Security Issues and Best Practices for Water/Wastewater Facilities

Jeff Hayes

Product Manager

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Contents

Introduction 4
Premises 4
Targets 5
Closed Loop Corrective Action for Plant Security 5
Risk Analysis 6
- Risk Management Components 6
- Internal risks 7
- External Risks 7
- Risk Management Mistakes 7
- Data Breach 7
- Root Causes 8
- Network Vulnerabilities 8
- Protocol Vulnerabilities 8

Security Policies 9
Countermeasures 10
- Security Architecture 10
- Vulnerability Assessments 10
- Penetration Testing 11
- Authentication Services 11
- Firewalls 13
- Encryption & VPN 13
- Mobile Devices & Applications 14
- Intrusion Detection 14
- Web Application & Content Control 15
- Operating System Hardening 15
- Physical Security 16
- User Awareness & Training 16

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Monitor & Measure 17
Facility & System Monitoring 17
Business Continuity Planning 17
Disaster Recovery Planning 18
Security Incident Response 18
Conclusions 19
Resources / Sources 20
Beijer Electronics 21

Author Bio

Jeff Hayes is Product Manager for Beijer Electronics. Based in its Americas HQ in Salt Lake city, UT, he helps set the strategic and product direction for Beijer's automation products. He has a special focus on automation deployments in environmentally challenging industries such as oil/gas, mining, water/wastewater and packaging. He has over 20 years' experience in various roles in a number of technology companies. He is the current president of the Utah Chapter of the Information Systems Security Association. He has held his Certified Information Security Systems Professional (CISSP) credentials from $(ISC)^2$ since 2002. He has presented at various national and state events including International Society of Automation (ISA), DistribuTECH, Water Environment Federation (WEF), American Water Works Association (AWWA), and Rural Water Association. In 2012 and 2013, he gave over twenty presentations at events on best security practices for water/wastewater facilities. He is a member of International Society of Automation, the Water Environment Federation, and the American Water Works Association.

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Introduction

The security posture of many industrial environments is less than stellar. The rule seems to be surface-level security and security-by-obscurity, not defense-in-depth and system security leadership. The main reason is that these facilities were not designed to be secure against modern attack methodologies. Many of the controls and automation components are not secure-by-default, they lack reasonable security features, or the features are disabled or not fully utilized. Frequently, plant personnel are not properly educated on the "who, what, why, when and how" of facility and system security. Casual attention to security does not work for critical infrastructure. The potential for harm is too significant.

Security incidents in industrial and infrastructure environments are on the rise. Vulnerabilities with PLCs, instrumentation, SCADA packages, and HMIs are being identified and exploited. Processes and practices for addressing both known and zero-day vulnerabilities, though well-established in the enterprise, are not as well-developed in industrial environments. Security breaches are beginning to take their financial and societal tolls. Reasonable actions are required.

This paper explores the motivation behind and the best practices for an appropriate security posture for water / wastewater environments. It will look at common risks, vulnerabilities and incident management. It will explore the relationship between physical security and information security. It proposes some ideas for prudent security policies given the vulnerabilities and risk and suggestions for implementing the appropriate technologies and practices to support the policies, standards and guidelines.

Premises

Information and physical security for water/wastewater infrastructure facilities are minimized, un-funded, and not part of “best practices” thinking. Security is not a core competency for most of the engineering, system integration, and construction companies that design, expand and modernize these facilities. Many of the facilities are decades old, built prior to the Internet era. Few IT personnel and plant operators have the security knowledge required to design and deploy prudent security architecture. This knowledge and know-how are not part of most workers’ educational background and training.

Serious security incidents in water/wastewater facilities have not created ample awareness or panic that spurs actions like risk analysis, gap analysis, and funding requests.

Most water/wastewater facilities have networks directly connected to the administrative side of the facility. The operational and process control side of the plant shares network resources and connectivity with the customer, financial, public relations, and business side of the plant. This raises concerns over how networks are isolated, segmented and secured.

The main role of a water facility is to provide reliable and safe water to its customers. A wastewater treatment plant is there to accept and process wastewater and discard the effluent safely back into the environment. Safety and service availability are jobs #1 and $2. There are individuals and groups in the world that target these tasks. Securing these facilities secures a town, even a nation.

