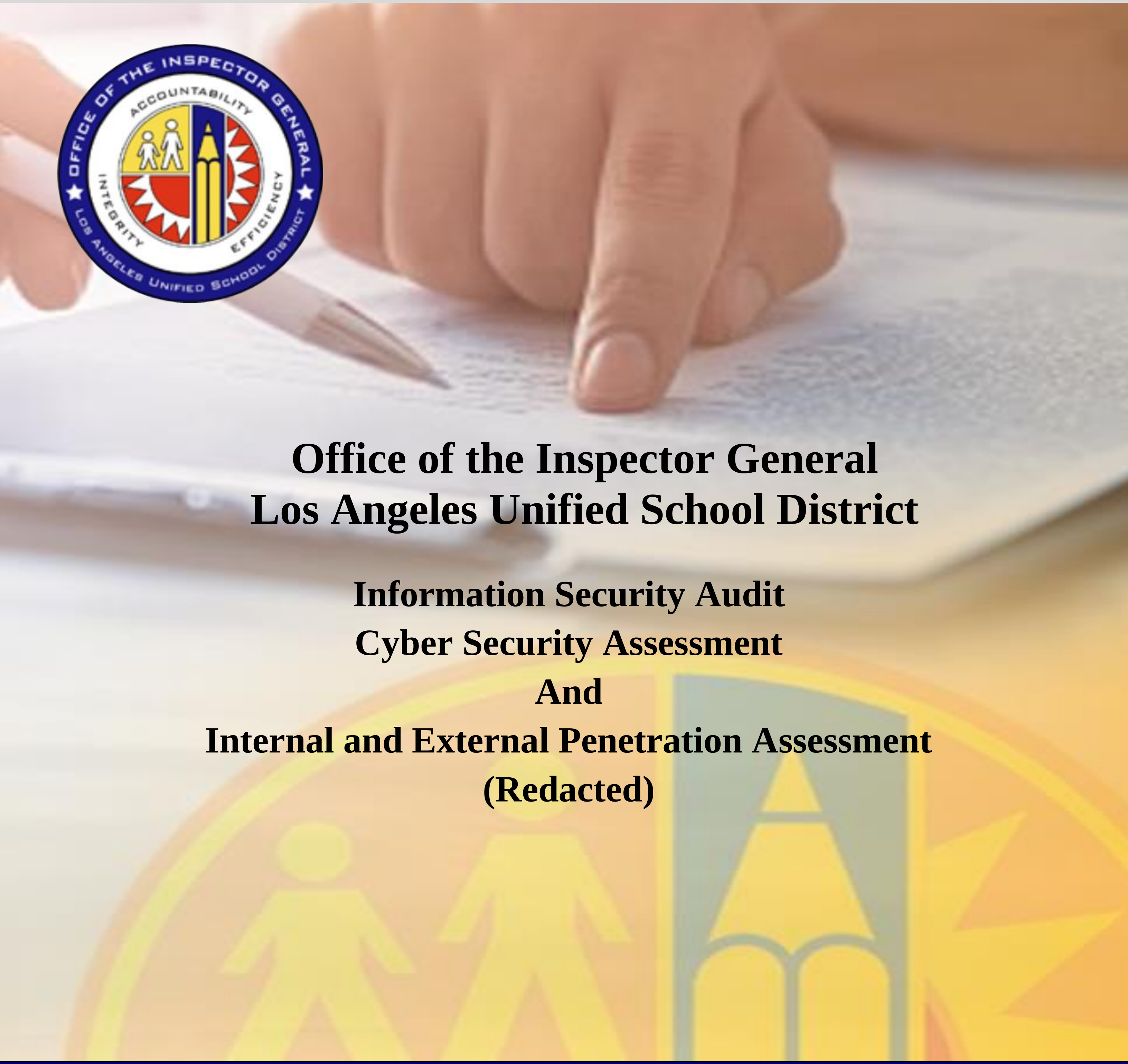


Office of the Inspector General
Los Angeles Unified School District

Information Security Audit
Cyber Security Assessment
And
Internal and External Penetration Assessment
(Redacted)

