Security Logging in the Utility Sector: Roadmap to Improved Maturity

Seth Bromberger

National Electric Sector Cybersecurity Organization

Clifford Maraschino

Southern California Edison

Acknowledgement / Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000516.

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

The authors would like to thank the following individuals and organizations for their participation in the NESCO Security Logging Working Group and for their valuable contributions to this paper:

Justin Clarke, *NESCO*

Kyle Hussey, *Grant County PUD*

Balaji Palanisamy, *Coalfire Systems*

Justin Turner, *Dell SecureWorks*

David Hatchell, *McAfee*

Eric Knapp, *NitroSecurity*

Ingrid Rayo, *Florida Power and Light*

Document Number	WP2012-01-02
Revision	1.0
Publication Date	12 March 2012

1. OVERVIEW

Logging and analysis of event and status data from critical and non-critical assets is a common fundamental requirement for an effective information security program. However, standards for event logging vary widely; this disparity extends to the implementation of processes as well as technologies. This paper provides an overview of current recommendations for establishing effective security logging. While the paper has been written with the electric sector as a primary audience, the concepts and recommendations should be applicable for other sectors as well, especially those sectors designated as being Critical Infrastructure / Key Resource (CI/KR).

Understanding the criticality of effective security logging (and, by extension, robust monitoring), the U.S. Department of Energy (DOE) and the National Electric Sector Cybersecurity Organization (NESCO) convened a "Security Logging Working Group" (SLWG) to suggest recommended capabilities to industry and the vendor community for this foundational activity. The group met between August and November 2011 via conference calls and online collaboration to create these recommendations. This document is the joint product of the SLWG.

NOTE: Logging and monitoring within the electric sector is required by current cybersecurity standards: see, *e.g.*, CIP-007 Version 1, R6[1]. While this document provides recommendations that may be used to help meet these regulations, the authors do not guarantee that specific implementations based on this document will be sufficient to meet current or future standards.

2. APPROACH

A simple list of "best practices" is problematic for a number of reasons: the definition of a best practice is vague; and most lists of best practices are binary evaluations: either an organization implements a practice, or it does not; and it is difficult to see the interrelatedness among the listed practices. The SLWG decided instead to approach the discussion of capabilities using a Capability Maturity Model (CMM) that provides some flexibility in evaluating an organization's ability to effectively collect and analyze data that might be security-significant.

A CMM provides a way for an organization to determine its current level of capability of an area of focus (called a *process area*) relative to a set of objective metrics. It also provides guidance on improving capabilities and performance within the process area. More information on the structure and advantages of a CMM approach may be found in Section 3.0 of the SSE-CMM[2] and in Section 2 of the IA-CMM[3]. We reproduce two paragraphs from the latter document for additional clarification:

[1] http://www.nerc.com/files/CIP-007-1.pdf, retrieved 28 December 2011

[2] http://www.sse-cmm.org/docs/ssecmmv3final.pdf, retrieved 28 December 2011

[3] http://www.isatrp.org/IA-CMMv3_1.pdf, retrieved 28 December 2011

> A capability maturity model (CMM) ... describes the stages through which processes progress as they are defined, implemented, and improved. The model provides a guide for selecting process improvement strategies by determining the current capabilities of specific processes and identifying the issues most critical to quality and process improvement within a particular domain. A CMM may take the form of a reference model to be used as a guide for developing and improving a mature and defined process.
>
> A CMM may also be used to appraise the existence and institutionalization of a defined process that implements referenced practices. A capability maturity model covers the processes used to perform the tasks of the specified domain, (e.g., security engineering). A CMM can also cover processes used to ensure effective development and use of human resources, as well as the insertion of appropriate technology into products and tools used to produce them. The latter aspects have not yet been elaborated for security engineering.[4]

3. STRUCTURE OF THE CMM

The SLWG CMM approach provides a six-level model for gauging the maturity of a given process area. These six levels, numbered 0 through 5, are defined as follows:

CMM Level 0 (Not Performed): Indicates that the organization does not perform the activity described in the process area definition.