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Targets

Is a water/wastewater facility a target for politically-motivated groups or free-lance hackers, criminal hackers or state-sponsored cyberterrorists? What about the curious tech-savvy-kid down the block?

Just because there is no record of a water/wastewater facility being exploited by unauthorized users does not mean it has not or will not occur. Water and wastewater facilities are part of society's infrastructure. The control, reliability and integrity of our energy production facilities, distribution grids, water/wastewater facilities, chemical production facilities and distribution systems, and even our food production and distribution system are critical to modern society.

The motivated anti-social individual or group should have no difficulty conducting undetected surveillance – physical or electronic. Most facilities seem to adhere to the "crunchy on the outside, chewy on the inside" paradigm. Once entrance is gained by whatever high-tech or low-tech means, further penetration and infiltration are unmitigated by non-existing defenses.

Are water / wastewater facilities more secure today than a year ago? Probably, however the attack surface is rapidly expanding and penetration and exploitation tools are more extensive.

After all we can do, if there is a will and a budget, all systems and facilities are vulnerable. So why bother? Do you lock your door at night? If someone "really" wants to break into your house to inflict damage, you will not stop them despite your best defensive efforts. But does this mean you do nothing? We do what is reasonable for our environment given the risk and damage potential.

Security, defense technologies and processes are our friends. But security always has been and always will be more of a people issue than a technology issue. Why break in if we have a key? Why steal passwords when we can simply ask for them, and obtain them more often than you'd think?

Closed Loop Corrective Action for Plant Security

The model proposed here is a simplified way to think about how the various elements of an organization's security posture fit and flow. Security is never done, rather evolving with time and technological advancements. Whether an organization has a well-established security culture or is in its infancy, an approach this is could include the following, and repeated:

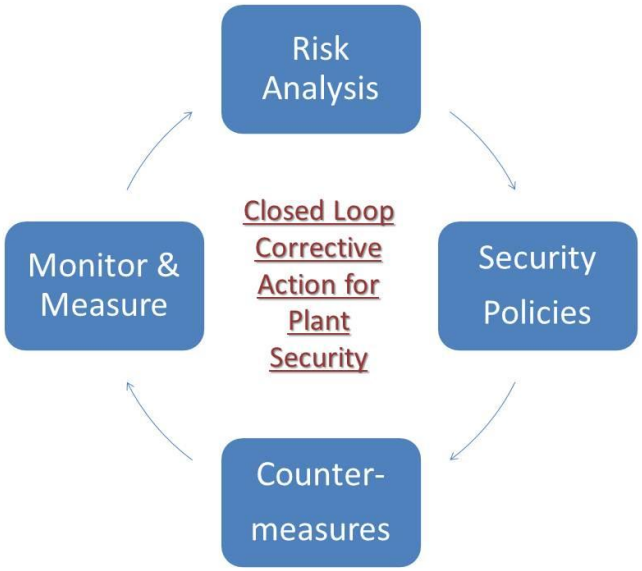
- Do a risk analysis
- Create and match the security policies to mitigate the risk
- Implement the supporting countermeasures
- Monitor and measure what have been implemented

How often? Regularly – a time frame to be determined by each organization. It is not something done once. If an organization is large enough to dedicate employees or contractors to the security roles, great. But smaller organizations may not have this

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

luxury. Some water/wastewater and industrial facilities are managed by less than five employees. In this case, the role must be shared. Security cannot be ignored, even when resources are scare.



Risk Analysis

Every industrial organization or facility will have a unique risk posture as it related to security. Each organization should look at its risk given internal and external factors using both quantitative and qualitative means. Quantitative looks at the probability of an event occurring and the associated loss, using loss expectancy and risk ordering tools. Qualitative looks a potential loss estimates using threats, vulnerabilities and controls methodologies. Whether the risk analysis is done by internal or external resources, there are some key components that should be considered.

