Malicious Control System Cyber Security Attack Case Study– Maroochy Water Services, Australia[1]

Marshall Abrams, The MITRE Corporation, abrams@mitre.org
Joe Weiss, Applied Control Solutions, joe.weiss@realtimeacs.com

Abstract

The 2000 Maroochy Shire cyber event is the second in a series of control system cyber events analyzed to determine the effectiveness of NIST Special Publication (SP) 800-53 controls on industrial control systems. The event has been documented in Court proceedings, a Maroochy Water Services presentation, and other documentation available in the public domain. The event was an intentional, targeted attack by a knowledgeable person on an industrial control system. The case study examines the event from a cyber security perspective. It provides the timelines and cyber issues, examines the NIST SP800-53 controls that were violated or not met, and posits the potential mitigation that would have occurred if the NIST SP800-53 controls had been followed. The intent of this analysis is not to criticize any actions taken, but to look forward as to how lessons learned from this case can be of help to prevent future incidents.

Attack Overview

Vitek Boden, a man in his late 40s, worked for Hunter Watertech, an Australian firm that installed SCADA (Supervisory Control And Data Acquisition) radio-controlled sewage equipment for the Maroochy Shire Council in Queensland, Australia. Boden applied for a job with the Maroochy Shire Council, apparently after he walked away from a "strained relationship" with Hunter Watertech. The Council decided not to hire him. Consequently, Boden decided to get even with both the Council and his former employer. He packed his car with stolen radio equipment attached to a (possibly stolen) computer. He drove around the area on at least 46 occasions from February 28 to April 23, 2000, issuing radio commands to the sewage equipment he (probably) helped install. Boden caused 800,000 liters of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel. "Marine life died, the creek water turned black and the stench was unbearable for residents," said a representative of the Australian Environmental Protection Agency.[2] Boden coincidentally got caught when a policeman pulled him over for a traffic violation after one of his attacks. A judge sentenced him to two years in jail and ordered him to reimburse the Council for cleanup. Boden's attack became the first widely known example of someone maliciously breaking into a control system. There are a few other reports of this attack. Slay and Miller, "Lessons Learned From the Maroochy Water Breach"[3] refer to a non-public analytic report by the civil

1 The authors thank Ron Southworth, DHS CSSC SME (Australia), and Jill Slay, University of South Australia, for sharing their insights into this attack.

2 http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

3 In IFIP International Federation for Information Processing, Volume 253, Critical Infrastructure Protection, eds. E. Goetz and S. Shenoi; (Boston:Springer), pp. 73–82. Available at http://www.wcc2008.org/site/IFIPSampleChapter.pdf.

engineer in charge of the water supply and sewage systems at Maroochy Water Services during the time of the breach as provided by Mustard[4].

Introduction

This case study analyzes the event to determine how the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls might have prevented or mitigated the event. The intent of this analysis is not to criticize any actions taken, but to look forward as to how lessons learned from this case can be of help to prevent future incidents.

The Maroochy Shire attack has been documented in the Crown criminal case[5]. The offences occurred between 9 February 2000 and 23 April 2000 when Vitek Boden accessed computers controlling the Maroochy Shire Council's sewerage system and altered electronic data in the sewerage pumping stations causing malfunctions in their operations.

NIST Special Publication 800-53 and Related Documents

NIST has established an Industrial Control System (ICS) Security Project[6] to improve the security of public and private sector ICS. NIST SP 800-53 revision 2, December 2007, *Recommended Security Controls for Federal Information Systems*, provides implementing guidance and detail in the context of two mandatory Federal Information Processing Standards (FIPS) that apply to all federal information and information systems, including ICSs. FIPS 200 requires that federal agencies implement minimum security controls for their organizational information systems based on the FIPS 199 security categorization of those systems. Private sector and other organizations may consider the use of these standards and guidelines as appropriate. NIST is working with all stakeholders and other interested parties to develop convergent guidance on the application of these security requirements to ICS.