CMM Level 1 (Performed Informally): Activity is characterized by ad hoc, chaotic, unplanned efforts. Little formality exists. "Individuals within the organization recognize that an action should be performed, and there is general agreement that this action is performed as and when required. There are identifiable work products for the process"[5]

CMM Level 2 (Planned and Tracked): The process area is documented such that attempts at repeating steps are feasible. "Performance according to specified procedures is verified. Work products confirm to specified standards and requirements. Measurement is used to track ... performance."[6]

CMM Level 3 (Well Defined): The activity is defined as a standard business operation with established, documented processes. "The primary distinction from Level 2 ... is that the process is planned and managed using an organization-wide standard process"[7]

CMM Level 4 (Quantitatively Controlled): The activity can be actively managed / improved and adapted to specific projects without a measurable decrease in quality or effectiveness. "Detailed measures of performance are

[4] *ibid.*

[5] http://www.sse-cmm.org/docs/ssecmmv3final.pdf, retrieved 28 December 2011, p. 67

[6] *ibid.,* p. 71

[7] *ibid.,* p. 89

collected and analyzed... Performance is objectively managed, and the quality of work products is quantitatively known."[8]

CMM Level 5 (Continuously Improving): Focus of activity is on applying improvements and changes to enhance the quality of the service provided based on the quantitative metrics produced by Level 4. *"The primary distinction from [CMM Level 4] is that the defined process and the standard process undergo continuous refinement and improvement, based on a quantitative understanding of the impact of changes to these processes"*[9]

Within each process area, several subcategories introduce common areas of focus, referred to as "critical aspects". It is important to note that critical aspects do not receive individual CMM ratings; only one rating (from *Level 0* to *Level 5*) is assigned per process area.

Each process area model is designed to be used both as a benchmark of existing capabilities, and as a guideline for future improvements within the respective process area. In the SLWG CMM, the models may be depicted as grids, with the maturity levels defined by row and critical aspects of the process area by column. The capability measurement for a given maturity level for a given critical aspect is listed in the box that intersects the given row and column. Where no capability measurement exists for a given level/aspect intersection, there is no additional capability required for that aspect at that level.

The critical aspects are used solely to provide delineation among different aspects of the process area and should not be used to provide multiple evaluations of an organization's maturity within a process area. Organizations are evaluated solely based on their meeting the capabilities across ALL critical aspects for a given maturity level; therefore, the organization's assessed level is the *lowest* measured capability rating among the set of critical aspects within the process area.

The critical aspects used for both logging and monitoring CMMs are defined as follows:

Prerequisite: defines capabilities that are required to be in place before an organization can start assessment at a particular maturity level.

Activity: provides details on the required activity of the organization in order to affect the desired outcome within the process domain.

Integration: describes the required relationships between the process domain and other external and internal organizational processes.

Process: describes the required documentation of uniform work steps, standards, and policy required for a given maturity level.

[8] *ibid.*, p. 101

[9] *ibid.*, p. 107

Staff: provides details on the required capabilities of staff and other personnel performing activities related to the process domain. This column also lists requirements for resources available to staff to perform the required duties effectively.

Tools: describes the maturity level of tools and systems used in the execution of the process domain activities.

Training: evaluates the presence and maturity of a training program relevant to the process domain.

4. LOGGING CMM

Appendix A contains the capability maturity models to be used by energy sector utilities when evaluating the maturity of their security logging process.

5. MONITORING CMM

No discussion of security logging would be complete without a discussion of the intended use of these logs; namely, to detect anomalous activity through aggregation, correlation, and monitoring of the logs and event data. While monitoring is arguably outside the scope of this project, the SLWG believes a cursory discussion of monitoring capabilities helps inform some of the related logging capabilities.

The monitoring CMM is a draft provided in Appendix B for discussion and contextual purposes.

6. DATA SOURCES

In addition to evaluating an organization's maturity in the logging and monitoring of security data, the SLWG evaluated the types, sources, and uses of the security-related event information. As each organization's business processes and deployed technologies are different, the group decided against creating a process area CMM dedicated to data sources. Additionally, when analyzing which data sources to include, it quickly became apparent that the end-state requirement is almost always to log everything possible and to store it for as long as permissible.

Organizations will usually focus on one of several standard issues when deciding which devices to monitor and which events to log. Many focus on what may be required to understand and respond to incidents which they have encountered or believe they will encounter. The most common example to this in any technology-driven company is *Failed Logon Attempt* errors.

A secondary decision point occurs when organizations realize that logging information will require continuously increasing funding as the retained data require additional storage space and processing power to store, correlate, and analyze. Organizations can choose to reduce retention of logs, disable logging of specific data altogether, or expand their logging infrastructure to meet increasing requirements. A common instinctive reaction is to disable logging of data perceived to be of no use. At least one group member recollected organizations which disabled logging of *Successful Logons* in their central authentication system.

