

IMPLEMENT PREVENTIVE PRINCIPLES, POLICIES, AND PROCEDURES SO THE HACKER HITS A BRICK WALL—NOT YOU

Plan for Network Security

ERIC BYRES, P. ENG., AND GORDON GILLESPIE

OVER THE PAST DECADE, THE TRADITIONAL CORPORATE NETWORK has come under siege from a proliferation of viruses and malicious intruders. As a result, numerous network security technologies, methodologies, and policies have been developed to secure the business system.

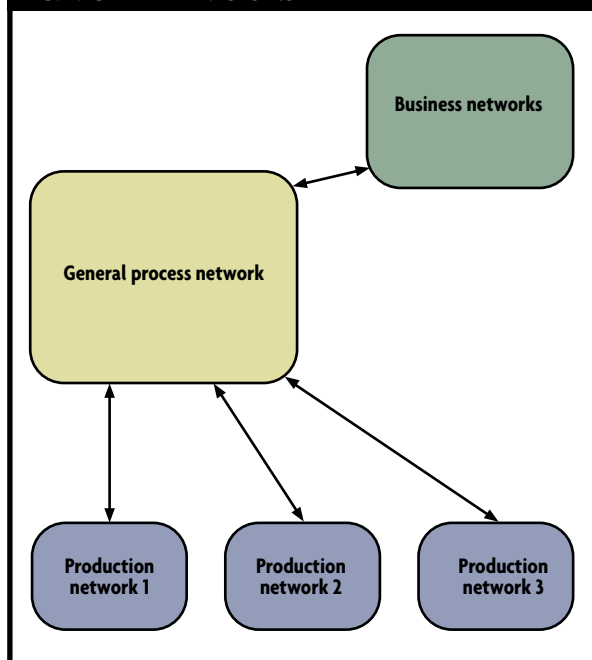
In comparison, process control systems, with their reliance on proprietary networks and hardware, have long been considered immune to cyber attacks. Now, with the move to open standards such as Ethernet, TCP/IP, and web technologies, the plant floor requires its own security procedures to eliminate undesirable access to production systems and to

maximize the uptime and efficiency of process networks.

Unfortunately, while engineers are becoming more aware of this need for cyber security on the plant floor, they can run into a brick wall when it comes to implementation. First of all, they quickly discover there is little information available on how to secure industrial network systems; all the methodologies are for business systems. Then they discover these business security techniques cannot be applied directly to the plant floor. The nature of process control systems, with their reliance on unusual operating systems and their strict operational requirements, means many business security solutions will interfere with the process systems.

So how are plant engineers to protect their plant floor networks?

FIG. 1: CREATE DIVISIONS



Dividing the plant into functional areas is a critical part of the security policy. In this example, users and servers requiring communication with both production and business networks are located on the general process network. Production networks should be high-security zones where maximum uptime is achieved by minimizing access. Notice that there is no communication allowed directly from the business networks to the production networks.

START WITH POLICY, NOT TECHNOLOGY

Here at the British Columbia Institute of Technology's Internet Engineering Lab, we have researched a large number of systems large and small, and noticed one common feature in all of the successful implementations: Successful security designs start with the development of a plant security policy, leaving technology details for later.

A security policy is simply a statement of the goals, responsibilities, and accepted behaviors required to maintain a secure production environment. It defines the direction, gives broad guidance, and demonstrates senior management support for security-related facilities and actions across the organization.

A security policy should be technology-independent and does not include the implementing procedures and processes. In other words, the security policy outlines what you want to achieve, not how to do it.

The primary objectives of a typical industrial cyber security policy are to:

- Establish a secure production communication infrastructure and a stable processing environment.
- Effectively manage the risk of security exposure and intrusion.
- Communicate the responsibilities of users, management, and information system staff for the protection of information and provide direction toward honoring this commitment.

Think You Have It All Locked Up? Think Again

While the obvious external access to company networks is through the Internet, and thus is usually managed by the IT department, most production departments have a number of low security (and forgotten) access points to the process network that are overlooked. Here are a few procedural tips that can reduce your risks.