Revision 2 of SP 800-53 incorporates guidance on appropriate safeguards and countermeasures for federal ICS, that is also potentially applicable and useful for the private sector. NIST's Computer Security Division (Information Technology Laboratory) and Intelligent Systems Division (Manufacturing Engineering Laboratory), in collaboration with the Department of Homeland Security and organizations within the federal government that own, operate, and maintain industrial control systems, developed the necessary ICS augmentations and interpretations for the security controls, control enhancements, and supplemental guidance in SP 800-53. The ICS augmentations and interpretations will facilitate the employment of appropriate safeguards and

4 http://www2.theiet.org/OnComms/sector/computing/Library.cfm?ObjectID=0482B3C1-D0B1-80C6-57EA91E4FB429C23

5 Supreme Court of Queensland r v Boden, Vitek 2002, CA Number 324 of 2001 DC Number 340 of 2001. http://www.courts.qld.gov.au/qjudgment/QCA%202002/QCA02-164.pdf.

6 NIST Industrial Control System Security Project , http://csrc.nist.gov/sec-cert/ics/index.html

countermeasures for these specialized information systems that are part of the critical infrastructure of the United States.

In developing the ICS augmentations and interpretations, the original set of controls, enhancements, and supplemental guidance contained in Appendix F in SP 800-53 were not changed. ICS Supplemental Guidance provides additional guidance on how to apply a control in ICS environments. ICS Enhancements are enhancement augmentations to the controls that are required for some ICS. ICS Enhancement Supplemental Guidance provides guidance on how to apply an enhancement in ICS environments.

FIPS Publication 199 provides standards for categorizing information and information systems based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Categorization of an information system must take into consideration potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts.

The security controls specified in SP 800-53 are organized into *classes* and *families* for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., management, operational, and technical) and seventeen security control families.[7] Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family. Table 1 summarizes the classes and families in the security control catalog and the associated family identifiers. A list of the minimum security controls, or security control baselines, for low-impact, moderate-impact, and high-impact information systems, as determined by applying the criteria in FIPS 199 have been published separately: LOW-impact baseline at sp800-53-rev2-annex1.pdf; MODERATE-impact baseline at sp800-53-rev2-annex2.pdf; and HIGH-impact baseline at sp800-53-rev2-annex3.pdf. These are available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-annex1.pdf, http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-annex2.pdf, and http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-annex3.pdf, respectively.

[7] The seventeen security control families in NIST Special Publication 800-53 are closely aligned with the seventeen security-related areas in FIPS 200 specifying the minimum security requirements for protecting federal information and information systems. Families are assigned to their respective classes based on the dominant characteristics of the controls in that family. Many security controls, however, can be logically associated with more than one class. For example, CP-1, the policy and procedures control from the Contingency Planning family, is listed as an operational control but also has characteristics that are consistent with security management as well.

TABLE 1: 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

Maroochy Shire Site Description

Maroochy Shire, a rural area of great natural beauty and a tourist destination, is located about 100 kilometers north of the Queensland State Capital of Brisbane. It has an area of approximately 1,157 square kilometers with a population of approximately 120,000. Maroochy Shire has 880 kilometers of gravity sewers treating an average of 35 million liters/day. Maroochy Water Services Sewerage SCADA System consists of 142 Sewage Pumping Stations with two Monitoring Computers utilizing three Radio Frequencies. Hunter Watertech Pty Ltd installed the "PDS Compact 500" computer device at each pumping station capable of receiving instructions from a central control center, transmitting alarm signals and other data to the central computer and providing messages to stop and start the pumps at the pumping station. Communications between pumping stations and between a pumping station and the central computer were by means of a dedicated analog two-way radio system operating through repeater stations. Each repeater station transmitted on a different frequency.

The Attack

The offences occurred between February 9, 2000 and April 23, 2000. Vitek Boden accessed computers controlling the Maroochy Shire Council's sewerage system, altering electronic data in particular sewerage pumping stations causing malfunctions in their operations. Vitek Boden had been employed by Hunter Watertech as its site supervisor on the Maroochy SCADA project for about two years until resigning in December 1999. At about the time of his resignation he approached the Council seeking employment. He was told to enquire again at a later date. He made another approach to the Council for employment in January 2000 and was told that he would not be employed. The sewerage system then experienced a series of faults:

- Pumps were not running when they should have been
- Alarms were not reporting to the central computer
- A loss of communication between the central computer and various pumping stations.