A well-known technology company has publicly stated that their logging practice is to identify metrics and event information which they believe would be necessary to identify an operational problem or security incident. This company also has a process to identify new metrics and events which are required when incident response procedures are activated. The company configures each of its systems to report all of these metrics across all servers, both new as well as those already deployed. This practice enables a consistent capability to report on all systems and allowing the incident response teams to address issues without worrying whether logs exist and are enabled for the specific systems under investigation.

A list of data sources that organizations should consider logging is provided in Appendix C. The list should be used as a starting point for discussion in reviewing current logging practices and as a roadmap for future development of log sources as the organization matures its logging and monitoring processes.

7. CONCLUSIONS / RECOMMENDATIONS

NESCO and the members of the SLWG make the following recommendations to the security organizations that have responsibility for critical electric infrastructure:

- Determine the ideal capability maturity level for the organization based on resource (staff and financial) availability and risk tolerance;
- Evaluate current capabilities for both security logging and security monitoring against the respective CMMs;
- Perform a gap analysis to determine the difference between current and ideal capability maturity levels;
- Participate in collaborative activities (such as information sharing) to augment current capabilities;
- Define and implement a plan for continuous improvement and periodic assessment of capabilities.

Appendix A: Security Logging Capability Maturity Model

CMM Level 0 (Not Performed):

Prerequisite: None.

Activity: New systems are not configured to log activity. Logging configurations are not consistent and no predefined logging configurations exist. Log analysis/aggregation systems do not exist. Log information is not dependable.

Integration: Logging is not integrated with other business processes.

Process: There are no policies to identify scope and storage of log data. There are no defined processes or standards to ensure consistent logging. The server or device provisioning process does not include log configuration.

Staff: No staff members are dedicated to the logging function.

Tools: No log analysis or log aggregation systems exist. Log tools are not supported by IT. No hardware is dedicated for logging.

Training: Training programs do not exist.

CMM Level 1 (Performed Informally):

Prerequisite: None.

Activity: Log analysis/aggregation systems are informal. Systems are installed with vendor default configurations for logging. Log information is difficult to find.

Integration: Other business departments presume that logging activities occur without verifying. Log functions are still relatively isolated with other processes.

Process: Policies and standards for logging configurations exist. IT manages logs at the device level.

Staff: Staff members are assigned to the maintenance and support of the logging infrastructure and configuration as a secondary duty.

Tools: *Ad hoc* logging tools are used on a personal level. Some hardware is dedicated for logging.

Training: Training programs are informal, consisting of peer training without job aids. Topics of training are specific to the current task and not to any other topics.

CMM Level 2 (Planned and Tracked):

Prerequisite: All requirements from CMM Level 1 must be met.

Activity: Minimum logging requirements have been defined. Systems are built using predefined logging configurations and are required before deploying the device. The systems only log at the required minimum level. Logs are stored on each device and personnel have to collect logs manually from different sources. Logs are available to operations and security staffs.

Integration: Logging is partially integrated with relevant business and security processes. Log fields and event codes for each data source are defined and documented.

Process: Logs are managed with consistency across the same type of system or the same classification of systems. The server or device provisioning process includes log configuration.

Staff: Staff members are dedicated to the maintenance and support of the logging infrastructure as a primary duty.

Tools: *Ad hoc* logging tools are installed and available for use by staff. Tools exist for the maintenance of logging configurations and the management of log data.

Training: Formal training programs exist, conducted as seminars, with appropriate materials for review and reference. Time is set aside specifically for the training and topics cover a wide range of areas.

CMM Level 3 (Well Defined):

Prerequisite: All requirements from CMM Level 2 must be met.

Activity: Security and Operational Log configuration requirements are identified at the project or program level. Post-installation validation of successful logging occurs. Logs are aggregated centrally in a limited fashion (e.g., only logs from systems of the same type or only logs from certain classified systems). Personnel collect logs from multiple aggregators or centralized loggers.

Integration: Logging is fully integrated with other business and security processes. Data sources are normalized within the logging system(s). Appropriate severity and priority categories are defined for each source.

Process: There is a documented process to ensure consistent application of logging configurations when adding new systems or modifying existing systems. These configurations include a determination of centralized or decentralized storage of logs and the retention period. Policies include type and scope of log data to be collected, as well as defined standards for data retention. Logging is defined as one of the criteria for assessing new projects in the project management process.

