gmail.com[3]

ABSTRACT

The question about the future of the digital economy is able to tailor cybersecurity technical solutions and not technical factors working together with business units, executives, providers, and end-users in the forming vitamin cyber USERNAME. In the last years, many targeted cyberattacks were performed against the critical infrastructures of all digital economies in the world.

It has led to permanent or long-term damage to critical infrastructures, and a constant increase of cyber and physical security-related events continue raising concern. Therefore, the paper looks into the vulnerabilities within critical infrastructures that attackers uses in carrying out these types of attacks. In that respect, the paper singles out software security vulnerabilities, poorly designed network architectures, and weak configurations as major factors that are used in the successful attack of major infrastructures.

It also identifies the non-technical vulnerabilities like talent gap, budget constraints, lack of management priority, weak mechanisms across geographical regions for the multinational businesses that make them weak to have a successful attack in the vital infrastructures.

Keywords: Cyber Attacks, Vulnerabilities, Weak Infrastructure, Loopholes, Network Design Vulnerabilities

Introduction

Indeed, the integration of digital technology has greatly enhanced the efficiency of business. However, this development has made businesses highly vulnerable to cyber attacks. Cyber-warfare is no longer the prototype image of hackers working with hoodies; instead, it has emerged as a serious threat capable of dislodging entire infrastructures and defaming the reputation of countries.

Critical infrastructure forms the backbone of modern society in any country. At the same time, it has become vulnerable to cyber attacks. This paper examines the modus operandi of these attacks. It first discusses the impact on North American industries; from power grids to financial systems to illustrate how no sector is immune. Then it classifies vulnerabilities under three technical categories: software bugs, inadequate network security, and faulty configurations, and non-technical factors that open systems to attack.

Eventually, it is hoped that by knowing these vulnerabilities, our defenses against cyber threats can be strengthened so that, hopefully, the war could be eventually won byte by byte.

Vulnerabilities in Cybersecurity

Inadequate Input Validation

It's a great technique for security that ensures an extra layer of security from an attacker who tries to probe for unauthorized files, infrastructure, or privilege escalation. It acts as a guardian visible screens the data that is going in and checks whether it is legitimate data and not some malicious code that tries to break through the system. Only valid data or authorized data is allowed to enter the system while unauthorized data or invalid data is kept out or filtered before it enters the system.

Lack of Bound Checking

The lack of proper validation to limit input within a particular range may cause the program to crash unexpectedly. It allows an attacker to insert invalid input in the form of very large numbers in an array that will definitely make the service crash. A poor coding practice leaves behind the loopholes to be exploited by the attackers, and it causes great loss and damages to the firm or company.

Command Injection

Command injection is a horrifying activity for malicious attackers that inject commands and various codes whose execution results from improper coding. There are basically two types of command injection: SQL, Structured Query Language, and OS command injection. In case the command happens to get executed, in turn, the attacker gets the privilege or the capability targeted to use and compromise the system.

Improper Limitation of a Pathname to a Restricted Directory Traversal

This is a massive risk when an application gives the user the ability to manipulate the file path in such a way as to exploit this feature and give access to files or directories that sit outside of the intended structure. This is usually found in cases where input validation or sanitizing of user input, used as part of the file path has not been done properly; hence, unauthorized access is given to sensitive files or directories.

For example, if an application constructs a path to a file from user input and does not implement sufficient filtering of directory traversal characters, (such as ".//" used under Unix-based systems and ".\\" for windows), the hacker will tamper with the input so as to cause navigation to restricted directories. In this case, there will be unauthorized access to sensitive data files or vital directories.

In a bid to ensure that directory traversal vulnerabilities do not arise, developers should:

1. Validate and sanitize all input used to construct file paths
2. Validate and sanitize all input used to build file paths.
3. Implement safe APIs made available either by the language or by the framework you use for handling file paths; for instance, Python has the os.path module.
4. Apply correct access control so that a user can access only those files and directories for which he's been given authority
5. Do not directly use user-given input within methods dealing with files without validating/sanitizing such input.

Poor Code Quality

Poor code quality refers to software that is not well-written or maintained, which often leads to security vulnerabilities. This can be for many reasons as elaborated below:

Lack of CM and base lining.

Inadequate testing and reviewing processes. Use of any unsafe functions or APIs that are not thoroughly validated.