An employee of Hunter Watertech, Mr. Yager, was appointed to look into the problem. He began monitoring and recording all signals, messages and traffic on the radio network. As a result of his investigations he concluded that many of the problems being experienced with the system resulted from human intervention rather than equipment failure. Other technical experts shared his opinion. Further, the evidence revealed that the problems associated with the attack ceased when Vitek Boden was arrested. On an occasion during Mr. Yager's investigations, he ascertained that pumping station 14 seemed to be the source of the messages corrupting the system. He physically checked the pumping station and ascertained that it was working properly and bore no signs of having been physically tampered with. He concluded that the source of the false messages was a PDS Compact 500 computer with an address of 14 and he changed the identification number of pumping station 14 to 3 so that any legitimate messages from that station could be identified as coming from station 3. Conversely, any messages coming from a station identifying itself as 14 would be known to be bogus.

On March 16, 2000, when malfunctions occurred in the system, Mr. Yager communicated over the network with a bogus pump station 14 that was sending messages to corrupt the system. He was temporarily successful in altering his program to exclude the bogus messages but then had his computer shut out of the network for a short period. The intruder was now using PDS identification number 1 to send messages. Further problems then occurred as a result of a person gaining remote computer access to the system and altering data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way.

The central computer was unable to exercise proper control and, at great inconvenience and expense, technicians had to be mobilized throughout the system to correct faults at affected pumping stations. On one occasion, a pumping station overflowed causing raw sewerage to escape.

On April 23, 2000, an intruder, by means of electronic messages, disabled alarms at four pumping stations using the identification of pumping station 4. The intrusions began just after 7:30 pm and concluded just after 9:00 pm. By this time Vitek Boden had fallen under suspicion and was under surveillance. Police officers located a vehicle driven by him. When Boden's vehicle was pulled over and searched at around 10:00 pm, a PDS Compact 500 computer, later identified in evidence as the property of Hunter Watertech, was found, as was a laptop computer.

On examination it was found that the software to enable the laptop to communicate with the PDS system through the PDS computer had been re-installed in the laptop on February 29, 2000. The PDS Compact computer had been programmed to identify itself as pump station 4 – the identification used by the intruder in accessing the Council sewerage system earlier that night. The software program installed in the laptop was one

developed by Hunter Watertech for its use in changing configurations in the PDS computers. There was evidence that this program was required to enable a computer to access the Council's sewerage system and had no other practical use. The unchallenged evidence of Sergeant. Kingsley, a police computer expert, was that the program had been used at least 31 times between April 7 and April 19 and that it was last used at 9:31 pm on April 23, 2000. Also found in the car was a two-way radio set to the frequencies of the repeater stations and the leads necessary to connect the PDS computer, the laptop and the radio.

Mr. Yager and others gave evidence that the conduct of the person responsible for the unauthorized interventions in the computer system displayed a detailed familiarity with the system, beyond that which was likely to be held even by Council technical staff. Technical experts other than Mr. Yager also gave evidence that the computer malfunctions, the subject of the charges, were the result of human intervention. When apprehended by police Boden asserted in a taped conversation that all the items in the vehicle were his own. He said he had been up to Rainbow Beach and that he used the computer for study, personal correspondence and work in his family business. He later sent a letter to the police requesting the immediate return of his property. Examination of the laptop found in the car revealed start up and shut down times (on and after February 28, 2000) consistent with the time of the attacks which Mr. Yager had uncovered and which he had logged.

The existence of other problems in the system showed that the malfunctions were the result of human intervention. Once it was demonstrated that the malfunctions resulted from human intervention, the existence of other problems became of limited significance. Mr. Yager was adamant that the malfunctions in the system could only have been caused by unauthorized human intervention.

Boden sought to establish that some of the electronic messages that gave rise to the charges could have been caused by system malfunction or by error on the part of Council employees. One of his arguments in this regard showed three sets of identical messages on the same day from addresses 000, 099 and 004. The Crown contended that only the message emanating from address 004 was initiated by Boden. Boden pointed to the other messages as evidence that defective messages of the nature of those relied on by the Crown may have been caused other than by human intervention.

