SANS ANALYST PROGRAM

Sponsored by RSA

2010 Sixth Annual

SANS Log Management Survey: Mid-Sized Businesses Respond

A SANS Whitepaper – June, 2010

Written by: Jerry Shenk

Why SMBs Collect Logs

How SMBs Use Logs

Log Collection

Log Management Challenges

Executive Summary

Every year since 2005, the SANS Institute has conducted a survey to find out how organizations collect and use their logs; what they aren't currently using their log for but would like to; and what they see as the biggest problems with log management.

This year, we are also taking a special look at how log management issues affect small and mid-sized businesses with fewer than 2000 employees. In our 2010 Log Management Survey, 223 respondents fit this category. These businesses represented a wide range of industries with financial organizations having the largest representation (21 percent), followed by government organizations (18 percent), education (10 percent), and telecommunications (8 percent). The remaining industries, in order, were spread across manufacturing, healthcare/pharmaceutical, energy/utilities, engineering/construction and retail.

The majority of survey respondents were on staff with their respective organizations, as opposed to being a consultant, with a nearly even breakdown between top four roles and a worthwhile representation of compliance staff to note (see Figure 1).

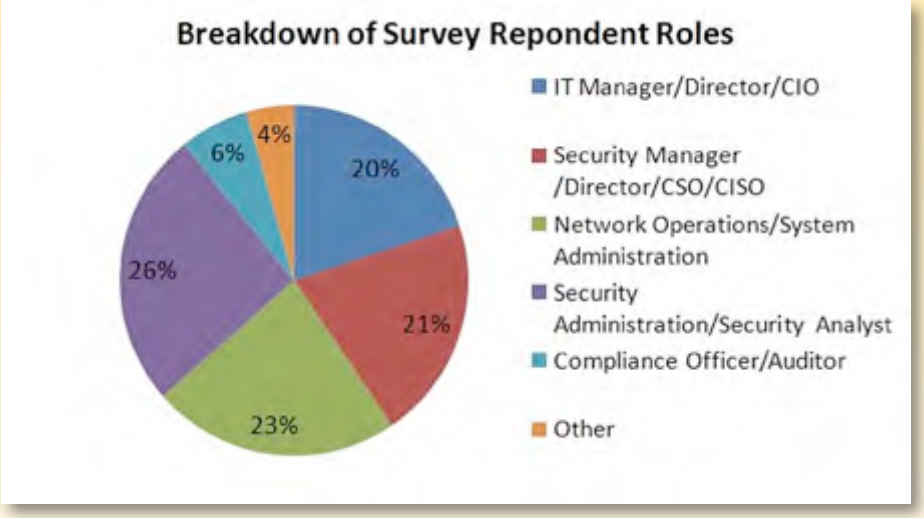

Figure 1: Respondent's Roles

Organizations in our sample size of 2000 or fewer employees usually have different issues than larger organizations do, particularly around budget and staffing, which was supported in our survey breakdown.

For SMB respondents, detecting events was clearly the most important reason for collecting logs; but they also show almost equal interest in the operational efficiency advantages of log management, particularly when asked about usefulness of those logs.

When it comes to usefulness of the data, the SMB group ranked "Forensic Analysis and Correlation" as most useful. It was, however, almost in a dead heat against the operational areas of "Detect/Prevent Unauthorized Access and Insider Abuse," "Track Suspicious Behavior," and "IT Troubleshooting and Network Operations." This replicates the kind of progression we're also seeing at larger organizations: Once they install their log management systems, they find practical, business-impacting value for log data analysis, which is leading to more uses of their logs.

The interesting finding in the SMB segment is the difference between why they collect logs and what they're actually using them for. SMB respondents chose "Detect/Prevent Unauthorized Access and Insider Abuse" and "Forensic Analysis and Correlation" as their first and second reasons for collecting logs, while they found forensics support to be the most useful, followed by detection. In the 2009 survey, the small business group also selected forensics as the most important use, followed by "Tracking Suspicious Behavior and Monitoring User Activity."

While surveys show growth in all areas of log management, the market has more to improve on, particularly in the area of providing useful information to business units.

Why SMBs Collect Logs

Detecting and preventing unauthorized access and insider abuse was clearly the top reason our SMB survey base chose for collecting log data (see Figure 2). After that, regulatory requirements, forensic analysis and troubleshooting all came in pretty much even with "Forensic Analysis and Correlation" having a slight edge for second place for those who considering this to be critical and important.