Staff: The logging function has clearly defined staffing requirements with full job descriptions that include responsibilities, daily tasks, and required certifications. Resources exist to ensure correct application of logging configuration and policies. These resources conduct periodic checks to ensure correct functioning of the logging processes.

Tools: Standardized tools exist to manage the configuration of servers to ensure consistent and continuous logging. Multiple decentralized logging tools are used.

Training: There are documented training courses for all staff members and these courses include a base level of understanding for each level of staff member. Training courses include specific topics that may be unique to a company's environment.

CMM Level 4 (Quantitatively Controlled):

Prerequisite: All requirements from CMM Levels 1 through 3 must be met.

Activity: Logging configurations and policies are regularly tested. Metrics relating to logging configurations and activities are generated. The organization has the ability to detect systems where logging has failed. Aggregated logs across infrastructure and different systems are available to analysts with a reasonable certainty. Changes to logging configurations are made in response to emerging threats and new vulnerability information.

Integration: Logging is recognized and regularly tested as a key component of the organization's business and security processes. Data sources from other business processes (e.g., Accounting, Finance, IT, Marketing, Sales, Physical Security, etc.) are available for correlation and analysis. Formal processes exist to integrate these data sources into the comprehensive logging practice. Documented processes exist to assign appropriate severity and priority categories consistently, across all data sources.

Process: Logging checks are defined in change control processes, and standard checks are defined in post change validation requirements. A log policy exists and is updated regularly.

Staff: Staff members have a documented performance goal related to logging activities.

Tools: Centralized logging is in place and tools are supported by IT and the business. Tools are consistently used, documented, well understood, and supported by appropriate resources.

Training: Relevant technical training is updated on a periodic basis, and is mandatory for staff involved in logging efforts.

CMM Level 5 (Continuously Improving):

Prerequisite: All requirements from CMM Levels 1 through 4 must be met.

Activity: An established lifecycle for enhancements to system logging configuration exists. Centralized Integrated logging extends beyond security requirements and collects operational, flow and activity logs for holistic view of the environment. Log messages are archived and access to log messages is controlled. Logging data is available to all analysts with a need to know.

Integration: Measures of program effectiveness are documented and regularly tested. Tests of related business and security processes include logging as a component. External data sources are regularly reviewed and tested for integration with the logging function. Where appropriate, event data is shared with other business departments.

Process: Efficacy of logging is validated by internal audit and reviewed by top management. Compliance against the log policy is reported regularly. Policies governing access to logging data are documented and regularly audited for compliance. Results of the audits are documented and fed back as proposed improvements to the program.

Staff: Staff redundancy exists to ensure uninterrupted availability of logging components and infrastructure.

Tools: Appropriate storage for long-term retention of logs is in place. Logging solution is a system with high availability requirements and full IT support, including clearly defined Service Level Agreements (SLAs). Tools for logging are reviewed and refined in response to feedback and effectiveness.

Training: Training is uniform across staff members. Even if completed by different analysts, logging configurations for the same type of system or same classification of devices will yield similar (if not exact) results. The training program is documented and integrated into staff performance goals.

Appendix B: Security Monitoring Capability Maturity Model

CMM Level 0 (Not Performed):

Prerequisite: None.

Activity: Organization's monitoring efforts are *ad hoc*, not coordinated, and not planned.

Integration: Monitoring is not integrated with other business or security processes, or is not included in/aligned with the organization's incident response plan.

Process: Systems and processes for consistent analysis of data do not exist or are not formalized/standardized.

Staff: Staff members are not dedicated to monitoring function; monitoring is a secondary duty.

Tools: Tools for monitoring are not standardized.

Training: Training programs are informal or do not exist.

CMM Level 1 (Performed Informally):

Prerequisite: None.

Activity: Monitoring is performed in response to incidents or other external events.

Integration: No change from previous level.

Process: No change from previous level.

Staff: No change from previous level.

Tools: Standard tools for monitoring exist.

Training: No change from previous level.

CMM Level 2 (Planned and Tracked):

Prerequisite: All requirements from CMM Level 1 must be met.

Activity: Monitoring is performed as a regular operation.

Integration: No change from previous level.

Process: Systems and processes for consistent analysis of data exist.

Staff: Monitoring is performed by security staff as a secondary or auxiliary job duty.