Another witness, Mr. Lewer–an engineer specializing in computer engineering who, for a time, was Hunter Watertech's project engineer on the installation of the computerized sewerage system– said that all three messages were generated by the PDS configuration program used on the PDS Compact computers. Mr. Lewer's opinion was that the messages, other than the ones from address 004, were generated by persons attempting to rectify the result of the alleged unauthorized intervention. He also gave evidence that that 000 and 099 messages were not causing damage to the computer system. Mr. Yager gave evidence some days later than Mr. Lewer and thus had more opportunity to consider the possible explanations for the 000 and 099 messages. His evidence was that these messages occurred over several days and resulted from the actions of maintenance staff

who were either employees of Hunter Watertech or Council employees under direction of the former. He ruled out the possibility of mechanical error. He said that the 004 messages were definitely generated by a person different from the one who generated the other messages.

Timeline

1997-December 1999 - Vitek Boden employed by Hunter Watertech as site supervisor
December 3, 1999 - Boden resigns from Hunter Watertech
Early December 1999 - Boden approached City Council seeking employment
Early January 2000 - Boden reapproached City Council and was turned down
February 9-April 23, 2000 – SCADA system experiences series of faults
March 16, 2000, Hunter Watertech investigator tried to troubleshoot system
April 19, 2000 Log indicates system program had been run at least 31 times
April 23, 2000 Boden disabled alarms at four pumping stations using the identification of pumping station 4. The intrusions began just after 7:30 pm and concluded just after 9 pm
April 23, 2000 Boden pulled over by police with computer equipment in car
October 31, 2001 –Boden convicted in trial – sentenced to 2 years
March 21, 2002 – Appeal rejected

Evidence

The counts on which Boden was found guilty related to acts of cyber penetration which commenced on or about February 28, 2000.

- The laptop taken by the police from Boden's vehicle had been reloaded with most of its software operating programs on February 28, 2000
- PDS software file had been installed or re-installed on the laptop on February 29 at 3:46 pm. This is the software used to run or access the computers in the sewerage system.
    - Run at least 31 times prior to April 19
    - Last run on April 23
- Two-way radio was of the type used in the Council's communication system.
    - Tuned into the frequencies of the repeater stations
    - Serial numbers on the radio matched delivery docket provided by the supplier of the radios to Hunter Watertech.
- PDS Compact 500
    - Address set to 004
    - Serial number identified it as a device which should have been in the possession of Hunter Watertech.

Attack Summary

- Vitek Boden was an insider who was never an employee of the organization he attacked.
    - He was an employee of a contractor that supplied IT/control system technology to the Maroochy Shire Council.

    - With his knowledge he was the “ultimate insider”.
- The service contract was deficient or inadequate concerning Watertech’s responsibilities
    - Management, technical and operational cyber security controls required
    - Personnel security controls that applied to its employees such as background investigations and protection from disgruntled employees
- A number of anomalous events occurred before recognition that the incidents were intentional.
    - As a skillful adversary, Boden was able to disguise his actions.
    - Extensive digital forensics were required to determine that a deliberate attack was underway
- There were no existing cyber security policies or procedures.
- There were no cyber security defenses.

Observations

As reported by Slay & Miller, Robert Stringfellow was the civil engineer in charge of the water supply and sewage systems at Maroochy Water Services during the time of the breach and has presented his analysis in closed forums. Stringfellow observed:

- At first it was easier to blame installation errors for the problems.
- Upon reinstalling all the software and checking the system, pump station settings kept changing beyond the ability of the system to do this automatically
- Conclusion: an external malicious entity was using wireless equipment to access the SCADA system.

Stringfellow's analysis of the incident made several important points:

- It is very difficult to protect against insider attacks.
- Radio communications commonly used in SCADA systems are generally insecure or are improperly configured.
- SCADA devices and software should be secured to the extent possible using physical and logical controls
- It is often that case that security controls are not implemented or are not used properly
- SCADA systems must record all device accesses and commands, especially those involving connections to or from remote sites; this requires fairly sophisticated logging mechanisms.

Stringfellow also recommended the use of anti-virus and firewall protection along with appropriate use of encryption. He emphasized a need for upgrade-able SCADA systems (from a security perspective), proper staff training, and security auditing and control.

