HARFORD COUNTY, MARYLAND
Office of the County Auditor

AUDIT OF NETWORK SECURITY MONITORING CONTROLS

Report Highlights

Why We Did This Audit

This audit was conducted as part of the County Auditor's risk-based Annual Audit Plan approved by the County Council for FY2015.

What We Found

We noted that controls should be improved to ensure all devices are correctly configured and monitored.

What We Recommend

Management should ensure inventory and RunBook lists are routinely reviewed and updated.

Report Number: 2015-A-01A
Date Issued: 09/18/2015

Council Members and County Executive Glassman:

In accordance with Section 213 of the Harford County Charter, we have performed an audit of Harford County's controls over Network Security Monitoring.

The audit found Presidio Network Solutions has been monitoring and reporting on network events in accordance with its contract. However, there are some networking devices that are not being monitored for unusual activity because Harford County has not updated the information it provides to Presidio. This issue is impacted, in part, by the County's ongoing network improvements. New devices are purchased, added to the network, and/or decommissioned frequently and related documentation is not updated timely. We also found that documentation related to network configuration changes could be improved.

More detailed results of the audit, our findings and recommendations for improvement are included in the attached report. We would like to thank the members of management for their cooperation during the audit. The audit team is available to respond to any questions you have regarding the attached report.

Sincerely,

Chrystal Brooks, CPA

Chrystal Brooks
County Auditor

cc: Mr. Ted Pibil, Director of Info. and Comm. Technology
Mr. Billy Boniface, Director of Administration

212 South Bond Street * Room 219 * Bel Air, Maryland 21014
410-638-3161 * www.harfordcountymd.gov/auditor

HARFORD COUNTY, MARYLAND
Office of the County Auditor

REVIEW RESULTS

We have audited Harford County's controls over Network Security Monitoring for the period of 7/1/2013 through 4/15/2015. Harford County has configured its information network across multiple sites and continues to update and expand the infrastructure. For all of the networking components, a vendor is primarily responsible for monitoring traffic and device events to detect and prevent threats to the network's integrity.

Our opinion, based on the evidence obtained, is the vendor, Presidio Networked Solutions, is meeting the terms of its contract with Harford County; however, Harford County can improve its communication with Presidio to ensure all active devices are monitored and properly configured. The audit approach focused on testing the key controls that address management's objectives for the process. Conclusions drawn are below.

Risk	Expected Control	Conclusion
The network infrastructure is inadequate for users' needs	Management is periodically advised of network availability trends and security incident trends.	Satisfactory
Unauthorized users gain access to County resources	Devices connected to the network infrastructure are monitored for unusual activity.	Unsatisfactory
	Allowed IP addresses have demonstrated justification.	Satisfactory
	Changes to infrastructure configurations are reviewed to ensure they were implemented correctly.	Needs Improvement
Users are unable to access required resources because of a network failure	Management is notified when devices are unavailable and when unusual activity is detected or prevented.	Satisfactory
Users inadvertently allow malicious software into the network	Devices connected to the network receive regular anti-virus and malware definition updates.	Satisfactory

Areas for improvement are described in the Findings and Recommendations section of this report. Management has been provided an opportunity to respond to this report; the response provided concludes this report.

FINDINGS AND RECOMMENDATIONS

Finding Number: 2015-A-01.01 RunBook Completeness

The RunBook, documenting monitored networking devices, is not up to date.

Analysis: We compared the list of monitored devices to the County's inventory list and noted that many were not being monitored. Based on management's explanation that some inventory items are not connected to the network, we selected a sample to determine if missing items were in fact, not in service. For our sample of 20 devices, 2 should have been included in the RunBook. If those results are extrapolated to the population, there may be more than 40 devices connected to the County's network that are not being monitored by Presidio for unusual activity.

Recommendation: We recommend ICT update the RunBook as network infrastructure changes are made and forward an updated version to Presidio at least monthly.

Management Response: Management agrees that the RunBook does not reflect the current status of network devices. Management believes that having the RunBook accurately reflect the current status of all networking devices is impossible. Management's current procedure is that once a project is complete or several sites have been upgraded an add/remove list is sent to Presidio, at a minimum the list is sent monthly. With all the major projects currently underway (renovations at 220, DES projects, HMAN, MES project, GasBoy project-to name a few), Management believes the most efficient and practical method for keeping the RunBook as current as possible is to send the monthly update and an updated list to Presidio continue the current practice.

Expected Completion Date: Recommendation by Auditor for monthly updates is Management's current practice.