Risk Management Components

The key components in most organization's security risk management scheme are:

- Evaluation and Assessment – identify assets and evaluate their properties, characteristics and loss impact
- Risk Assessment – discover threats and vulnerabilities that pose risk to assets
- Risk Mitigation – transferring, eliminating or accepting

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Internal risks

Internal threat can be identified and quantified as follows:

- People (employees, contactors, visitors, ex-associates)
- Processes and procedures
- Computer systems

External Risks

External threats can be identified and quantified as follows:

- Geography, weather events
- States, cities, neighborhood, neighbors
- Terror, war, criminal
- Political, social & economical

Risk Management Mistakes

When doing risk analysis, learn from the experts:

- Don't start from scratch; there are plenty of free and paid-for tools to get you started..
- Don't replicating the audit department; audit is micro in nature and looks where failures occur; risk is macro in nature and looks at the possible and resulting impact.
- Don't conflate precision with accuracy; make reasonable estimates and assessments.
- Don't overemphasize the risk register; one's "low" might be another's "medium."
- Don't use undefined risk concepts; have a set of agreed upon terms.
- Don't ignore having a real risk intelligence program; risk analysis is never done.
- Don't multiply ordinals; high, medium low for one entity may have no correlation to another set of high, medium and low numbers.

Data Breach

Data breaches are daily occurrences. They are not limited to stolen credit card numbers, medical reports, or social security numbers. Data breaches occur in every industry, some accidental, some not. The cost of data breaches continue to rise. Costs are associated with:

- Detection
- Response

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

- Notification
- Ex-post

The actual detection and fix might only be the tip of the iceberg. Costs associated with "damage control" can go on for months if not years.

Root Causes

The causes of data breaches can be groups into the following categories:

- Malicious/Criminal – the least likely but the most costly
- Negligence – user / operator error
- System Glitch – no software is bug free

Network Vulnerabilities

Industrial networks are often shared with the business side of the operation. VLANs, sub-networks, firewalls all help to create a layer defense, but are not impervious.

More and more organizations are allowing remote access, either view-only or actual remote control. When we try to do more with less personnel, we find ways to improve our productivity. Many of these productivity tools implement cursory security measures.

Cloud computing – the outsourcing of computer applications and data storage – is financially attractive. Everything that has historically been done locally can now be contracted to a third party. This implies all data is hosted by someone other than you. This scares even the least paranoid security officer.

Protocol Vulnerabilities

When the TCP/IP suite of protocols was invented, security was not core to the design. The ubiquitous nature of the protocols was not foreseen. The standards bodies – IEEE and IETF – have a done good job creating more secure versions. Some have become normal, many have not. For example, IP v6 will address many security issues but implementations are limited.

Historically, industrial communications were lower speed and serial in nature. But most new automation technology is Ethernet and TCP/IP-based – wired and wireless. Facilities cannot get away with "security by obscurity." You will be found and exploited.

Beijer ELECTRONICS

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Security Policies

Security policies are the basis for security design, architecture, implementation, and practices. They are high-level statements relating to the protection of information across the business and are usually produced by senior management. Standards are specific, low-level mandatory controls that help enforce and support the policies. Guidelines are recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place. If formal policies, standards and guidelines do not exist, then informal ones certainly do.

Security policies are found in written documents, widely distributed, frequently reviewed and regularly updated. Consider some computer, Internet, physical security and emergency management policies:

- Computer, email , anti-virus
- Internet
- Passwords
- Social media, blogging
- Privacy
- Pandemic
- Clean desk, cell phones
- Concealed weapons, bomb threats
- Industrial accidents
- Partners, contractors, consultants, vendors

Most water/wastewater facilities have weak policies. The reason is because historically, it has not been a point of emphasis. If you work at a water/wastewater facility, ask yourself if you have seen the document, read it, seen an update, read that, understood what you read, practice what you read and have seen it actually enforced?

For example, if your operation has a policy of no USB thumb drives, have you or someone you know used one? If Internet access is designated for work-related use only, have you ever used it for personal use?

If a suite of security policies do exist, do they…

- Describe who owns, controls, may access what information and in what manner?
- Delineate sharing vs. least privilege?
- Define separation of duties?

By understanding the security risks and defining the supporting policies, countermeasures can be added to mitigate the risk to an acceptable level for the organization.