Lack of Input Validation and Output Encoding.

Inability to apply the Principle of Least Privilege and access controls.

Secure development practices are intended to avoid vulnerabilities by writing better code in the first place. This involves:

Regular code audits for security issues and testing. Train developers in secure coding practices.

By following secure coding guidelines and standards such as OWASP Top 10.

Principles like least privilege, defence in depth, Addressing poor code quality involves improving the overall development process to ensure that security is considered from the initial design phases through to deployment and maintenance.

Permission, Privileges, and Access Controls

1. Permissions:

Permissions are the rules specifying the activities a user may do in a system. Typically, it would mean read, write, or execute collection of files or hierarchy of directories or running any systemic resources. Permissions, in Unix-like systems, are managed as part of attributes like read, write, and execute for owners, group members, and others. In contrast Windows manages permissions using Access Control Lists.

2. Privileges:

Privileges are the quantifier over which a user or system entity has access over resources. The higher the privileges for a user, the larger the access and the set of actions that he can perform over a system. Privilege escalation is the process through which an attacker exploits a system to gain higher privileges than those granted in the initial authorization. These kinds of privileges assist an attacker in beating security measures and gaining unauthorized access.

3. Access Controls:

Access controls Here refer to the mechanisms and policies that enforces security rules and restriction of who can access what resource. It involves authentication, such as confirming a user's identity as what he says he is; may include authorisation where specified permission if provided for the kind of access for which the user can have to certain resources and perform some kinds of actions, given his identity and roles. The mechanism includes auditing, which monitors and logs attempts at access for accountability and other purposes.

Impact of Inadequate Controls:

In case there is not proper permission, privileges and access control in the critical infrastructure systems, then following are some of the risks and possible impacts:

Unauthorized Access: The vulnerability can be exploited by the attackers so as to gain unauthorized access to sensitive systems or data.

Data Breaches: An attacker may steal sensitive information since the proper controls are not implemented; thus, there is a data breach of confidentiality.

Disruption to Service: Adversaries can disrupt services/operations by taking critical systems under control, down time, loss of productivity.

Damage/Loss: Loss of critical infrastructure components, data tampering can result due to unauthorized access, that is monetary, financial losses/fraud/ theft.

Reputation Loss: Incidents occurring due to lack of adequate controls can cause severe reputation and credibility damage to the organization among its stakeholders, customers as well as the general public.

Mitigation Strategies:

In order to mitigate such risks, The following robust security measures shall be in place by the organization:

Role-Based Access Control RBAC: RBAC will ensure that access rights are by role in the organization. This will limit the chance of too many privileges on the hands of a user.

Least Privilege Principle: A user shall be assigned the least privilege to enable him to perform his duties. In this way, when an account or system is compromised it limits the extent of the damage.

Regular Audits and Monitoring: Run some security audits regularly, that may highlight vulnerabilities, and monitor the access logs to get suspicious activities.

Strong Authentication: Use multi-factor authentication that will actually verify the user's identity before allowing access to sensitive systems.

Based on this:

The risk of cyber-attacks can be decreased significantly by implementing and maintaining effective permission, privileges, and access controls; such controls can prevent critical infrastructure from being damaged or operationally disrupted.

Improper Authentication

Weak Authentication Methods:

Weak forms of authentication, such as simple passwords and missing multi-factor authentication-MFA-make the account vulnerable for a number of reasons, including:

1. Guessing Passwords/Brute Force Attacks: The attacker can run automatic programs that try a combination of characters to guess passwords or even perform brute force attacks to gain entry into the account.
2. Stolen Credentials: In case of compromise of credentials through phishing, social engineering, or some other methods. What makes it quite easy to be used by the attacker to log in using stolen credentials is weak forms of authentication.

By-passable Authentication:

When multiple, different ways of exploiting identity authentication exist, either because software has vulnerabilities or may be misconfigured, then there are the potential possibilities that :

1. Gain Unauthorized Access: It fully bypasses the authentication mechanism, thereby letting have direct access to critical systems or data

2. Privilege Escalation: a person who has already broken into the system can raise their access levels much higher than what was actually granted to him.

Implications Critical Infrastructure End

Operational Disruption: Unauthorized access may disrupt the operation of critical infrastructures; such disruption may also lead to some downtime or loss of service availability in related sectors, and, ultimately, damage in the energy or transport sector.