Tools: No change from previous level.

Training: Formal training for staff is available on a limited basis.

CMM Level 3 (Well Defined):

Prerequisite: All requirements from CMM Levels 1 and 2 must be met.

Activity: No change from previous level.

Integration: Monitoring is integrated into other business/security processes and into the organization's incident response plan.

Process: Systems and processes for consistent analysis are formalized/standardized.

Staff: Monitoring is performed by security staff as a primary duty.

Tools: Standard tools exist and are exclusively used in the normal course of operations.

Training: Training on security monitoring is included as part of a formal training program.

CMM Level 4 (Quantitatively Controlled):

Prerequisite: All requirements from CMM Levels 1 through 3 must be met.

Activity: Monitoring process is 24x7 without interruption.

Integration: No change from previous level.

Process: Formal processes exist and are implemented for monitoring. Institutional knowledge is applied to analysis process. SLAs exist for timely review of event data and other logs. Compliance to processes is checked regularly.

Staff: Security staff members assigned to monitoring role have relevant formal training / certifications.

Tools: Tools to support monitoring are documented, well understood, and supported by appropriate technical resources.

Training: Training specific to security monitoring is available and encouraged (or mandatory).

CMM Level 5 (Continuously Improving):

Prerequisite: All requirements from CMM Levels 1 through 4 must be met.

Activity: Monitoring is performed around the clock by trained professionals (as evidenced by certification and training programs).

Integration: Monitoring program is recognized and regularly tested as a key component of organization's incident response plans and other relevant business/security processes. Results of testing are fed back as proposed improvements to the program. Measures of program effectiveness are documented and regularly tested.

Process: Concurrent, integrated monitoring of multiple sources is performed, with correlation and aggregation of data with appropriate application of institutional knowledge. Ability to perform ad hoc queries and advanced correlative analysis (both in terms of resources and capability), and to migrate these queries/analyses into regular monitoring cycles within a reasonable period, exists.

Staff: Staff redundancy exists to ensure continuous monitoring. Peer review of analysis prior to release is formalized and encouraged.

Tools: Tools to support monitoring are reviewed and refined in response to feedback and effectiveness.

Training: Training is uniform across monitoring resources. Analysis of the same data by different analysts will yield similar (if not exact) results. Training program is documented and integrated into staff performance goals.

Appendix C: Data Sources

Remote Access (VPN, Citrix, Web Mail, Dial-Up)

- Source information
    - IP Address
    - Automatic Number Identification (ANI) / Caller Identification (CID)
- Session Information
    - User ID
    - Event ID (to be correlated with vendor ID's used) / Where vendor has not progressed to using Event IDs - a summary or description of event
    - Source ID (could be packet info, vendor session id's, ip address, hostname, etc...)
    - Source Application (Source process that is sending the event - System, Web server, Database etc. may also use Process id)
    - Destination ID
    - Start Time
    - End Time
    - Volume of Data Transferred (In and Out as separate values)

Smart Metering & AMI

- Tamper Switch Activation
- Boot, Reboot, Last Gasp
- Metrology data (reads, voltage information)
- Service Disconnect status
- Operational events

Control Network Systems

- ICCP
- OASIS
- OATI
- SCADA
- Tagging

Core IT Systems / Intranet Services

- Web Proxy Logs, including all available information regarding SSL connections
- Email Logs from DMZ mail relays as well as internal MTAs and Exchange, Notes, or other corporate email systems
- Outbound firewall allow/deny events
- DNS resolution traffic for all hosts
- DHCP events
- centralized authentication events
- Windows AD events
- LDAP events
- TACACS and RADIUS events
- SecureID or other two-factor
- Application authentication events
- Application and network performance events and alerts
- NAC
- ARP cache information
- Network equipment events / logs, with sources to include IDS, IPS, switches, routers, load balancers, and DLP.
- Host CPU, memory, network I/O, other performance, capacity, or utilization statistics
- Port Scan activity
- Anti-virus/Anti-malware logs
- Host-based firewall/IDS/IPS logs
- Netflow/Jflow/Cflow/Cflowd/Rflow/IPFIX/NetStream data (access to the raw data)
- Service specific logs (*e.g.*, Citrix AppFlow data, web server logs, application logs)
- Source-Routed Traffic
- All physical security events (access granted, denied, wrong time, wrong pin, door forced, door held, reader failure, controller failure, *etc*.