Bellingham Control System Cyber Security Case Study

Marshall Abrams

Joe Weiss

15 August 2007

MITRE

Case Study Synopsis

- Examine actual control system cyber event
  - Resulted in significant environmental and economic damage as well as deaths
  - Operating policies and procedures had readily identifiable cyber security vulnerabilities
  - Timelines, control system response, and control system policies
- Operating policies and procedures had readily identifiable cyber security vulnerabilities
- Identify NIST SP 800-53 management, operational, and technical safeguards or countermeasures that, if implemented, could have prevented or ameliorated the event

Incident Overview

- June 10, 1999 a gasoline pipeline ruptured
  - Gasoline leaked into two creeks in the City of Bellingham, Washington and ignited
  - Fireball killed three persons, injured eight other persons
  - Caused significant property damage
  - Released approximately ¼ million gallons of gasoline causing substantial environmental damage

Pipeline System

- Remotely operated from a central control center where pipeline controllers can
  - Monitor key variables
  - Monitor and operate mechanical components, such as pumps and motor-operated valves
- Pipe rupture scenario
  - External damage to the pipeline in the vicinity of the eventual rupture caused by a contractor installing water lines across the pipeline in the vicinity of the rupture.
  - During construction pressure relief valves were installed that were found to be improperly configured or adjusted, and the actions taken by the company to test and correct the valve settings were ineffective.
  - On the day of the accident, the SCADA system that controllers used to operate the pipeline became unresponsive.

Timeline

- 3:00PM – Controller changes gasoline delivery points; System administrator enters two new records into SCADA2 Historical database
- 3:10PM – SCADA2 began to generate error messages related to historical database. System administrator checked records and left for 15 minutes
- 3:18PM – SCADA2 becomes erratic and non-responsive
- 3:24PM – SCADA2 taken off-line
- 3:27PM – Backup SCADA1 brought on-line
- 3:28PM – Pipeline ruptures
- 3:44PM – SCADA2 back on-line
- 3:48PM – SCADA2 operational after new records deleted
- 4:04PM – SCADA1 back on standby
- 4:29PM – Leak detection alert

At time of incident: SCADA2 = primary controller, SCADA1 = alternate controller

Personnel Actions

- The system administrator may have been programming some new reports on a terminal in the control center computer room
  - Open to question because key personnel have refused to respond to questions, exercising their Fifth Amendment rights
  - Records entered just before the slowdown were deleted supposedly to stop the abnormal operation
  - Computer logs corresponding to the time the SCADA was unresponsive were “missing”

National Transportation Safety Board (NTSB) Cyber-Related Findings and Recommendations

- The unresponsiveness of the SCADA system was the proximate cause of the rupture
- Degraded SCADA performance thought to have resulted from the development work done on the live SCADA system
  - Should have been performed and thoroughly tested on an off-line system
  - Errors resulting from revisions may have been identified and repaired before they could affect operation
- Olympic did not adequately manage the development, implementation, and protection of its SCADA system
  - Inadequate Security Policies
  - Access Control and Privileges
  - Network Separation
  - Audit
  - Configuration Management
  - Inadequate Training
  - Inadequate Forensics
  - Virus Protection

Cyber Security Perspective

- Examine NIST SP 800-53 controls
  - Controls violated or not met
  - Potential mitigation that would have occurred if these controls were followed
- Not all bad things that happened are cyber security issues
  - SCADA operator and other key personnel refused to testify
  - Pressure trend displays presenting potentially misleading data
    - If data not available from SCADA system (such as during non-responsive operation), graph would draw straight line implying conditions not changing.
    - No highlighting feature to alert operators that graph contains gaps in the displayed data.