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Countermeasures

Understanding the security risks, there is a need to implement policies, processes, guidelines and technologies according to the risk mitigation plan. A good starting point is the definition of a security architecture.

Security Architecture

The goal of a security architecture is to properly aligned people, processes and tools, so all are able to work together to safeguard organizational assets while facilitating goals and strategic direction.

Potential components of a security architecture might include the following:

- Account and identity management
- Access and border control
- Vulnerabilities and base configurations
- Privacy and integrity
- Security monitoring
- Incident response
- Disaster recovery
- User training
- Network, computer and material classification

The architecture should consider the confidentiality, integrity and availability of the information and computing systems. It may also address accountability and quality assurance.

Vulnerability Assessments

A vulnerability assessment is the process and tasks associated with identifying, quantifying, and prioritizing the vulnerabilities in a "system". The following are process and procedures that can be used to identify vulnerabilities.

- Scanning – is used to discover running processes in a system, open ports on servers, user devices and network devices, details of operating systems and security devices, user accounts, executable and DLL files. Examples of these scanning tools include free ones such as Nmap or proprietary ones such as Nessus.
- Security, configuration and compliance audit – specific to a set of guidelines established by industry norm, law, or best practices to understand the security stance of a particular network, subnetwork or computing machines.
- Patch management – is the process or program an organization uses to update its software in order to fix bugs, security issues, user issues and overall product performance.
- Zero-day exploits and responses – the exploitation of previously unaware or new vulnerability which the product or software owners have had zero time to fix or patch the weakness.

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

- Mobile device management – a program, usually implemented by software, that secures, monitors and manages smartphones, tablets, laptops/notebook or other mobile computing devices so the devices and the information contained therein are not accessed by unauthorized users.
- Monitoring and correlating logs and events – the aggregation of system logs and events from multiple systems and computers including security devices to a centralize system to assist with problem tracking and resolution management, historical issues and trending.
- Analysis and communication – the plans and actions associated of the results of scans, patches, exploitations, and device findings with the goal of improving an organization's security posture.

Penetration Testing

A pen test is a live test of the effectiveness of security defenses through mimicking the actions of a real-life attacker. It is used to determining the feasibility of a particular set of attack vectors against an organization's existing defenses. Pen tests are helpful in identifying vulnerabilities that may be difficult or impossible to detect with automated tools. The goal is to assessing the impact of successful attacks, existing defenses, notification and responses. Ideally, it enables a firm to quantify what further investments is security defenses may be required

Pen tests should include:

- Internal tests – where the attacker appears as if he/she is operating as a semi-authenticated user, such as an employee, contractor or individual that has infiltrated physical security.
- External tests – the traditional hacker operating outside the physical barrier, typically via the Internet or wireless means.
- Social engineering – a low-tech security breach usually associated with one or more individuals manipulating other(s) into providing private information. It can be as simple as pretending to be someone and just asking for information such as a user ID, password, employees list, etc. It often includes tricking others to believe in trusting a person that should not be trusted, such as the repair man, or getting people to do things they should not such as inserting a source/content-unknown UBS thumb drive into a computer.
- "Ethical hacking" – where a security expert attempts to exploit a computer or network on behalf of their owner(s). Usually a firm pays someone to pretend to be a criminal, often accompanied by a "get-out-of-jail" card if caught, in order to see what damage a motivated attacker can do.

Authentication Services

Authentication services is a broad heading dealing with approved access to information and information systems. It includes identification (who "you" are), authentication (proving you are who you say you are) and authorization (now that I know who you are, you have the right to do the following). There are many sub-groups belonging to authentication services.