Applying SP 800-53 Controls

This case revolves around a disgruntled insider who was never an employee of the organization he attacked. Some of the issues raised by analysis of this case are just being addressed by cyber security practitioners 8 years later. Some are unresolved with no solution in sight. .

All of Boden's malicious activities are addressed by SP 800-53 controls, as detailed below. Several pervasive prophylactic measures covered by SP 800-53 controls immediately come to mind. These measures, not related to an specific malicious activity are discussed first. Table 2 lists problems uncovered by the investigation into the attack and the corresponding SP 800-53 control that could have prevented or mitigated it.

TABLE 2: SP 800-53 PERVASIVE PROPHYLACTIC CONTROLS

PROBLEM	CONTROL FAMILY
Policy and Procedures	The first control in every control family addresses policy and procedure.
Personnel Security	Personnel Security (PS)
Hardware & Software	System and Services Acquisition (SA)
Awareness and Training	Awareness and Training (AT)
Audit	Audit and Accountability (AU)
Contingency Planning	Contingency Planning (CP)
Incident Response	Incident Response (IR)
Information Protection	System and Communications Protection (SC)

Policy and Procedures

Every organization should have cyber security policy and procedures. There are many discretionary and judgmental activates that require guidance. Common sense isn't sufficient; dos and don'ts need to be written down.

Neither organization had cyber security policies or procedures in place. For example: AC-18 Wireless Access Restrictions (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system.. Such policy would have addressed the two-way radio that was used by Boden.

The first control in every control family addresses policy and procedure. With minor variations, the control begins: "The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate …." Although enumerated for each control family, the family policy can be included as part of the general information security policy for the organization. Family control procedures can be developed for the security program in general, and for a particular information system, when required.

Personnel Security

Since Boden was never a Maroochy Council employee, direct hiring controls by the Maroochy Council were technically not applicable. However, is it prudent for to have a key personnel clause to protect the client from unilateral changes in key personnel by the contractor. In general, the contract should extend applicable Personnel Security controls to contractor employees. Determining which controls to apply to on-site contractor

personnel may not be easy since it depends on the role played by the individual. The Personnel Security family (PS) contains the following controls:

PS-1	Personnel Security Policy and Procedures	PS-5	Personnel Transfer
PS-2	Position Categorization	PS-6	Access Agreements
PS-3	Personnel Screening	PS-7	Third-Party Personnel Security
PS-4	Personnel Termination	PS-8	Personnel Sanctions

PS-7 identifies the need for contractual obligations on the subcontractor concerning personnel security. Controls PS-3 and 4 should certainly be considered. In practice many positions may be occupied by employees or contractors. The contractual obligations should support equal treatment for direct employees and contractor employees.

System and Services Acquisition

Hunter Watertech supplied hardware, software, and services to the Maroochy Shire Council. The cyber security responsibilities of the contractor organization (e.g., Hunter Watertech) and the contractor's employees (e.g., Boden) should be included in the contract between the organizations. Almost all of the controls applicable to direct employees are also applicable to contractor employees, but the exact details may vary. Many of these controls also obligate the contractor organization concerning record keeping and other support services. Applicable security controls are in the System and Services Acquisition family (SA) are listed below. There is no indication that any of these controls were included in the contract between Hunter Watertech and Maroochy Shire Council. All the controls are important; we believe that SA-4 and 11 might have helped directly in in this case.

SA-1	System and Services Acquisition Policy and Procedures	SA-7	User Installed Software
SA-2	Allocation of Resources	SA-8	Security Engineering Principles
SA-3	Life Cycle Support	SA-9	External Information System Services
SA-4	Acquisitions	SA-10	Developer Configuration Management
SA-5	Information System Documentation	SA-11	Developer Security Testing
SA-6	Software Usage Restrictions		

Awareness and Training

Personnel were not trained in preventing, recognizing, or responding to cyber-related incidents. Security awareness and training inform personnel of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks. The Awareness and Training family (AT) contains the following controls:

AT-1	Security Awareness and Training Policy and Procedures	AT-4	Security Training Records
AT-2	Security Awareness	AT-5	Contacts with Security Groups and Associations
AT-3	Security Training		

Every control except AT-5 could have helped in this case. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program,* provides additional information.