- **Deny Everything You Can**—The basis for secure access is that communication that is not expressly permitted is prohibited. Use a firewall between the business network and the process networks. This firewall device should be the only access point between the production network and the rest of the plant's networks and/or the Internet. Any form of cross-connection that bypasses the firewall should be strictly prohibited. When configuring the firewall, one possibility is to block services and protocols from between business and process to start and then grant access on a case-by-case basis. Have a professional set up the firewall and teach you how to allow/disallow traffic.
- **Phone Lines**—Modems and phone lines present a significant threat of unauthorized access to most production networks. Don't allow modems on users' computers; provide a modem server that is protected and managed. Remote users typically save the phone number, username, and password for the connection in either paper documentation or as part of a saved remote access server (RAS) session. This information is easily copied for misuse. Remember, when you grant inbound phone access to a user, you may also be inadvertently granting unauthorized access to that user's children.
Use leased line (point-to-point) communication for SCADA systems where possible to ensure that you know who is at the other end. Where dial-up lines are required, use callback functionality to ensure that the other end of the connection is where you expect it to be. Always use full username/password access for modem connections either through Windows RAS functionality or by purchasing a modem with built-in authentication.
- **Inbound Access From the Internet**—Although the IT department assures you that the inbound access is secure, does that mean that all external users of the business network should be allowed on the process networks? Require a range of virtual private network or RAS addresses for inbound access process users that is separate from those allowed on the business network.
- **Outbound Access to the Internet**—Do not allow Internet access from the production network. Internet access should only be allowed from the general process network.
- **E-mail**—Do not allow e-mail on the production network. E-mail is such a major source of viruses it is considered a very high-risk activity. E-mail should only be allowed on the general process network. An exception to this is outbound-only notification of alarms.
- **Examine the Log Files**—You won't know if someone is trying to break in unless you look. Save and analyze the logs of servers and firewalls to determine normal usage and help to identify unauthorized events. Use an automated intrusion detection system to examine the firewall logs for intrusion signatures.

- Provide a requirements outline for those staff charged with technical implementation.
- Promote understanding and compliance with all applicable laws and regulations.
- Limit company liability and preserve management's options in the event of a security incident.

Ideally, the primary responsibility for a security policy should reside at the highest organizational level possible with an individual or group that can accept risk on behalf of the organization. At this high level the responsibilities surrounding the security policy include development, approval, and compliance management. Below this should be a production-based technical team charged with standards implementation, technical management, and enforcement. The consistent application of the security policy will reduce the risk and liability of all persons involved.

It is easy to get bogged down in the policy details as it is developed, which is missing the whole point. The idea is to not mix technology-specific procedures into your policy, but make that part of lower-level security standards, processes, and guidelines. The following are definitions and examples for security policy, procedures, and standards development that contrast the differences.

- A **Security Principle** is a statement of value, operation, or belief that defines the organization's approach to security; it's the organizational philosophy that forms the foundation for the security policy. An example of this might be: "The XYZ Company believes it is critical for reliable plant floor operations that all data coming to and from the plant floor be managed in a consistent and clearly documented manner, regardless of source, destination or purpose."
- A **Security Policy** is a statement of intent and guidance by senior management to the organization regarding the commitment, ownership, and requirements applicable to security. The security policy defines the expected behaviors, responsibilities, and rules that are required. A security policy might be: "The plant floor security manager shall approve, manage, monitor, and maintain all data transfer points to and from the production environment. No plant floor to business/external data transfer points shall be implemented without the manager's approval."
- A **Security Standard** is a requirement for compliance as a means of executing an element resulting from a security policy. The security standard defines what methods and mechanisms will be used to enforce the policy. For example, "All communication links to and from equipment in the process areas, including PLCs, HMIs, analyzers, data servers, and personal computers, shall be through an officially approved connection interface. Use of desktop modems, wireless links, etc., that are not approved will result in disciplinary action." In many companies a security policy and a security standard are combined and referred to as the security policy.
- A **Security Procedure** defines what steps are required to

apply a security standard. The start of a typical procedure might include: "Maintenance staff wishing to have a connection to the plant floor equipment via modem shall use the plant floor remote access server (RAS) system. To have a connection set up, please contact the plant floor security manager using electronic form

S-897. If you have any questions while completing the technical details of this form, contact any member of the process LAN team because, by ensuring all the correct information is available, you will speed the deployment of your connection."

- A **Security Process** is a collection of activities that have definable inputs,

specific measurable objectives, and a resultant value to the organization's security goals. The security process defines the activities that are required to support the security standards. For example, "The plant floor security manager will ensure that plant floor to business/external data transfer points shall be registered in document S-543 and will include the following information..."

- A **Security Guideline** is a statement of advice suggesting good business practices to retain a secure environment. A security guideline describes optional and additional security measures and procedures that can be followed to enhance security. For example, "The plant floor security team recommends strongly against using as passwords any word contained in English or foreign language dictionaries, spelling lists, or other lists of words."