Beijer ELECTRONICS

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

- **Identity and access management** (IAM) or identity management access (IAM) is an electronic framework for managing user and machine identification, authentication and authorization systems, log-on processes and procedures, and system logs and historical records.
- **Single- vs. multi-factor authentication** can be defined by something we know (used ID and password), something we have (card or token), and something we are (biometric). Single factor authentication uses one of these items. Multi-factor authentication uses two or three. Multi-factor authentication is more secure, though often more complex and costly.
- **Identity consolidation and single sign-on** are ways to streamline the user identification and authentication process. Users would prefer to log-on once to their computer, network and applications as opposed to being required to go through this process repeatedly, especially when it is within one organizational domain. SSO helps aggregate this process with a focus on user productivity.
- **Passwords** are secret character strings used for authentication. Password crackers are software tools used to uncover the secret strings. Organizations should have policies that make it more difficult for passwords to be guessed and used by unauthorized users, including:
    - The use of alpha, numeric and special characters, of at least a specific length, in non-dictionary or proper noun formats, changed or a regular basis and not useable again for some period of time.
    - Passwords are never to be stored in clear text.
    - When a new password is assigned or when a replacement password is given, the user or system should be forced to change it immediately, thus helping to ensure the assigner does not know the password.
    - One-time passwords are only used once. They typically consist of two parts: something you know, like a PIN, and something that it only valid for a short period of time, like 60 seconds. OTP systems are usually comprised of a central server and some device end users possess that generates the unique, second part of a short-lived, log-in string. These are very good for remote user access.
    - Switches and routers have user IDs and passwords for administration. These default settings are public and should be changed by the device owners.
    - Virtual Local Area Networks (VLANs) and Access Control Lists (ACLs) on switches and routers often support authentication services that assist with network access. For example, most switches support IEEE 802.1x, a port-based user authentication standard that when used, forces users to identify themselves at a certain network ingress point. Some manufactures provide a similar dialogue with source/destination IP addresses and TCP and UDP ports.
    - Wireless access is almost always accompanied by some user authentication dialogue. A wireless access point (AP) can be hidden (not broadcast) and accessible only if the SSID is known. Access points should use modern encryption technologies like WPA2 (not WEP) and trustworthy authentication services. Keys should be long and not easily guessed. Careful consider should be taken to place access points and the connected users into the appropriate, authorized VLAN or network.
    - Remote access is to grant specific authorized users access to organizational resources over a telephone network, private communications lines (T1) or public network (Internet). Policies should ensure the device

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

and/or user are authorized and that the communications are insured of integrity and privacy (often through secure VPN protocols).

Firewalls

A network firewall is system or combination of systems that enforces a boundary between networks. This usually occurs between a private network and a public network; e.g., Internet. These firewalls are often designed to differentiate between trusted (private), un-trusted (public) and semi-trusted (DMZ from demilitarized zone) networks. In industrial environments, a firewall can be used to separate the business or enterprise side of the organization from the process control side. There is little need for the billing applications and users to be on the same network as the one hosting the SCADA and PLCs.

Firewall implementations range from basic to very sophisticated. A basic firewall can be in a router, access point, multi-layer switch, or any device that support OSI Layer 3 (IP) and Layer 4 (TCP & UDP) protocols. **Access control lists** or access rules can be established to allow or deny data paths and connections to/from specific source/destination IP addresses as well as source/destination TCP/UDP ports, like FTP, DNS, HTTP and SNMP.

A **stateful firewall** keeps track of the "state" of network data connections, allowing packets that match what is expected for that type of connection. **Application firewalls** inspect higher level protocols, namely the application, to ensure proper compliance for what would be expected. A **deep-packet inspection firewall** goes further by looking for protocol non-compliance, mal-ware, or anything beyond what is expected for the data flow over specific ports. It attempts to uncover abnormal data within what might be considered normal data, rejecting the offending packets and cutting off the data flow.

Firewall deployments can be positioned on multiple devices and in multiple locations throughout a network:

- **Network-based** – firewalls supported on security appliances, Linux or Windows-based software implementation, routers, switches, access points, etc.
- **Host & server systems** – firewalls supported on end user laptops/notebooks, desktops and on application servers.

Encryption & VPN

Encryption is the process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (cipher text). The purpose of encryption is to insure the integrity and privacy of data while at rest (stored on a hard drive) and/or while in motion (moving from one machine to another). Integrity implies the data cannot be manipulated or changed without authorization and without notification. Privacy implies the data can only be read by the authorized parties that sent and received the data.