1. Breaches of Sensitive Data: Many critical infrastructure sectors possess confidential data. Once accessed, that becomes a breach of sensitive data.

2. Regulatory requirement: Security standard and regulation non-compliance can cause legal and financial implication for the organization responsible for those critical infrastructures.

Insufficient Verification of Data Authenticity

The lack of proper data to be transmitted authentication, especially on the grounds of CSRF, puts them at serious security and integrity risk. It is for that regard that this paper delves into the impacts such vulnerability has on critical infrastructure systems, as well as mitigation to those impacts:

Understanding CSRF and Its Impact:

CSRF comes into play when an attacker induces the web browser of a user to perform undesired requests to a web server to which the user is authenticated in. This exploit abuses the trust that a site implies in a user's browser and allows various malicious activities:

1. Unwanted Actions: An attacker can request actions be performed on behalf of an authenticated user, like transferring money, altering settings or deleting data.

2. Data Modification: An attacker can modify data in transit between the client and server, changing vital information or even inserting malicious content into a stream of otherwise legitimate data.

3. Server Compromise: CSRF attacks can also be used to compromise the running severity of the Web server itself. Since CSRF might support unauthorized commands, it might even lead an attacker to acquire a foothold in the network.

Implications for Critical Infrastructure.

Speaking of critical infrastructure, reliability and security of the systems are of vital condition; therefore, the outcomes of CSRF vulnerabilities are extremely hazardous in such situations:

Operational Disruption: The executions of unauthorized actions or data alteration disrupt operations. It leads to downtime, service disruption, or erroneous system behavior in such a situation.

Data Integrity: Data in transit can be altered which degrades and distorts the integrity and accuracy of critical information used for decision making in such a situation, and Operational efficiency.

Trust and Reputation: Incidents occurring due to CSRF attacks will result in the loss of trust among stakeholders or the users and also have a bad impact on the reputation of the organization.

Cryptographic Issues:

Most specifically, encryption techniques with weaknesses, hashing methods, and vulnerable libraries of SSL are the most critical risks that greatly threaten the security of information being transferred through critical infrastructure networks. Therefore, in what follows, we go into the details of such issues and discuss mitigation techniques:

Weak Encryption Techniques:

When data is transmitted from one client to another over a network with weak encryption, each of the risks below could actually materialize :

1. Data Interception: An attacker may eavesdrop by intercepting network traffic in an attempt to gather sensitive information, including but not limited to usernames, passwords, and other vital information sent in clear text.

2. Data Tampering: As data will be unencrypted, an attacker may alter the data packets in transit and send information to cause unauthorized changes in information or the command sent to installations and critical infrastructure systems.

3. Man-in-the-Middle: Weak encryption gives the opportunity to an attacker to put his(media) in between communication channels-man in the middle- and then intercept and probably change data that the client and server are exchanging during communication.

Vulnerable Cryptographic Components:

These are driven primarily by the following exposures:

1. Insecure Hashing Algorithms: Insecure hashing algorithms could be exploited to reverse engineer passwords or other sensitive information from hashed values.

2. Poor Pseudorandom Number Generation Design: Random number generation that is done inadequately can result in easily predictable cryptographic keys or initialization vectors, thus weakening encryption strength.

3. Unpatched SSL/TLS Libraries: Vulnerabilities in libraries handling SSL and TLS operations could be used to decrypt intercepted traffic or impersonate legitimate servers, thus compromising data confidentiality, integrity.

Vulnerable Cryptographic Components:

These are driven primarily by the following exposures:

Insecure Hashing Algorithms: Insecure hashing algorithms could be exploited to reverse engineer passwords or other sensitive information from hashed values.

Poor Pseudorandom Number Generation Design: Random number generation that is done inadequately can result in easily predictable cryptographic keys or initialization vectors, thus weakening encryption strength.

Unpatched SSL/TLS Libraries: Vulnerabilities in libraries handling SSL and TLS operations could be used to decrypt intercepted traffic or impersonate legitimate servers, thus compromising data confidentiality, integrity.

Network Security Vulnerabilities:

It is very crucial to make the network architecture secure, so as to enable remote monitoring and access to business processes, while denying any unauthorized traffic, in order to maintain the integrity and secrecy of systems that are critical for infrastructural operations.