Audit

The Maroochy communications and control components lacked sufficient audit capability to support fault determination or forensic analysis. Audit is concerned with collecting information that is significant and relevant to the security of the information system. Audit supports other control families such as incident response, access control, and flaw remediation. The Audit and Accountability family (AU) contains the following controls:

AU-1	Audit and Accountability Policy and Procedures	AU-7	Audit Reduction and Report Generation
AU-2	Auditable Events	AU-8	Time Stamps
AU-3	Content of Audit Records	AU-9	Protection of Audit Information
AU-4	Audit Storage Capacity	AU-10	Non-repudiation
AU-5	Response to Audit Processing Failures	AU-11	Audit Record Retention
AU-6	Audit Monitoring, Analysis, and Reporting		

AU-2, 3, 4, 6, 7,9, and 11 apply to this case.

Contingency Planning

The analysis indicates that there were no plans to deal with an emergency or system disruption. Effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. The Contingency Planning family (CP) contains the following controls:

CP-1	Contingency Planning Policy and Procedures	CP-6	Alternate Storage Site
CP-2	Contingency Plan	CP-7	Alternate Processing Site
CP-3	Contingency Training	CP-8	Telecommunications Services
CP-4	Contingency Plan Testing and Exercises	CP-9	Information System Backup
CP-5	Contingency Plan Update	CP-10	Information System Recovery and Reconstitution

CP-2, 3, 4, 5, and 8 apply to this case. NIST SP 800-34 provides guidance on contingency planning.

Incident Response

Response to the sewerage discharge was ad hoc. Considerable time elapsed during troubleshooting before malicious intent was considered. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, restoring computing services, and apprehending malefactors. Because performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources. Establishing clear procedures for assessing the current and potential business impact of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data. Building relationships and establishing suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement) are also vital. The Incident Response family (IR) contains the following controls:

IR-1	Incident Response Policy and Procedures	IR-5	Incident Monitoring
IR-2	Incident Response Training	IR-6	Incident Reporting
IR-3	Incident Response Testing and Exercises	IR-7	Incident Response Assistance
IR-4	Incident Handling		

All of these controls are applicable to the Maroochy system. NIST SP 800-61 provides guidance on incident handling and reporting. NIST SP 800-83 provides guidance on malware incident handling and prevention.

Information Protection

Cryptography is employed as a protective mechanism for many objectives. A second line of defense that was widely deployed only in 2006 was encryption protection of information in stolen and lost devices.

The US Office of Management and Budget (OMB) issued a policy memorandum in June 2006[8], recommending safeguards for all federal government agencies. Safeguards relevant to this case are:

- Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by the Deputy Secretary or an individual he/she may designate in writing.
- Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

While this OMB policy was issued in response to loss or theft of devices containing Personal Identification Information (PII), its phrasing encompasses protection of all sensitive data and information. The specific intent of this policy is to compensate for the protections offered by the physical security controls when information is removed from, or accessed from outside of the agency location and when information is physically transported outside of the agency's secured, physical perimeter (this includes information transported on removable media on portable/mobile devices such as laptop computers and/or personal digital assistants).

The System and Communications Protection family (SC) contains 23 controls. The controls addressing cryptography are:

SC-1	System and Communications Protection Policy and Procedures	SC-13	Use of Cryptography
SC-9	Transmission Confidentiality	SC-17	Public Key Infrastructure Certificates

The OMB policy is more explicit. This policy would have addressed the laptop and two-way radio that were in Boden's possession when he was arrested. However, since Boden had reloaded the software and no data disclosure was involved, the practical impact is little to none.

Malicious Activities

Table 3 lists Boden's malicious activities and the corresponding SP 800-53 control that could have prevented or mitigated it.