Network encryption is widely used over a secure **Virtual Private Network** (VPN). This enables private communications over a public network. It helps avoid a man-in-the-middle attack. It is the basis of secure remote access where i) a user device like a laptop or tablet can communicate securely to central resources like databases, file stores and applications, and ii) one machine can communicate security to another to insure the integrity and privacy of the data exchange.

Beijer ELECTRONICS

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Common protocols used to implement VPNs are IPSec, HTTPS, SSL and SecureShell.

Mobile Devices & Applications

Smartphone, tablets and ultra-mobile computing device deployment continue to grow while notebook/PC deployment continues to demise. In industrial environments, these mobile devices will be used for remote access and application control. Whether these devices are issued by the organization or part of the growing "bring your own device" (BYOD) trend, securing these devices is paramount.

Mobile device policy needs to address authentication and authorization as well as integrity and privacy via a VPN. Globally, the number of lost and stolen phones is astounding – in the hundreds of thousands annually. These devices contain organization email, confidential document or access, and industrial monitoring/management applications. I the wrong hands, great damage can result if not properly anticipated.

Those that write malware do so for the operating systems and applications that benefits them the most. As mobile devices become more prolific and core to industrial network access and control, exploitation of these devices will increase. Presently, the security of mobile devices and applications is weak at best. However there are many mobile device security applications that a firm can use to address most of the security concerns.

Intrusion Detection

Intrusion detection is the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. An intrusion detection system (ISD) can be considered a "burglar" alarm for computer networks. When properly tuned, network activity outside of the "norm" can trigger alarms. For example, is it normal for one of the non-technical administrators to be doing a large file transfer from a remote location Sunday morning at 2am?

There are two classes of IDS: network-based (NIDS) and host-based (HIDS). NIDS systems are nodes or hardware/software sensors placed at key locations on a network. HIDS are typically software packages running on end systems like Windows or Linux servers or end user PCs/laptops.

An **intrusion prevention system** (IPS) take IDS one step further: they attempt to stop or block the violation in addition to alerting and recording it. These are classified as network-based intrusion prevention system (NIPS), host-based intrusion prevention system (HIPS), as well as wireless version (WIPS) and network behavior analysis (NBA).

A **physical IDS** can be considered an extension of the computer-based IDS. Doors, gates, lights, cameras are part of a complete IDS. With proper surveillance, intruders will take the easiest path to get to their desired goal. If the path of least resistance is cutting a hole through the fence and walking in and stealing something, modifying settings, or installing a Trojan horse (perhaps using stolen credentials), why not follow this course?

Beijer ELECTRONICS

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

A **honeypot** is a trap or decoy. It is an isolated computer system setup to appear real but it is actually a facade. Its purpose is to deflect attacks from the main network while gather information regarding an attack methodology. Production honeypots are limited in scope and interactivity. Research-based honeypots are more extensive and interactive, mainly for academic interests. Industrial honeypots are in their infancy with their worth questionable.

Web Application & Content Control

Web site, web applications and web services are ubiquitous. Many software developers focus more on the benefit and value of the user's experience with the application, often to the detriment of security. Ease of use and interactivity tend to trump security which often stifle the perceived user experience.

Web applications like PHP, ASP, C#, Java, .NET are popular programming tools/languages. Good program design can help mitigate the potential security threats web applications and services can introduce. Good programmers will consider the following in their design:

- Authentication & authorization (cross-site scripting)
- Data validation & handling (SQL injection)
- User and session management
- Points, time and state issues
- Error handling
- Encryption
- Content Filtering
- Limitations and enforcement points
- Legal issues
- Productivity issues
- Bandwidth/network issues

Industrial system administrators would be wise to validate how web application services behave and respond to known attacks.