Below is how security zones and access control rules are important in reducing network security vulnerabilities. Importance of Secure Network Design

1. Remote Access and Monitoring: Many critical infrastructure systems need remote access and monitoring for operation efficiency. Such activation without security measures weakens these systems to a number of risks, including unauthorized access and data breaches.

2. Prevention of Unauthorized Traffic: All kinds of unauthorized traffic-maliciously intended from the bad guys or unintentional due to misconfigured devices or software-is straddling operations, exposing sensitive data, and probably system compromise or even downtime.

Implementing Security Zones and Access Control:

Security zones and access control are yet again a network security framework that basically breaks the whole network into various parts, each of which requires or needs some specific kind of security.

1. Segmentation: The network is divided into security zones based on the sensitivity of systems and data hosted. Critical infrastructure components, for example, might be control systems and shall go to a highly restricted zone while less critical things like the administrative offices might be in a less restricted zone.

2. Access Control Rules: Clearly define and enforce access control rules between security zones to restrict traffic flow to access in accordance with business needs and security policies, such as only allowing selected personnel and devices to communicate with systems used to support critical infrastructures.

3. Firewalls and Gateways: It will be mandatory to install firewalls and gateways in the boundaries between security zones in order to inspect and filter the in-bound and out-bound traffic. Firewalls and gateways must be configured in a way that they implement an access control policy to block unauthorized traffic along with the logging of network activity for monitoring and analysis purposes.

4. Virtual Private Networks (VPNs): Require VPNs for remote access to critical systems. These give the user an encrypted tunnel to send information through, but also provide greater assurance on who is connecting to the network because additional authentication will be required.

5. Intrusion Detection and Prevention Systems: Implement an intrusion detection system that reviews all types of traffic sent across the network to identify suspicious activity, or probable security breaches. The intrusion detection system can identify and respond to unusual activity, like attempting to bypass access controls or exploitation of vulnerabilities.

Benefits of Security Zones and Access Control

a. Risk Reduction: Segregation of topology into different zones gives access control rules a shallow attack space. This makes sure that there is least possibility of any unauthorized access or the spread of malware across the network.

b. Regulatory Compliance: Access control and security zone best practices help organizations meet the set regulations, laws, and standards related to the protection of data and cybersecurity.

c. Continued Operative: In any case, critical infrastructure systems that are properly network segmented and access-controlled shall offer increased resilience against cyber threats. These systems shall continuously operate with reduced consequences from security incidents.

Poor Network Design

Poor network design is specifically worrying in terms of the absence of defense in depth. High risk accrues in case the essential security layers that include, though are not limited to firewalls, DMZs, and proper segmentation are missing. Details are provided below on the issues and recommended improvements towards ensuring security in critical infrastructure:

Problems Caused by Inadequate Network Design:

Lack of Defense-in-Depth: The defense-in-depth concept applies multiple defensive layers necessary to protect against different threats. If it is not applied, then there will be only a single layer of security used that in itself becomes the line of defense for the entire system, and, if breached, the whole system is at stake.

1. Direct Connection to Corporate Networks: A direct connection across critical infrastructures into the corporate network without appropriate segregation puts the sensitive operation at risk from less secure corporate environments.

2. No Firewalls and DMZs: The firewalls control traffic between the networks. The DMZ's provide an isolation area that isolates this critical infrastructure from the networks external to it. If they are not present, then there is nothing to stop access from the Internet, either if it is unauthorized or even an attack.

3.. Unrestricted Access to the Internet: The gains in the access line that allow direct access to the Internet from the critical infrastructures network allow the attackers to exploit the vulnerability remotely and increase the chance of a successful cyber-attack.

Proposed Changes Or Recommended Improvements:

In order to help avert all these risks and therefore improve the security of the CIs, best practices to the effect are shown below.

1. Defense-in-Depth Strategy: A "Defense-in-depth" approach is where multiple layers of security controls are deployed. When it comes to security control, three types can be used, physical, technical, or administrative. Therefore different types of threats can be effectively resisted.

2. Network Segmentation : network segmentation allows division of the network into its functional area or sensitivity basis. For example, Isolation of critical infrastructure systems from corporate networks prevents access by unauthorized individuals.