TABLE 3: MALICIOUS ACTIVITY AND CORRESPONDING CONTROLS

MALICIOUS ACTIVITY	CONTROL FAMILY
Stealing equipment	Media Protection (MP)
Issuing radio commands	Access Control (AC) Identification and Authentication (IA)
Falsifying network address	Access Control (AC)

8 Office of Management and Budget, *Protection of Sensitive Agency Information*, M-06-16, June 23, 2006. http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf

Sending false data and instructions	System and Information Integrity (SI)
Disabling alarms	

Access Control

Access Control is the process of granting or denying specific requests for obtaining and using information and related information processing services. This is one of the fundamental controls on any IT system. Most access controls are based on the identity of the person, process, or device involved. Therefore, Identification and Authentication are intimately tied with access control. Access controls need to be applied appropriate to the communications environment.

Access controls are the first line of defense against error and omissions and malicious attacks from insiders and outsiders. The Access Control family (AC) contains the following controls:

AC-1	Access Control Policy and Procedures	AC-11	Session Lock
AC-2	Account Management	AC-12	Session Termination
AC-3	Access Enforcement	AC-13	Supervision and Review—Access Control
AC-4	Information Flow Enforcement	AC-14	Permitted Actions without Identification or Authentication
AC-5	Separation of Duties	AC-15	Automated Marking
AC-6	Least Privilege	AC-16	Automated Labeling
AC-7	Unsuccessful Login Attempts	AC-17	Remote Access
AC-8	System Use Notification	AC-18	Wireless Access Restrictions
AC-9	Previous Logon Notification	AC-19	Access Control for Portable and Mobile Devices
AC-10	Concurrent Session Control	AC-20	Use of External Information Systems

Multiple access controls would have alleviated or prevented the attack, including: **AC-2 ACCOUNT MANAGEMENT** "The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts…"; **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 documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions…."; **AC-18 WIRELESS ACCESS RESTRICTIONS** "The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system." With the enhancement **"**The organization uses authentication and encryption to protect wireless

access to the information system."; and **AC-20 USE OF EXTERNAL INFORMATION SYSTEMS** "the organization restricts the use of personally owned information systems."

Identification and Authentication

Identification is the process of determining the identity of a user, process, or device, and authentication is the process of verifying the putative or claimed identity, often as a prerequisite to allowing access to resources in an information system. The Identification and Authentication family (IA) contains controls that would prevent unauthorized access to the control system:

IA-1	Identification and Authentication Policy and Procedures	IA-4	Identifier Management
IA-2	User Identification and Authentication	IA-5	Authenticator Management
IA-3	Device Identification and Authentication	IA-6	Authenticator Feedback
IA-4	Identifier Management		

IA-2 USER IDENTIFICATION AND AUTHENTICATION "The information system uniquely identifies and authenticates users (or processes acting on behalf of users) … through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination therein…."; and **IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION** "The information system identifies and authenticates specific devices before establishing a connection, [using] either shared known information (e.g., Media Access Control (MAC) or Transmission Control Program/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication)" are the primary controls. IA-4 and IA-5 provide management for the parameters used.

Portable Device Protection

Part of defense-in-depth is recognizing that when some protections fail, there should be more controls to help protect the organization. Theft of portable electronic equipment occurs, often for the value of the equipment rather than the information stored. Boden's attack was an exception to this generality.

The control specified in MP-2, *Media Acces*s, is deceptively simple: "The organization restricts access to information system media to authorized individuals." Supplemental guidance elaborates: "Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access.

Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access."

System Monitoring

Another part of defense-in-depth is determining that something is going wrong. The cause may be an intruder, often masquerading as an authorized user, or a malfunction. **SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES** "The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system" provides a context for alerting personnel of a suspected anomaly. If applied regularly and systematically, the type of forensics performed by Hunter Watertech and the police might have detected the attack earlier.

Conclusions

The 2000 Maroochy Shire cyber event is important because it provides a public record of an intentional, targeted attack by a knowledgeable person on an industrial control system. The attack by an insider who is not an employee demonstrates several critical physical, administrative, and supply chain vulnerabilities of industrial control systems. The key issue is the treatment of vulnerabilities coming from suppliers or others outside the organization. Contractor and sub-contractor personnel are often overlooked as a potential attack source. The technical issues demonstrate the difficulty in identifying a control system cyber attack and retaking control of a "hijacked" system. Once alerted to this type of attack, ICS owners and operators may have adequate controls to protect their assets. However, a determined, knowledgeable adversary such as Vitek Boden could potentially defeat these controls.