OA 20-1261-R **January 13, 2021**

Los Angeles Unified School District
Office of the Inspector General

Kelly Gonez, President
Dr. George J. McKenna III
Mónica García
Scott M. Schmerelson
Nick Melvoin
Jackie Goldberg
Tanya Ortiz Franklin
Members of the Board

Austin Beutner
Superintendent of Schools

William Stern
Inspector General

January 13, 2021

Soheil Katal, Chief Information Officer
Information Technology Division
Los Angeles Unified School District
333 S. Beaudry Avenue, 10th Floor
Los Angeles, CA 90017

RE: Information Security Audit

Dear Mr. Katal,

This is a redacted copy of our report on the Information Security Audit of the Los Angeles Unified School District (LAUSD) Information Technology Division (ITD). The audit consisted of a Cybersecurity Assessment to assess the controls over information security and Internal/ External Penetration Testing to assess the ability of the LAUSD network to resist attacks from internal threats and from outsiders able to gain access to the internal network and to resist attacks from the Internet and other external sources. The audit was conducted by Crowe, LLP a subject matter expert in Cybersecurity.

The report contains an abbreviated summary of the significant issues identified during the audit. Due to the sensitive nature of the findings from the audit, we have redacted the findings in the full report provided to ITD under a separate cover. The OIG has determined that it would be inappropriate to disclose the full report to the public. Publishing the full report on the Internet or providing full reports in sessions where they are exposed to public records requests would expose highly sensitive information that could be leveraged by attackers targeting the District. In some instances, threats on the internal network just need publicly available tools to exploit findings identified in audit reports, or the gaps that are actively being used by attackers in ransomware attacks. The full report can provide a blueprint on how to target the District with cybersecurity attacks.

While the OIG has a responsibility to make sure certain parties are informed of organizational risks, we balance this responsibility against the introduction of additional risk exposure through the disclosure of detailed reports.

We appreciate your continued support of our services.

Sincerely,

Austin E. Onwualu   William Stern

Austin Onwualu, CPA, CGMA, CIG
Deputy Inspector General, Audits

William Stern, MBA, CIG, CISM, CPP, CFE
Inspector General

C: Ms. Megan Reilly, Deputy Superintendent

Smart decisions. Lasting value.™

Los Angeles Unified School District

Performance Audit Report
Cybersecurity Assessment & Internal and External Penetration Assessment

September 2020

Cybersecurity Assessment

I. Executive Summary

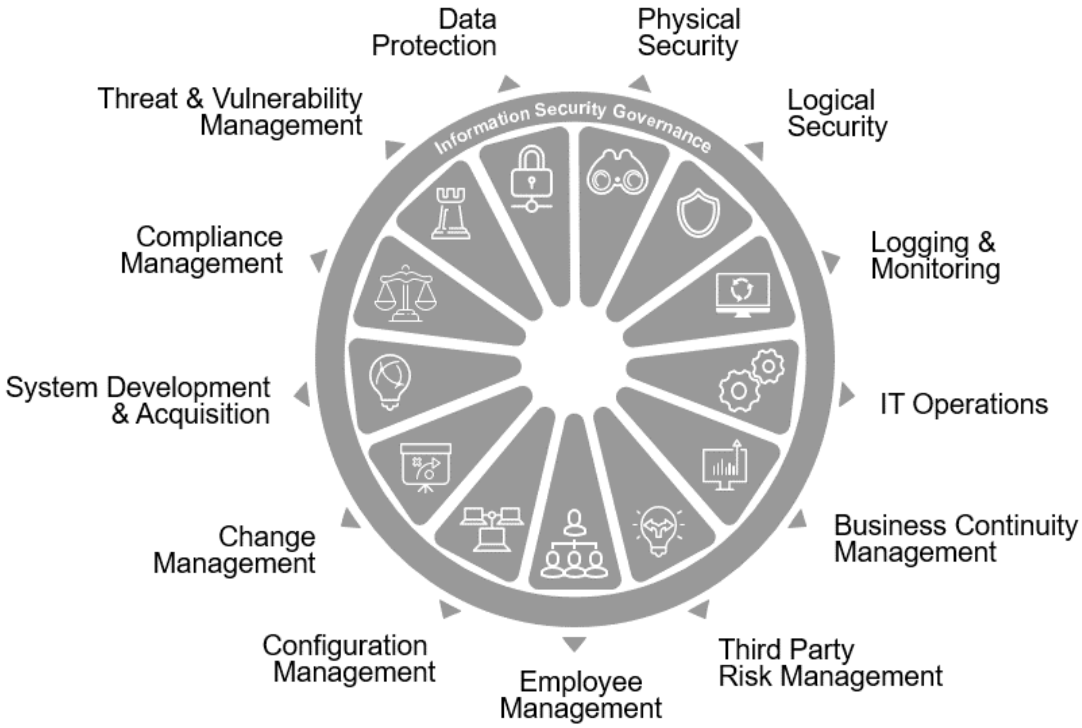
Crowe LLP (Crowe) performed an Information Security Audit of the Los Angeles Unified School District (LAUSD) Information Technology Division (ITD). The audit consisted of two primary procedures: A Cybersecurity Assessment and Internal/ External Penetration Testing. This section of the report includes the results of the Cybersecurity Assessment as of September 4, 2020.