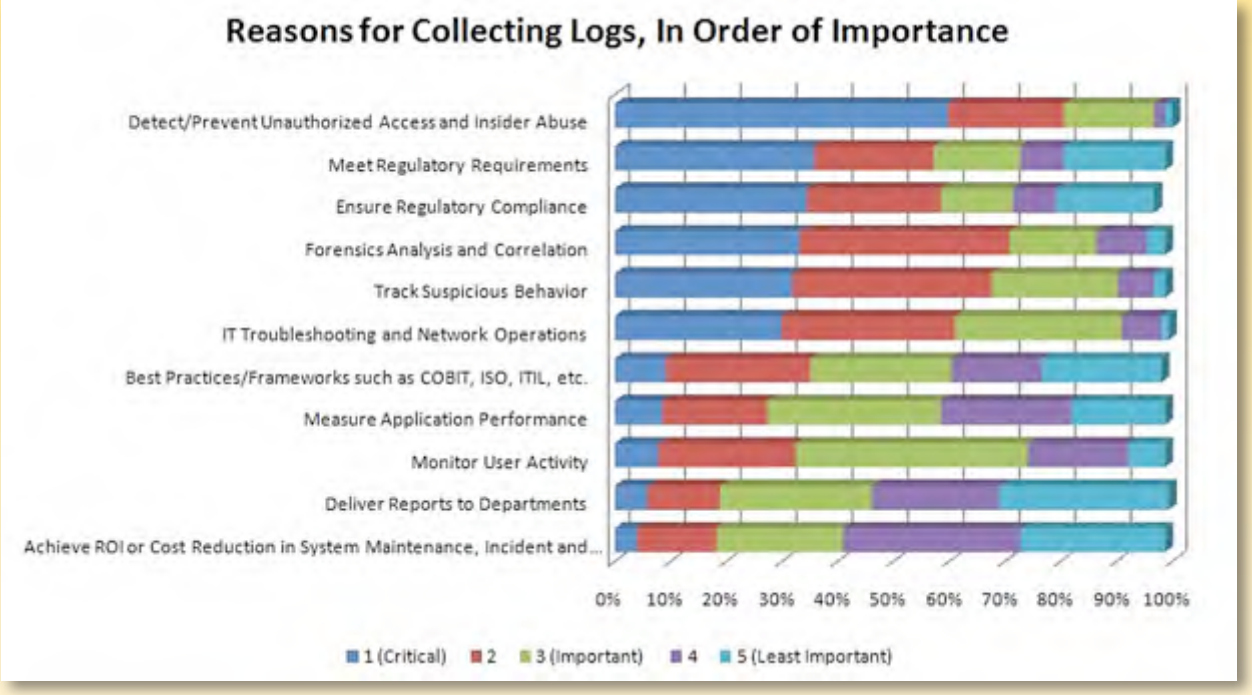

Figure 2: Reasons for Collecting Logs—Small- to Mid-Sized Businesses

One somewhat troubling issue is that "Deliver Reports to Departments" came in almost last in terms of log collection. With the stated importance of security, it seems the ability to get meaningful reports to business units should also be higher on the list of reasons for collecting logs. Perhaps this low statistic is because reporting is lagging behind where SMB personnel know that it should be—so perhaps they've given up a bit on the reporting. Reporting aspects of log management also rated low in the 2009 log management survey among this group. Log management vendors are doing a lot of work on the reporting front end. Expect to see more enhancements to their reporting functions over the next few years.

How SMBs Use Logs

While they may be collecting logs first to detect and prevent unauthorized access and abuse and second for forensics and followup, the majority of SMBs reported their usefulness in the reverse order. They responded that logs are most useful for "Forensics Analysis and Correlation," followed by "Detect/Prevent Unauthorized Access and Insider Abuse." This is an interesting flip and a positive sign that small- to mid-sized businesses are getting additional value out of their log management systems.

The difference for usefulness was not that vast. Usefulness for both detection and forensics came in at over 90 percent, while detection as a reason for collection was almost 80 percent and forensics was almost 70 percent. In the 2009 survey, roughly 60 percent of this group chose forensics, and about the same percent ranked another category of tracking suspicious behavior as the top uses for logs.

Based on this year's survey, there are four categories in which SMBs find log management systems to be most useful: Forensics, detection, tracking and troubleshooting (see Figure 3). The most useful feature of log management systems was "Forensics Analysis and Correlation," followed closely by "Detect/Prevent Unauthorized Access and Insider Abuse," "Track Suspicious Behavior" and "IT Troubleshooting and Network Operations."

These are all categories in which people are actually getting things done, not just marking a checkbox on a form to say they're doing it.