Operating System Hardening

The process of hardening an operating system is to configure a computer or other network device to resist attack. Most operating systems are designed to be open or insecure by default. The software supplier leaves it up to the administrator to determine which services and features to remove, hide, limit or activate. The hardening process will vary from OS to OS – what is hardened on a Windows Server may be similar to what one hardens on a Linux machine but how it is done can vary significantly. Some common hardening steps can include the following:

- Perform initial system install

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

- Remove unnecessary software
- Disable or remove unnecessary usernames, passwords and accounts
- Disable or remove unnecessary services
- Apply patches
- Run a scan

Physical Security

Historically, industrial environments have focused a great deal of their security countermeasures on physical security. The engineering and construction firms involved in the designed and building of the facilities know civil engineering, not IT security. Fences, door and latch alarms, outdoor vegetation control, physical relationship to the surrounding neighborhood and terrain, indoor and outdoor lighting, and cameras/CCTV are common deterrents. These are often supplemented by key control and access cards and their management, as well as intrusion detection systems including motion sensors, glass break detectors and alarm integration with local law enforcement.

Physical security is part of a holistic security posture for an industrial environment. It is based on the concept of a layered defense design where a breach in one system or layer will not compromise the security of the entire facility. The breadth of physical security includes

- Asset protection
- Video surveillance and monitoring
- Employee protection and workplace violence prevention
- Fraud prevention
- Loss prevention
- Investigations & forensics

User Awareness & Training

Given all of the modern security technology, people are still the biggest security weakness or vulnerability. Many of the biggest security breaches are a result of human error or knowingly violating security policies. Employees, contactors, visitors, and other stakeholders all play a role in the security of an organization. These individuals need to know and understand their role in organizational and informational security. Their behavior and actions must support the security policy, provided a) there is a formal security policy, b) that it is available, read and updated on a regular basis, and c) is enforced.

Each organization should decide for itself the scope of a formal security awareness training program. Elements of an effective user awareness and training program could include:

- Constantly reinforce messaging to change behavior

Beijer ELECTRONICS

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

- Shared successes
- Management support
- Partnering with other departments
- Creativity and multiple mode delivery
- Metrics
- Scope and timing
- Role-playing or exercises

Monitor & Measure

Have the deployed countermeasures done an effective job of mitigating the risks and supporting the security policies of the organization? Monitoring and measuring what has been implemented and how well it is working will help answer this. Consider facility and system monitoring, business continuity/disaster recovery, and incident response planning as three areas to address.

Facility & System Monitoring

A vulnerability assessment – scan, pentest, etc. – results in actions. The actions are tasks to fix the discovered problems. These tasks can be to update and patch software, change default settings, improve password management, harden some of the operating systems, do a better job of controlling mobile devices, and tighten up the firewall rules. It takes time to secure

- Security devices and software
- End systems and servers
- Network equipment

However, by executing a plan, progress will be made. The security posture will be improved. Is it where it needs to be or is there more to do? Success is achieved step-by-step over time, not overnight.

Business Continuity Planning

A business continuity plan (BCP) helps an organization understand its susceptibility to internal and external threats, how it should respond when threats surface, and how it can recover in a timely and effective manner. A BCP, as suggested by USA's FEMA, can include the following:

- Business Impact Analysis identifies time-sensitive or critical business functions and processes and the resources that support them.
- Identify, document, and implement to recover critical business functions and processes.

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

- Organize a business continuity ad-hoc team and compile a business continuity plan to manage a business disruption.
- Conduct training for the business continuity team and testing and exercises to evaluate recovery strategies and the plan.

Disaster Recovery Planning

A disaster recovery plan (DRP) is a subset of a business continuity plan. It is a plan to help recover from intentional or accidental events, be they man-made, environmental or natural.

With top management support, the written plan from the ad-hoc DRP team leverages an organization's risk analysis, prioritizes assets and functions, delineates recovery options, outlines stakeholder communications, and describes the scope and frequency of practicing the plan.

Security Incident Response

A security incident response program can also be considered a subset of BCP. The focus is more on computer and IT issues. It is the complete response set of an organization to an abnormal event, such as an unauthorized user; e.g., hacker, gaining access to internal computer systems or a breached fence or gate. An incident typically references a human cause where there is intent to do harm.

Security information and event management (SIEM) is a homegrown or commercial solution set that attempts to aggregate and correlate real-time data and analysis of security alerts generated by security-oriented devices like firewalls, VPN equipment, intrusion detection systems, switches, routers, and security-savvy-applications. SIEM solutions can be thought of as the heart of a security monitoring program, centralized in a control center. In industrial environments, it might be a supplement to a SCADA system. SIEM solutions can be part of an incident response system, as it will display the logs, alerts and historical trends, often in the form of a dashboard.