Overview

Cybersecurity provides the assurance of the confidentiality, integrity, and availability of critical organizational assets. Crowe performed a comprehensive analysis of LAUSD by evaluating the people, processes, and technologies supporting the organization’s information security efforts.

The overall objective of the Information Security Audit was to assess the controls over information security by utilizing Crowe’s Integrated Cybersecurity Framework (CICF), which provides balanced IT security coverage including both information security governance components that support the overall program, as well as the technical implementation of the infrastructure, applications, and endpoints within the organization. The CICF includes standards from various cybersecurity standards, including NIST (SP 800-53, Cybersecurity Framework, etc.), ISO, and the CIS Top 20 Critical Security Controls, as well as various regulatory requirements.

The CICF consists of 13 domains segmented into control categories, which are mapped at the control level with various regulations and industry frameworks. These 13 domains are surrounded by a 14th domain, Information Security Governance.



© 2021 Crowe LLP

This report has been prepared by Crowe LLP in accordance with the terms of our engagement letter dated January 28, 2020. This report is furnished solely for the information and use of management, the Board of Education of Los Angeles Unified School District, and its regulatory agencies, and the report is not intended to be and should not be used by anyone other than these specified parties or entities.

Crowe conducted working sessions with LAUSD's personnel to better understand the current state of cybersecurity controls, reviewed selected policies and procedures, conducted selective testing, identified gaps against cybersecurity standards, and rated control gaps by severity of risk.

This report provides a summary of the assessment results including recommendations and proposed action plans to improve LAUSD's existing IT security controls and ultimately reduce cybersecurity risk.

Project Methodology & Approach

All controls were assessed by the IT Audit team based upon the scope approved by LAUSD, which covered the organizations information systems and several applications. The following steps represent the actions performed to deliver the assessment:

1. **Phase One – Project Planning and Kickoff**
   During Phase One, an information request list was submitted to gather existing policies and procedures. Additionally, a kickoff meeting was held to discuss the project timeline and expectations. Interviews were scheduled for information-gathering sessions with both business and IT management.

2. **Phase Two – Assessment**
   An assessment of information security controls was performed to obtain an understanding of the environment. Numerous interviews were conducted with Management from a cross-section of departments throughout the organization, as well as with IT subject matter experts. Crowe performed penetration testing and reviewed technical configuration of systems within the environment.

3. **Phase Three – Project Deliverables**
   Detailed results and accompanying recommendations from fieldwork are documented in a report including findings and associated recommendations.

Reporting Methodology

In this report, we provide a summary of our results and recommendations as well as management's responses. To assist you in analyzing our recommendations, we have provided our suggestions for corrective action based on the finding's exposure to loss or increased regulatory scrutiny, as follows:

High – Requires immediate remedy and, if left uncorrected, exposes LAUSD to significant or immediate risk of loss, asset misappropriation, data compromise or interruption, fines and penalties, or increased regulatory scrutiny.

Moderate – Requires timely remedy and, if left uncorrected, may expose LAUSD to risk of loss or misappropriation of company assets, compromise of data, fines and penalties, or increased regulatory scrutiny. These issues should be resolved in a timely manner, but after any high priority issues.