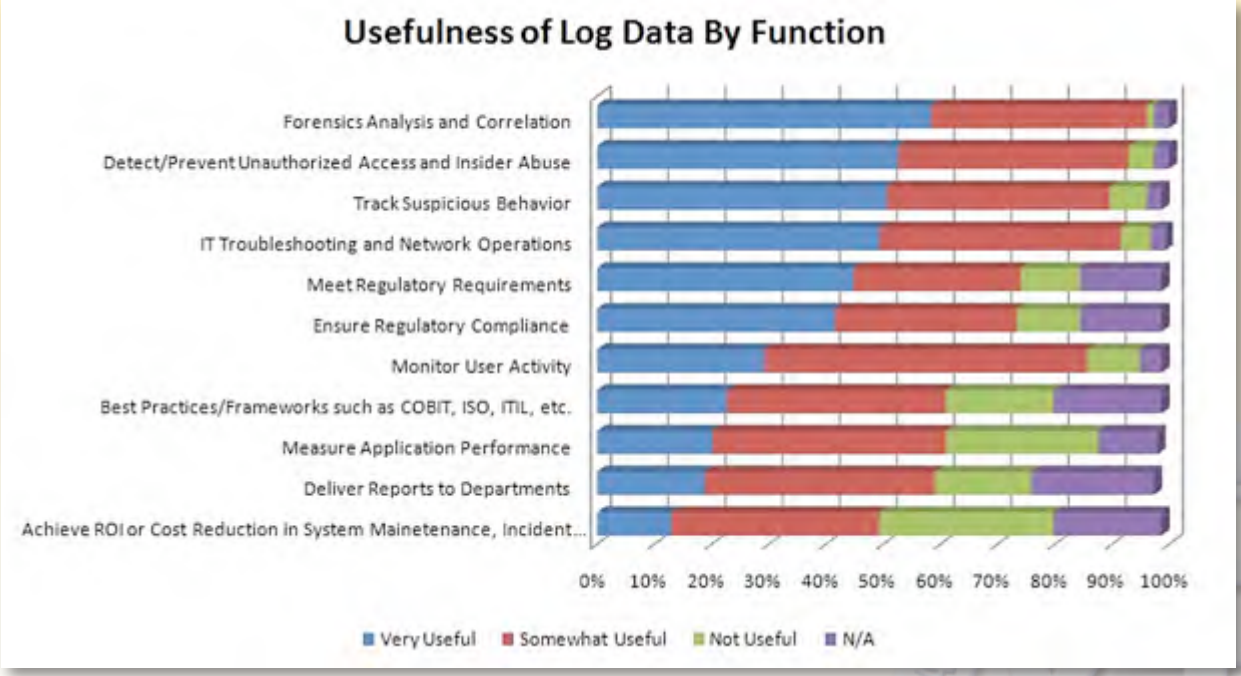

Figure 3: Usefulness of Log Data

While reporting scored low in terms of reasons for collecting logs, they are getting useful information for purposes like forensics analysis and other top usefulness categories. This indicates that organizations are able to get the data they need from their logs, even if they don't have the reporting features that they would like.

Another useful function of the logs was for meeting regulatory requirements, although logs are not as useful for that purpose as for others. One factor that would decrease the usefulness of this function for SMBs is that the smallest organizations are not subject to some of the regulatory burden that is placed on the larger organizations.

Even though security is most popular use for log data, it is important to note that when "Very Useful" and "Somewhat Useful" responses are combined, over 95 percent of the SMB respondents found their logs to be useful for "IT Troubleshooting and Network Operations." This is a solid indication that log management products are maturing and that log management personnel are also learning how to get what they need from these systems.

Log Collection

The SMBs that responded to the survey are collecting logs from the expected sources, including security and network devices, servers and mainframes. We're also seeing that 49 percent of SMBs are collecting log data from "Physical Devices" like badge access systems and plant control systems. This is a new category that was added this year due to feedback from last year's survey respondents. Some of the comments specifically referenced HVAC systems and other systems that are typically not considered to be involved with IT. This is an encouraging development, indicating that log management has moved past simply being a toy for the IT group to play with to being an integral part of the organization as a whole. It will be interesting to see how this use of log management systems plays out in the future.

This year, 84 percent of small- to mid-sized businesses have log servers: 31 percent of these organizations have a single log server, 42 percent have two to five log servers, and the remainder have more. Of these organizations, 41 percent spend "A few man-hours per week" analyzing logs, with 14 percent spending a few hours a day managing logs.

Log Management Challenges

Since our first SANS Log Management Survey in 2005, we've been monitoring the challenges associated with log management. In our early surveys, collection was the largest problem for all survey respondents. For the SMBs that were surveyed in 2010, collection was not a major problem, rather it the majority said collection was their "Least Challenging" problem (32 percent of responses).

This year, as shown in Figure 4, the most challenging aspect of log management is "Searching through Data," followed closely by, "Analysis and Reports." Searching and reporting are critical areas on which log management vendors continue to spend their resources. There are a number of reasons for the problems with analysis. One major reason is that different devices report events differently. Application and software vendors need to work on consistency in reporting he log data that they generate.