TOPICS YOUR POLICY SHOULD COVER

Like any policy document, security policy can cover a wide number of issues. Which issues merit the highest attention can differ greatly from industry to industry and company to company. But at the top of any list should be responsibility: Who is responsible for maintaining security, monitoring the system for problems, and reacting when something happens?

It is also important to determine the chain of command: Who makes decisions during implementation disputes or during a crisis? And don't forget enforcement: Who is responsible for watching that the policies are being followed, and how do they enforce (or change) them if they aren't?

The security policy should mandate the division of the facility data systems based on different operational roles. For example, as shown in Figure 1, a factory's systems could be divided into three levels of importance from an integrity and access viewpoint to ensure that network problems, viruses, and/or intruders are not passed through to the critical process control equipment.

The policy would also define the general information flow between levels or security zones. For example, the policy might state that no communication is allowed directly from the business network to the production networks. Later, in the standards and procedures development, routers might be specified to divide the network into smaller broadcast domains (subnets), and firewalls could provide access management based on the critical level of the attached devices.

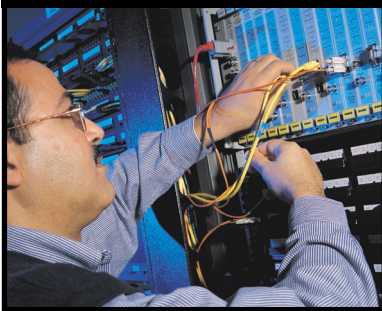
One of the challenges in the industrial control sector is authentication of operations and personnel. The need to maintain uninterrupted visibility and

working closely with the vendor of your process control systems.

Once authentication of a user is accepted, it is not enough to know who the user is. You also must be able to supervise what information or applications the user can view and modify. This is known as Authorization Policy. It is important that access to

resources is restricted only to those who are entitled to use them. Security managers typically define sets of users for access to particular applications. Therefore, when a user attempts to use a resource, an administrator can check the Authorization Policy to determine if that user merits access to the information.

FIG. 2: PRE-EMPTIVE STRIKE



The BCIT lab uses a SmartBits load generator to create hundreds of thousands of messages to send to an Ethernet-based instrument or controller to test its ability to handle denial-of-service or malformed packet attacks. Although the machine is too pricey for most plants, network professionals can bring instruments into the lab or BCIT can bring the machine to clients.

control as opposed to the standard IT practice of logging in makes authentication an ongoing issue. It often is assumed that strong authentication is not compatible with PLC and DCS equipment and therefore should not be implemented. As a result, in many industrial plants the operator stations have black passwords or trivial ones such as "password."

It is important that any thorough plant floor security policy consider the options carefully and investigate methods for implementing stronger authentication policies. Often this will mean

EXTERNAL ACCESS—WHO'S ALLOWED IN?

Whether you realize it or not, there are access points to your plant network. When asked, most plant managers will immediately tell you that no one from outside their plant can communicate with the equipment on their plant floor. Unfortunately they have forgotten about modem lines for remote sup-

port from vendors or staff, wireless SCADA links, interfaces to partner companies, and a myriad of other backdoors. Defining the management of these secondary access points is part of the security policy.

No matter how well you design a security system, there will always be exceptions. For example, you may

have developed a policy that forbids all direct external connections to process equipment...then new environmental legislation comes along that requires a government link to some flux gas analyzers.

Since the number one goal for most facilities is reliable production, not ease of security, banning all non-standard connections outright is usually not a solution. What is needed is a system of recording exceptions to the model and ensuring that they are being secured by means other than the standard procedures.

Many times we have worked with companies that know they are being hacked but don't know how to deal with it. Rather than waiting until they were in crisis, these firms should have established a policy for incident response. Typically this includes a pre-defined security response team and a process to deal with security incidents. The team should monitor events and be prepared to act quickly in the event of a serious incident.

The above topics for a network security policy are certainly not the only ones to consider. However, if you start with these you will quickly discover the other issues that your plant floor security policy needs to address.

Remember not to get caught up in the technological details as you begin developing your policy. We all are well aware of just how fast technology changes, and that can make your security project never ending. You want to get at least some security in place before the hackers come calling on your plant floor.

Eric Byres, P.Eng., manager, British Columbia Institute of Technology's Internet Engineering Lab, holds the Advanced Systems Institute research fellowship for industrial network security. He can be reached at ebyres@bcit.ca.

Gordon Gillespie is senior network designer at Artemis Industrial Networking, a firm specializing in the design of plant floor network and fieldbus systems. He may be reached at ggillesp@artemisnetworks.com.