Low – Should be addressed as time and resources permit. While it is not considered to represent significant or immediate risk, repeated oversights without corrective action or compensating controls could lead to increased exposure or scrutiny.

This report has been prepared by Crowe LLP in accordance with the terms of our engagement letter dated January 28, 2020. This report is furnished solely for the information and use of management and the Board of Education of Los Angeles Unified School District, and the report is not intended to be and should not be used by anyone other than these specified parties or entities.

Ratings have also been assigned to the level of effort required to remediate the findings. Our assignments are subjective based on the current infrastructure at LAUSD and our experience with other clients.

High – This will take a substantial level of effort (3 Months to 1 year) and/or significant cost to remediate. Management should consider this a project to remediate.

Moderate – This will take a reasonable level of effort (1 to 3 Months) or a moderate investment to remediate.

Low – This will take a small level of effort (1 week to 1 Month) with a small investment or no cost to remediate.

This performance audit was conducted in accordance with the Generally Accepted Government Auditing Standards (GAGAS). Those standards required that the audit was planned and performed to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on audit objectives. The evidence obtained throughout the assessment provides a reasonable basis for the findings and conclusions here based on the audit objectives.

Background – Cybersecurity Assessment

The LAUSD network environment consists primarily of Windows and Linux servers, including both physical and virtualized systems. LAUSD utilizes a common anti-virus solution throughout the LAUSD environment on servers and workstations. Network security is provided via multiple, redundant firewalls with content filtering and intrusion detection system capabilities.

The main data center is located at the Beaudry facility while the backup site is located at the Van Nuys facility. The primary data center consists of an entire floor of the South Beaudry facility, while the Van Nuys facility is a modular Data Center that currently acts as a disaster recovery site.

Windows Server Update Services is leveraged to manage the distribution of updates and hotfixes to Windows devices in the environment. A configuration manager is utilized to configure the large number of Windows-based computers in the environment as well.

This is the first Information Security Audit performed for LAUSD by Crowe.

Summary of Results

The table below displays the number of recommendations identified through our procedures, categorized by priority.

Area of Assessment	High	Moderate	Low
Information Security Governance	2	-	1
Business Continuity Management	1	2	-

© 2021 Crowe LLP

This report has been prepared by Crowe LLP in accordance with the terms of our engagement letter dated January 28, 2020. This report is furnished solely for the information and use of management and the Board of Education of Los Angeles Unified School District, and the report is not intended to be and should not be used by anyone other than these specified parties or entities.

Threat & Vulnerability Management	1	1	-
Logical Security	1	-	-
Data Protection	-	1	-
Employee Management	-	-	-
Third Party Risk Management	-	1	-
Logging & Monitoring	-	-	1
Physical Security	-	-	1
System Development & Acquisition	-	-	-
IT Operations	-	-	-
Change Management	-	-	-
Compliance Management	-	-	-
Configuration Management	-	-	-
Total	**5**	**5**	**3**

Detailed observations and recommendations are provided in Section II – Detailed Results and Remediation Plans in the unredacted report. The most significant issues identified during our assessment include the following:

- **IT Risk Governance** – While ITD has a security function who defines policy for the organization, they currently do not have a process in place to validate control compliance across the District for those systems that ITD does not directly supervise or operate. LAUSD has not implemented an IT Risk Assessment process in order to validate the organization's compliance with information security standards and directives that have been disseminated by the IT Division's security team. By not verifying compliance with ITD security standards and policies, the organization may not be able to identify areas of high risk and take the appropriate steps to prioritize and implement the appropriate mitigating controls. ITD is currently working to hire an IT Security Risk manager who will have the primary responsibility of performing IT Risk Assessments, correlating results, developing remediation plans with recommendations and expected costs/benefits.
- **Incident Response Training** – Crowe identified that the LAUSD does not currently provide incident response training to employees who would typically be involved with the incident response process, such as information system administrators and ITD security personnel. Without incident response training exercises, LAUSD personnel may be unaware of their roles and responsibilities, or gaps in the incident response plan may go unnoticed due to a lack of visibility. LAUSD should develop simulated and tabletop incident response security training exercises designed to walk employees through various categories of incidents (minor, moderate, and major incidents) to test their responsiveness, understanding of incident reporting processes, and ensuring they understand the appropriate steps to take to minimize the impact to the organization.