3. Firewalls and DMZs:

a. Firewalls: Firewalls implemented at key places in the network shall control as well as prevent traffic from entering the network. The implement firewall rules that will follow the strict access controls on any computers, servers, or applications.

b. DMZs: It is required to form DMZs that shall segregate critical systems from the external networks. This is known as the buffer zone, and it forms the DMZ where services are hosted that need to be accessible from the Internet and protection in the internal network.

4. Secure Remote Access:

a. Implement Virtual Private Networks for secure access to remote critical systems access. As they encrypt the traffic, moreover, they have an option of authentication also; thus, they refuse unwanted people access to critical systems.

b. Implement MFA to perform remote access so as to ensure that only authorized personnel or users, properly authenticated, associate to, make a query, or input data on sensitive systems.

5. Intrusion Detection and Prevention Systems (IDPS) Deployment: IDPS detect tracking activities in network traffic and simply respond to a potential threat in real time.

6. Regular Security Audits and Penetration Testing: Occasionally making security audits helps to identify and reduce the various vulnerabilities in the network design. Penetration testing can be, therefore, described as attacking a system to establish the action a threat may portray.

Credential Control Management:

Credential Control Management is a very important cybersecurity topic that takes on even greater significance when it comes to critical infrastructure. Poorly managed credential control, such as when the password is transmitted in clear text; displayed on the web; or, generally, insecurely stored, can be highly susceptible. This article explains what's at stake and how to effectively counteract:

Issues with the Control of Credential Management:

<u>Clear Text Transmission:</u>

a. Unencrypted Credentials: If the transmission of credentials across the network is in a clear text form, then it is pretty easy for an attacker to sniff them by using a network sniffing tool.

b. Man-in-the-Middle Attacks: If communications between two parties are not encrypted, then an attacker may intercept them. They may even modify the communications.

<u>Insecure Database Configuration:</u>

a. Exposed Administrator Passwords: Insecurely configured database service that will actually give away the administrator password in some web page or other interface provides attackers an open door to high privilege accounts.

b. Weak Access Controls: Weakly configured access controls create the possibility of entering sensitive database info for a potential hacker.

<u>Improperly Secured Password Hash Files:</u>

a. Weak Hashing Algorithms: Storing passwords with weak hashing algorithms or even old ones that are not supported helps an attacker to crack the hashed passwords.

b. Insecure Storage: It is highly insecure to store these hash files in any location that might be accessed by other unwanted users.

CONTROL MEASURES:

The following strategies will help to move credential control management forward in providing an added layer of defense to organizations' critical infrastructure:

1. Implement Robust Encryption:

a. TLS/ SSL for Data Transfer: All authentication credentials and other sensitive information should be transmitted across the network by making use of strong encryption protocols like TLS/SSL.

b. End-to-End Encryption: There should be an implementation of end-to-end encryption so that data remains secure right from its origin to destination.

2. Secure Configuration of a Database:

a. Do Not Output Credentials: Under no circumstances should password or any other form of sensitive information be output in web pages or other public interfaces available.

b. Database Access Controls Ensure that databases are installed with access controls, which would limit access to only those who are authorized.

3. Secure Password Storage:

a. Strong Hashing Algorithms: Use strong, modern hashing algorithms like bcrypt, Argon2, or PBKDF2 to hash passwords safely.

b. Salting: Add a unique salt for every password before hashing to prevent rainbow table attacks.

Secure Storage Locations: Store hash files and other sensitive data in secure places where access is controlled.

4. Implement MFA:

Additional Authentication Factors: Additional factors like OTP, biometrics should be used apart from passwords to gain access to critical systems and services.

Talent Gap:

The shortage of cybersecurity talent is a nightmare for enterprises across the globe, with the demand for qualified cybersecurity experts increasing. This shortage hinders the ability of enterprises to fully protect themselves against cyber threats in a world where critical infrastructure is becoming more and more vulnerable. Here's a closer look at the issue and some potential strategies to address it:

Impact of the Cybersecurity Talent Gap:

1. Increased Susceptibility:

a. Inadequate Defense: Without proper numbers of qualified workforces, it is not easy to develop, monitor and manage systems' security defense. That.enable the systems to be attacked.

b. Delayed Response Since it takes a longer period for detecting and responding to the attack, understanding the cause and impact of the cyber incident is increased.

