THE METROPOLITAN WATER DISTRICT
OF SOUTHERN CALIFORNIA

Report
Office of the General Auditor

Internal Audit Report for July 2017

Summary

One report was issued during the month:

1. **Cyber Security Review – SCADA Network**

Discussion Section

This report highlights the significant activities of the Internal Audit Department during July 2017. In addition to presenting background information and the opinion expressed in the audit report, a discussion of findings noted during the examination is also provided.

Cyber Security Review – SCADA Network

Background

The Water Systems Operation Group (WSO) uses commercial SCADA solutions to provide enterprise-wide, real-time monitoring and control of remote terminal units (RTUs), programmable logic controllers (PLCs), instruments, and various operations systems. These components operate 24/7 throughout the Colorado River Aqueduct, treatment plants and the conveyance and distribution system. Moreover, the SCADA system supplies information for more than 80 core business functions at Metropolitan. These functions include water billing, maintenance management, geographic information systems, regulatory compliance, and power management.

WSO is responsible for maintaining the SCADA network and applications whereas the Information Technology Group provides technical support. The SCADA systems are based on Hewlett-Packard (HP) servers using Windows, Red Hat Linux, Oracle relational databases, and SCADA applications.

Our review consisted of evaluating the adequacy of cyber security controls over the SCADA network. Specifically, we conducted vulnerability scans to identify potential weaknesses, evaluated intrusion detection and prevention mechanisms, reviewed user account and password management, assessed physical security for remote, unmanned SCADA devices, and examined incident management procedures. In addition, we reviewed the Cyber Vulnerability Assessment Reports performed by an outside security consultant in 2012 and 2015.

Opinion

In our opinion, the cyber security controls over the SCADA network include those practices usually necessary to provide for a generally satisfactory internal control structure. The degree of compliance with such policies and procedures provided effective control for the period ending November 30,

2016. Although this opinion is an acceptable rating, we do express concern over the lack of documentation that details action plans to resolve the software and hardware findings noted in the cyber vulnerability assessment reports. Moreover, we note that the recommendations made in a 2015 report indicated the fact that they were included in the 2012 report but had not been resolved. We also identified additional vulnerabilities in our review.

Furthermore, we are concerned that communication of the two consultant reports along with a corrective action plan was not made to available executive management. This conduct suggests that the reports and the findings were withheld for parochial reasons.

Comments and Recommendations

MANAGEMENT REPORTING

Metropolitan’s SCADA network represents a significant investment and is a key information system that supports essential aspects of operations and the business continuity. The critical nature of these operations dictates that a comprehensive cybersecurity policy framework of computer security be established to prevent, detect, and respond to cyber-attacks. Implicit to this strategy is the fact that any compromise or attack of the SCADA system could cause damage and/or disruption to the flow and treatment of water.

In response to these concerns, the information technology infrastructure unit established data security controls that segregated the SCADA system from business systems by use of a DMZ and firewalls. In computer networks, a DMZ (demilitarized zone) is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet. External-facing servers, resources, and services are located in the DMZ so they are accessible from the Internet but the rest of the internal LAN remains unreachable. This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data via the Internet.

In addition to these operational strategies, the infrastructure unit contracted with an outside security consultant in 2012 to complete a cybersecurity assessment of the SCADA system. These efforts disclosed a large number of vulnerabilities, due in a large part to the older outdated Windows operating systems running in the SCADA environment, and due to technical difficulties that prevented updating the servers and workstations with the latest hardware and software security patches. The majority of these cyber vulnerabilities were attributed to security findings that could have been remediated by applying the latest vendor software patch or by upgrading to the latest software version. This outside review exposed the need for attention and focus in the area of patch management whereby program updates are installed that are designed to improve the usability and performance of systems and applications.

It is important to note that the consultant also opined that mitigating controls, such as the DMZ, provides an extra layer of protection, since any attacks coming from the internet or the business networks will have firewall segments that will need to be breeched before the malicious code could have an effect on the SCADA system components.

Documentation of communication to executive management of these concerns along with corrective actions could not be located. That a detailed management report and formal response could not be found suggests that the report was not disclosed to superiors and that the findings were withheld for parochial reasons.

Moreover, this conjecture seems to be corroborated by the results of a second cybersecurity assessment performed in 2015, by the same outside security consultant. The objective of this review was twofold. First, how well did the District remediate prior security findings from the 2012 cyber assessment? Secondly, had any new vulnerabilities emerged that required remediation?

The 2015 review revealed that many of the issues identified in the prior report had not been resolved and new vulnerabilities were noted. Specifically, it stated: "The need for greater diligence for patch management was pointed out in the 2012 security assessment, and this is still an issue that has both technical and operational constraints that should be resolved so the SCADA servers and workstations can be patched on a more frequent basis." Moreover, we note that both the 2012 and 2015 assessment reports were withheld from executive management. We provided these reports to management in February 2017, at the conclusion of our audit fieldwork.