© 2021 Crowe LLP

- **Internal Penetration Testing** – LAUSD has not conducted an internal penetration assessment in the last year. By not conducting internal penetration assessments, the organization may be unaware of vulnerabilities and gaps in control implementations that malicious parties could use to compromise the internal network. LAUSD should seek to contract with an independent third party to perform internal penetration testing (not just vulnerability scanning) on an annual basis. The organization should also consider annual testing or whenever significant network changes occur, such as the implementation of new endpoint protection technologies or architectural changes to the network.
- **Account Management** – Certain classes of accounts were found to be deficient in their logical access controls.

In addition to the items summarized here, other items are also documented in later sections of the unredacted report. These items are issues that do not represent significant risk at this time but offer opportunities for LAUSD to further strengthen controls and processes.

Information security is an ongoing process and Information Security Audits cannot guarantee the security of a network. Since new vulnerabilities are discovered daily, LAUSD should continue with ongoing security assessments.

II. Summary of Scope

The scope of procedures, which was developed using industry Cybersecurity guidance, included inquiry and/or testing in the following activities and processes:

The scope of procedures, which was developed using industry Cybersecurity guidance, included inquiry and/or testing in the following activities and processes:

Cybersecurity Governance Review

Information Security Governance
- Information Security Program
- Roles & Responsibilities
- Oversight & Strategy
- IT Risk Management

Data Protection
- Data Management (Handling & Classification)
- Data Inventory
- Data Protection Controls
- Data Sanitization & Destruction
- Encryption

Threat & Vulnerability Management
- Malicious Code Detection
- Patch Management
- Threat Intelligence
- Vulnerability Management

Physical Security
- Physical Information Security
- Data Center Security
- Physical Access
- Physical Monitoring & Detection
- Physical Audit Log & Review
- Clean Desk

Logical Security
- Identification & Access Control
- Authentication
- Access Management
- Access Reviews

Logging & Monitoring
- Audit & Logging Management
- Audit Configuration
- Audit Log Aggregation
- Audit Monitoring & Detection
- Audit Alerting
- Audit Log Review

© 2021 Crowe LLP

IT Operations

- Asset Management
- Asset Lifecycle

Business Continuity Management

- Business Impact Assessment
- Business Continuity & Contingency Planning
- IT Resiliency & Backup Processes
- Disaster Recovery Planning
- Incident Response Procedures

Third Party Risk Management

- Third Party Security Oversight
- Third Party Inventory
- Third Party Network Access
- Third Party Contracts
- Third Party Due Diligence

Employee Management

- Employee Standards
- Hiring Practices
- Job Transition Practices
- Termination Practices
- Security Training

Configuration Management

- Approved Infrastructure
- Standard Build Procedures
- Configuration Certification

Change Management

- Change Control
- Maintenance

System Development & Acquisition

- Development & Acquisition Standards
- Project Management (System Security Plans)

Compliance

- Compliance & Regulatory Standards

The specific procedures performed were based on the concepts of selective testing. Although Crowe's testing was performed in some areas without exception, Crowe can provide no assurance that exceptions would not have been detected had procedures been changed or expanded.

Information technology assessments are an ongoing process. An Information Security Audit does not guarantee the proper functioning of controls reviewed or security of a network or systems assessed or physical security or prevention of fraud or privacy of data or compliance with banking regulations. The nature, timing, and extent of the procedures performed were based on the concepts of selective testing. This report presents findings and recommendations resulting from the performance of these procedures. Although our testing was performed in some areas without exception, we can provide no assurance that exceptions would not have been detected had procedures been changed or expanded. While we rate our findings, we encourage management to consider addressing all findings as all findings (regardless of rating) over time may pose risk to the District's security and controls.

It should also be recognized that internal controls are designed to provide reasonable, but not absolute, assurance that errors and irregularities will not occur, and that procedures are performed in accordance with management's intentions. There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal controls. In the performance of most control procedures, errors can result from misunderstanding of instructions, mistakes in judgment, carelessness, or other factors. Internal control procedures can be circumvented intentionally by management with respect to the execution and recording of transactions, or with respect to the estimates and judgments required in the processing of data. Controls may become ineffective due to newly identified business or technology exposures. Further, the projection of any evaluation of internal control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, and that the degree of compliance with procedures may deteriorate.