2. Operational Strain:

a. Overworked Staff: Existing cybersecurity teams can be over-stressed, which will ultimately result in burnout and decrease their overall performance.

b. Lack of Proper Skill Fit: Thestaff may be made to carry out duties for which they are not fully qualified, and that will negatively impact the standard of security operations.

3. Compliance Risks:

Regulatory Challenges: A lack of sufficient staff to deal with regulation and compliance can render organizations not able to keep up with the rigors, thereby exposing them to fines and legal actions.

Strategies to Offset the Talent Gap:

This is probably a multi-faceted approach that involves developing internal talent to deal with any eventualities, leveraging external resources in the form of strategic partnerships and alliances, and using technology effectively.

1. Grow from Within:

a. Training and Licensing: Invest in continuing education and certification programs to upskill existing employees. Give them an opportunity to acquire recognized cybersecurity certifications like CISSP, CISM, CEH, etcetera.

b. Career Development Pathways: Specify the obvious career development pathways for retaining and growing talent within the organization. Mentorship programs should be combined with appropriate rotational assignments to build diverse skill sets of both mainstay and contingent employees.

2. Enhancing Technology and Automation:

a. Security Automation: Ensure automation tools and technologies such as Security Orchestration, Automation, and Response or SOAR should perform the "knee-jerk" types of activities so the cybersecurity pros are left free to focus on more difficult challenges.

b. Intelligence Artificial and Machine Learning: Take advantage of AI and machine learning to broaden threat detection, analysis, and response capabilities - thereby relieving human analysts' workloads.

3. Promote Cybersecurity understanding:

a. Organization-Wide Training: Provide training in cybersecurity awareness to all employees so that they inculcate a culture of security in the organization. Train employees to recognize and act upon common threats such as phishing.

b. Executive Support: The leadership of the organization needs to understand the essence of cybersecurity and hence should allocate appropriate resources for support of security initiatives.

All of these systems form a part of the critical infrastructure and hence the competitive basis of any developed nation's economy. All of these systems are subject to a wide range of threats that can be technical or non-technical in nature.

Conclusion

Regional Variations in Cyber Readiness

1. Global Cybersecurity Standards:

a. Standardization: Global cybersecurity standards and frameworks shall be applied uniformly; for instance ISO/IEC 27001 and NIST Cybersecurity Framework-, across all business operations geographical regions.

b. Local Adaptation: They shall be adapted to local regulations compliance requirements and aligned to regional threats.

Protection of critical infrastructure is a very complex activity that has to be holistically addressed along a wide range of threat spectrums by implementing a technical and equally non-technical approach. Adoption of standardized cybersecurity practices internationally, robust security measures, investment in skill development, and alignment of perceptions by management will help minimize the vulnerabilities and improve the resilience of critical infrastructures.

Defense-in-depth strategies

Secure network architectures

Regular audits.

Skill Development-Invest in training programs and partnerships to minimize the talent gap

Management Alignment-Train executives and define a channel of clear communication between different tiers of management

Global Standards-Adopt and contextualize global cybersecurity standards throughout all geographies of operation

Resource Prioritization-Risk assessment to be done and resources to be provided accordingly. Application of security practices will be uniform across the globe.

By putting each of these areas in the center of its attention and activity, an organization can significantly reduce the possibility of a successful attack against its critical infrastructure and, because of that fact, maintain its competitive advantage within the framework of the global economy.

References

[1].Information Security Breaches, GCHQ, www.gov.uk/government/publications/information-security-breaches-survey-2014.

[2].https://www.researchgate.net/publication/274071767_UNDERSTANDING_SECURITY_POLICIES_IN_THE_CYBER_WARFARE_DOMAIN_THROUGH_SYSTEM_DYNAMICS

[3].Information Security Breaches, GCHQ, www.gov.uk/government/publications/information-security-breaches-survey-2014.

[4].DeNileon & Guy, (2015), “The Who, What Why and How of Counter-terrorism Issues,” American Water Works Association Journal, May 2015, Volume 93, No. 5, pp. 78–85

[5].Lewis, J, (2012), “Assessing the Risks of Cyber Terrorism, Cyber War and other Cyber Threats: Center forStrategic and International Studies, Washington, DC.

[6].ANSI/ISA–99.(2007), Security for Industrial Automation and Control Systems Part 1.