SP 800-53 Security Control Classes, Families, and Identifiers

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

Cyber Security Issue: Security Policy and Procedures

- No cyber security program (including control system policies and procedures)

- SP 800-53 policy and procedure controls
  - The first control in every control family is policy and procedure – The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, <*family*> policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the <*family*> policy and associated <*family*> controls.
  - CA-2 Security Assessments – The organization conducts an assessment of the security controls in the information system [*Assignment: organization-defined frequency, at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Cyber Security Issue: Incident Notification and Response

- **Prompt notification that the SCADA system appeared to be malfunctioning may have initiated appropriate corrective action**

- **SP 800-53 Incident Response controls**
  - **IR-2 Incident Response Training – The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].**
  - **IR-4 Incident Handling – The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.**
  - **IR-6 Incident Reporting – The organization promptly reports incident information to appropriate authorities.**
  - **IR-7 Incident Response Assistance – The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.**

Cyber Security Issue: Unsecured Remote Access

- Terminals and workstations were connected through network connections or via modems
- Direct dial-in access to SCADA computers available from the outside

---

- SP 800-53 Access Controls
  - AC-2 Account Management – The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency, at least annually*].
  - AC-3 Access Enforcement – The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.
  - AC-17 Remote Access – The organization authorizes, monitors, and controls all methods of remote access to the information system.

Cyber Security Issue: Uncontrolled Privileges

- All authorized Olympic computer operators used the same login with system administrator privileges
  - Severely limited ability to audit system or assign individual accountability for actions performed on the VAX or SCADA system
  - All authorized users could manipulate or delete any and all files

---

- SP 800-53 Controls limiting privilege
  - AC-5 Separation of Duties – The information system enforces separation of duties through assigned access authorizations.
  - AC-6 Least Privilege – The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.
  - AU-9 Protection Of Audit Information – The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Cyber Security Issue: No Network Separation

- Single control room Ethernet connecting:
  - SCADA host computers, control room computers, leak detection computer
  - Bridge connected control room Ethernet with company administrative computer network
- Administrative computer network reported to have some Internet connectivity
- Several other departments allegedly used data obtained from the SCADA system

---

- SP 800-53 SC-7 Boundary Protection
  - The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Cyber Security Issue: Audit

- No record of the commands entered via one of the remote terminals or workstations
- VAX-VMS system logging capability
  - Designed to log all system operations, errors, and hardware failures.
  - Security log kept a record of who was logged into the system
  - Security log contained no evidence of an unauthorized attempt to access the system.

- SP 800-53 controls
  - AU-2 Auditable Events – The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].

Cyber Security Issue: Configuration Management

- Database revisions performed on primary online SCADA system instead of an offline system

- SP 800-53 Configuration Management controls
  - CM-3 Configuration Change Control – The organization authorizes, documents, and controls changes to the information system.
  - CM-4 Monitoring Configuration Changes – The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.
  - CM-5 Access Restrictions For Change – The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.

Cyber Security Issue: Training

- **No mention of any computer security training provided or taken by any of the staff**

- **SP 800-53 training controls**
  - **AT-2 Security Awareness – The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency, at least annually*] thereafter.**
  - **AT-3 Security Training – The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.**
  - **AT-4 Security Training Records – The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.**

Cyber Security Issue: Forensics

- Parent corporate software support group reviewed pipeline control software after the pipe rupture event
  - Attempted to replicate the SCADA computer performance anomaly
  - Image copy of the SCADA system disk installed on support group development computer
  - Development system and software different from SCADA system
  - No performance anomalies could be created
- Key logs were inexplicably missing including during the period when the SCADA was unresponsive

---

- SP 800-53 controls
  - IR-4 Incident Handling – The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Cyber Security Issue: Code and data protection

- No virus protection

- SP 800-53 controls
  - SI-3 Malicious Code Protection – The information system implements malicious code protection.
  - SI-7 Software And Information Integrity – The information system detects and protects against unauthorized changes to software and information.

Additional Information

- **Authors**
  - **Marshall Abrams <abrams@mitre.org>**
  - **Joe Weiss <joe.weiss@realtimeacs.com>**
- **Incident**
  - ***Pipeline Accident Report, Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10, 1999*, NTSB/PAR-02/02, PB2002-916502. http://www.ntsb.gov/publictn/2002/PAR0202.pdf**
- **Case Study**
  - **http://csrc.nist.gov/sec-cert/ics/papers.html**
- **NIST Industrial Control System Security Project**
  - **http://csrc.nist.gov/sec-cert/ics/index.html**
- **NIST Project Managers**
  - **Stu Katzke <skatzke@nist.gov>**
  - **Keith Stouffer <keith.stouffer@nist.gov>**