As indicated in their answers about what they find useful, small- to mid-sized businesses know the data is available. What organizations want is better reporting tools to put it in context.

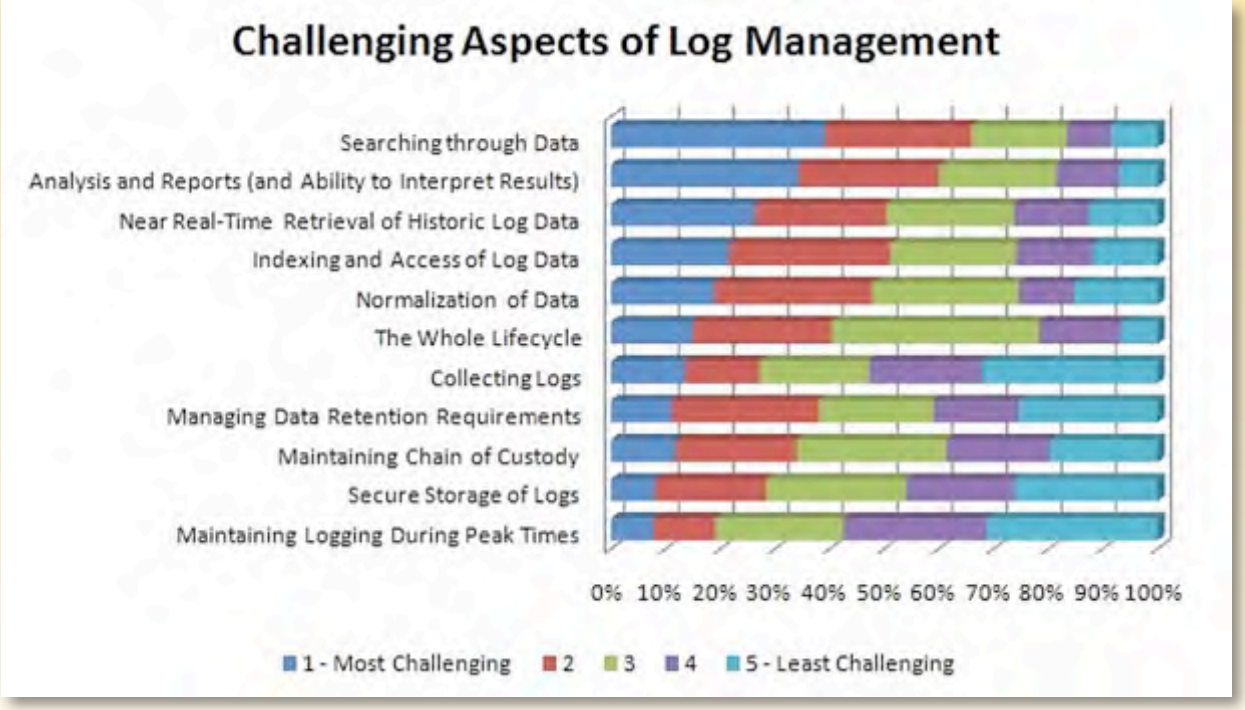

Figure 4: Log Management Challenges

Summary

Log management systems are becoming more embedded in day-to-day operations. This year's survey respondents are even collecting and managing log data from physical plants and other nontraditional log sources. SMB organizations are finding value in log management systems for non-IT needs, such as HVAC and badge access systems, as well as the more traditional IT functions of detecting and preventing suspicious behavior, forensics analysis and troubleshooting.

The widespread collection and evolving uses of log data indicate that log management is maturing. Regulatory requirements are also driving organizations to enhance their log management systems.

Small- and mid-sized organizations are getting data from their log management systems when they search for it, and they are doing that more than in the past. They are, however, having difficulty when it comes to generating reports that can be shared with other departments and management.

We expect to see that regulatory requirements to be a driving force to behind log management in the future. Organizations will also continue to find new value in their log data as they become more familiar with what is available and as reporting improvements continue to be made to the log management systems. In addition, log management systems will improve with the addition of tools that will add intelligence to the analysis process through better reporting, presentation and decision support capabilities. These enhancements will blur the line between a traditional log management system and a Security Information and Event Management (SIEM) system.

About the Author

Jerry Shenk currently serves as a senior analyst for the SANS Institute and is the senior security analyst for Windstream Communications in Ephrata, Pa. Since 1984, he has consulted with companies and financial and educational institutions on issues of network design, security, forensic analysis and penetration testing. His experience spans small home-office systems to global networks. Along with some vendor-specific certifications, Jerry holds six GIAC certifications, all completed with honors: GCIA, GCIH, GCFW, GSNA, GPEN and GCFA. Five of his certifications are Gold certifications.

SANS would like to thank this paper's sponsor:

The Security Division of EMC