A security incident response program and SIEM solution will provide the following benefits to the industrial organization:

- Secure critical evidence to support investigation/litigation
- Defend against internal and external exposure
- Determine the source, scope, and sensitivity of a data loss
- Identify your legal and regulatory obligations
- Retain customers and opportunities
- Apply processes for future prevention

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Conclusions

Water/wastewater facilities, along with the electrical grid, energy sources and processing facilities, chemical plants, and the communication networks, are part of society's infrastructure. These facilities are all potential targets for anti-social individuals or groups, be it simple hacking exploits to extreme terrorism. Cybersecurity is essential in defending these facilities.

The security goal of industrial facilities should be to create a reasonable security posture given the risk, risk acceptance and security policies. The countermeasures are deployed to mitigate the risk and enforce the policies. The monitoring and measuring activities are designed to access progress and close the gaps between the real versus the desired security posture.

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Resources / Sources

- AWWA Standards (G430)
- Chemical Facilities Anti-Terrorism Standards Risk-Based Performance Standards Guidance
- CSO (CXO Media, Inc.), http://www.csoonline.com/. Including George Hulme, September 26, 2012, CSO
- DoDI 8500.2
- U.S. Department of Homeland Security (DHS) Catalog of Control Systems Security: Recommendations for Standards Developers
- U.S. Department of Homeland Security FEMA, http://www.ready.gov/
- DHS Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies
- Executive Order (EO) 13,636, "Improving Critical Infrastructure Cybersecurity," and Presidential Policy Directive (PPD)-21, "Critical Infrastructure Security and Resilience," February 2013.
- Gartner, http://www.gartner.com.
- ISA99 Industrial Automation and Control Systems Security, ANSI/ISA 99
- ISO/IEC 27000-27007 Information technology - Security techniques - Code of practice for information security management (formerly ISO/IEC 17799:2000)
- ISO/IEC 15408 (Common Criteria)
- National Institute of Standards and Technology (NIST) SP800-82 Guide to Industrial Control Systems (ICS) Security
- NIST SP800-53 Rev. 3 with Appendix I Recommended Security Controls for Federal Information Systems and Organizations
- Nuclear Regulatory Commission, Regulatory Guide 5.71 (NRC RG 5.71), Cyber Security Programs for Nuclear Facilities
- NIST Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems
- ISA/IEC-62443 (Formerly ISA-99) Industrial Automation and Control Systems Security, including TR99.00.02
- NERC 1300 CIP-002-1 through CIP-009-2 (CIP=Critical Infrastructure Protection).
- North American Electric Reliability Corporation (NERC) 1300 Critical Infrastructure Protection (CIP) standards CIP-002 – CIP-009
- Security Risk Analysis Directory, http://www.security-risk-analysis.com/.
- Security Search, http://searchsecurity.techtarget.com/.
- Water ISAC

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00

Beijer Electronics

For over 30 years, Beijer Electronics has designed and manufactured human machine interface (HMI) products for OEM and vehicle systems integrators. Products include automation software, operator panels, panel/industrial PCs, industrial networking, and mobile data terminals. Key industries include mining, oil/gas, water/wastewater, heavy construction, marine and off-shore. Beijer is a fast growing technology company with extensive experience in industrial automation and data communications. The company develops and markets competitive products and solutions that focus on the user. Global headquarters are in Sweden with Americas operations based in Salt Lake City. Beijer sells and supports its products all over the world.

- Beijer Group – http://www.beijergroup.com/
- Beijer Electronics (global) – http://www.beijerelectronics.com/
- Beijer Electronics, Inc. (USA - Americas) - http://www.beijerinc.com/

US Office
Beijer Electronics, Inc.
1865 West 2100 South
Salt Lake City, Utah 84119-1303 USA
BeijerInc.com / 801-466-8770

Headquarters
Beijer Electronics Products AB
P.O. Box 426
201 24 Malmö, Sweden
www.BeijerElectronics.com / +46 40 35 86 00