Finding Number: 2015-A-01.02 Network Configuration Changes

Documentation was not available to confirm that implemented network configuration changes were approved prior to implementation or reviewed after

implementation.

Analysis: The current Control Objectives for Information Technology (COBIT5) guidance for configuration management (CM) explains that to mitigate the risk of uncontrolled changes, management should "manage all changes to the CM project and post implementation operational activities in a controlled manner. This mitigating action pertains to any change relating to business processes, applications and infrastructure. The "controlled manner" implies the following: • Using change standards and procedures • Performing an impact assessment • Prioritization and authorization • Tracking • Testing • Reporting • Closure • Documentation updates."

For the purposes of this review, we noted that many of the components occurred simultaneously for Harford County's changes, with the final Testing and Reporting steps being the most important components. We requested confirmation of change reviews (Testing and Reporting) from management, but emails were not available for our review. However, we found that Presidio maintains correspondence sent to and from Harford County. We were able to review the documentation maintained by Presidio, to determine that some changes were tested by ICT.

For 7 of 30 sampled network configuration changes, documentation was not available to confirm that the changes were approved by ICT prior to implementation or reviewed after implementation. In a number of cases, the confirmation of review was made by the Presidio representative after a phone call instead of a specific email confirmation. We also noted that Presidio implemented changes and closed the service tickets without confirmation from ICT, instead, they were closed based on the time lapsed without ICT reporting a problem.

In the event of a misconfiguration, management might need to review prior change testing documentation as part of its troubleshooting procedures. It is not clear that the testing occurred in each case.

Recommendation: We recommend ICT confirm, via email to Presidio, that all network configuration changes were correctly implemented.

Management Response: Every network change is requested and documented. An email is received for every ticket entered by Presidio and whenever a change ticket is resolved. Management will retain all emails sent to Presidio that document changes.

Expected Completion Date: All emails will be retained effective immediately.

MANAGEMENT RESPONSE

The Office of Information and Communication Technology has invested a considerable amount of resources over the past two years trying to mitigate the risk of exposure for the County for security breaches or system failures. The Office has adopted an overall Cybersecurity Plan and is currently working to implement the procedures outlined within that Plan.

BACKGROUND INFORMATION

PROGRAM DESCRIPTION AND KEY STATISTICS

Harford County has configured its information network across multiple sites and continues to update and expand the infrastructure. For all of the networking components, a vendor, Presidio Network Solutions, is responsible for remotely monitoring traffic and device events for unusual events. Once identified, those events are addressed by the vendor and reported to Harford County in real time. The vendor is also responsible for making changes to network configurations and reporting on network availability and event trends.

Harford County's Network Engineer manages the physical hardware on-site. In support of the services Presidio provides, Harford County is responsible for ensuring the list of monitored devices is up to date and ensuring that changes Presidio makes are correctly implemented. Quarterly, management meets with Presidio to review the services provided and discuss trends identified by Presidio.

REVIEW OBJECTIVE, SCOPE AND METHODOLOGY

The objective of this audit was to determine if the Department of Information and Communication Technology is properly monitoring the Network Management Services contract to ensure services were performed in accordance with the contract.

The audit focused on activity during the period of 7/1/2013 through 4/15/2015. Our audit procedures included interviewing personnel, observation and testing. Specifically, we tested identified incidents to ensure the County received prompt notification and that incidents were categorized properly for severity and priority. We tested a sample of network configuration changes to ensure they were properly reviewed. We reviewed a sample of IP addresses allowed to access the network to ensure they were justified. We compared the County's inventory of devices to the list of monitored devices (the RunBook) and antivirus software to determine that required items were included. We confirmed that Presidio can summarize the County's event history for at least 30 days, indicating that the vendor has the capability to maintain log files, as required by the contract. Management may want to consider if the data stored is adequate for its need. Finally, we reviewed documentation of quarterly business review (QBR) meetings and attended a QBR meeting.

This audit is considered a 'Performance Audit' because the procedures described above required the audit team to draw conclusions about conformance with contract terms and the adequacy of management's processes unrelated to specific financial transactions. Accordingly, to comply with §213(c) of the Harford County Charter, the audit was approved by the County Council in resolution 029-14.

Harford County management is responsible for establishing and maintaining effective internal controls. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets and compliance with applicable laws, rules and regulations are achieved. Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected.

The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Team:

Chrystal Brooks
CPA, CIA, CGAP, CISA, CGFM, CRMA
County Auditor

Laura Tucholski
CPA, CIA, CFE, CRMA
Managing Auditor