Our concern is twofold. First, detailed action plans to resolve the hardware and software vulnerabilities on a timely basis should have been crafted. Such plans could not be located. Secondly, the decision to accept the inherent risk of disregarding reported cyber vulnerabilities was made by line management. It is critical that technical managers as a collective not aggregate to themselves the powers and influence to make strategic decisions that should be made at a more senior level.

We believe it is imperative that strategic planning function at the executive management level. This is especially true when an organization is considering the risk/control dynamic and setting priorities, focusing energy and resources, and accepting inherent risk levels in accordance to their risk tolerance.

TONE AT THE TOP

Employees must be convinced of the District's commitment to a transparent climate, and of the central role that they play in ensuring that the District's code is followed. They must view compliance with the code of conduct, standards, and control systems as a central priority, and understand that they will be rewarded for their behavior, even if it uncovers some problem that others might prefer to remain undisclosed.

During our review, we noted:

- There is clear evidence of line manager involvement accompanied by a veil of secrecy in the administration of the two SCADA Cyber Vulnerability Assessment consultant reports. This resulted in an absence of transparency in the decision making process, over reliance on the DMZ/firewall strategy, and inflated expectations regarding risk mitigation. These actions were embedded in a culture of nondisclosure that was both reckless and ill-advised.

- The cyber security contractor contributed to these transgressions. Whether legal or illicit, there was at least an implicit link between the softened 2012 report and the expectation that a future contract would be awarded. If the contractor had been open, transparent and thorough in discussing identified vulnerabilities with executive management, concern that such links existed would certainly have been diminished.

One of the principal factors that senior management should recognize is the possibility that they will not be able to discover or even have reasonable grounds to suspect that line management may have or is engaging in improper conduct. Collusion among members of management to engage in and hide improper conduct is difficult to detect even by prudent oversight in the normal and rigorous course of the District's affairs.

We recommend that WSO and Information Technology Management collaborate in reminding personnel of the importance of compliance with the policies that govern business practices that requires decisions and policy to be made in the proper channels of governmental structure.

VULNERABILITY MANAGEMENT

Vulnerability management is a process that detects, responds to, and remediates security flaws in networks and communication infrastructures. Effective security controls enhance cyber security defenses around networks to protect data confidentiality, integrity, and availability. These controls include password management policies, system logs, event monitoring, vulnerability scans, penetration tests to identify weaknesses in the network, online alert mechanisms for detecting intrusions, and cyber security incident management procedures.

During our review we noted:

1. Scans of over 60,000 plug-ins identified five "High" and 14 "Medium" vulnerabilities.
2. The system log analysis and event monitoring procedures were not thoroughly documented. We also noted an automated log analysis tool was not configured to provide immediate alerts.
3. No dedicated intrusion detection devices are installed inside the SCADA Network to prevent security compromises and threats by unauthorized users. It should be noted that two firewalls and demilitarized zones are installed to restrict unauthorized access from outside the network.

4. Screen lockout time settings for SCADA operating systems and applications are not consistent. SCADA OnSite application is set to time out after one hour. SCADA desktops are set to timeout after 30 minutes. Finally, ClearSCADA, an AMR application, is set to timeout after 10 hours.
5. One testing account ID in SCADA OnSite application was still active at the time of our review.

The vulnerabilities identified above, could expose Metropolitan to undetected intrusions, resulting in disruptions to water operations and financial losses to the District.

We recommend that WSO and Information Technology Management collaborate to:

1. Conduct periodic vulnerability assessments and resolve noted issues.
2. Complete log analysis and event monitoring procedures and configure the automated log analysis tool to provide immediate alerts.
3. Consider implementing intrusion detection devices inside the SCADA network.
4. Reevaluate the screen time lockout policies to ensure they are reasonable and consistent.
5. Deactivate testing account IDs.

PHYSICAL SECURITY CONTROLS

Physical security controls help prevent, detect, and minimize security risks to physical property, information systems, and other assets. For Metropolitan's remote SCADA devices, physical security controls should reduce the risk of theft, sabotage, intrusion, and malicious intercepts.

During our review, we noted that one SCADA RTU located in Long Beach suffered three break-ins between the period of December 2015 and January 2016. A router, a cellular modem, and an uninterruptible power supply (UPS) were stolen as a result. Although WSO reinforced a steel box enclosing the RTU after the second incident, the corrective action was not sufficient to prevent the third intrusion.

Without adequate physical security, cyber assets can be stolen or damaged. Unauthorized physical access might also allow intruders to compromise the network, causing disruptions to operations and financial loss to the District.

We recommend that WSO and Information Technology Management collaborate in conducting an assessment of security measures over critical SCADA assets and implement additional safeguards where needed.