© 2021 Crowe LLP

This report has been prepared by Crowe LLP in accordance with the terms of our engagement letter dated January 28, 2020. This report is furnished solely for the information and use of management and the Board of Education of Los Angeles Unified School District, and the report is not intended to be and should not be used by anyone other than these specified parties or entities.

Internal and External Penetration Assessment

I. Executive Summary

Crowe LLP (Crowe) performed an Information Security Audit of the Los Angeles Unified School District (LAUSD) Information Technology Division (ITD). The audit consisted of two primary procedures: A Cybersecurity Assessment and Internal/ External Penetration Testing. This section of the report includes the results of the Internal and External Penetration testing as of September 16, 2020.

Overview

The penetration testing activities were comprised of two components, which included an Internal and External Penetration Assessment.

- *Internal Penetration Assessment*: The overall objective was to assess the ability of the LAUSD network to resist attacks from internal threats and from outsiders able to gain access to the internal network. Crowe identified LAUSD systems and services that were accessible on the LAUSD internal network. Crowe then attempted to identify and verify vulnerabilities that could allow an attacker to gain elevated access to the LAUSD network or to gain access to sensitive information.

- *External Penetration Assessment*: The overall objective was to assess the ability of the LAUSD network to resist attacks from the Internet and other external sources. Crowe identified LAUSD devices and services that were accessible from outside the LAUSD network. Crowe then attempted to identify and verify vulnerabilities that could allow an attacker to gain access to the LAUSD network or to gain access to sensitive information.

LAUSD's Information Technology Security staff detected some of Crowe's activities during the technical portion of the assessment. LAUSD did not block Crowe's network access in order to allow Crowe to fully identify vulnerabilities that may be present.

Background

Internal Network Environment
An assessment of the LAUSD internal network address ranges identified around eighty-nine thousand (89,005) targets with a total of approximately three hundred thousand (259,220) services, including around eighty-five thousand (85,241) web services, around two hundred database services (195) and about fifty seven thousand (57,765) other services. Furthermore, there are about one hundred thousand (116,219) miscellaneous services including, but not limited to SSH, POP3 and NTP. LAUSD hosts all these devices and Crowe targeted them during the assessment. However, it is important to note that the internal LAUSD network is segmented and that the internal assessment was performed from the standpoint of an unauthenticated user connected to a restricted network segment. From this standpoint, the major applications hosted in the data center were determined to be properly segmented from the basic user network segment.

Externally Exposed Services
An assessment of the LAUSD Internet address ranges identified forty-six (46) targets with a total of one hundred and nine (109) services, including seventy-seven (77) web services and eight (8) voice over IP services. Additionally, there are twenty-four (24) miscellaneous services. LAUSD hosts all these devices and Crowe targeted them during the assessment.

© 2021 Crowe LLP

This report has been prepared by Crowe LLP in accordance with the terms of our engagement letter dated January 28, 2020. This report is furnished solely for the information and use of management and the Board of Education of Los Angeles Unified School District, and the report is not intended to be and should not be used by anyone other than these specified parties or entities.

This is the first Internal and External Penetration Assessment Crowe has performed for LAUSD.

Summary of Results

The table below displays the number of recommendations identified through our procedures.

Area of Assessment	High	Moderate	Low
Internal Penetration			
Windows and Active Directory System Security	1	4	-
Network Architecture and Infrastructure Management	-	-	-
Patch Management	1	1	-
Database Security	-	-	-
Email Architecture Security	1	-	-
Unix and Linux System Security	-	-	-
Web Application Security	1	1	4
Printers and Multi-function Devices	1	-	2
Data Storage and Access Controls	1	2	
External Penetration			
Security Awareness	1	-	-
Windows and AD System Security	-	-	-
Unix and Linux System Security	-	-	-
Database Security	-	-	-
Web Application Security	-	-	1
Email Architecture Security	-	-	-
Network Architecture and Infrastructure Management	-	-	2
Data Storage and Access Controls	-	-	-
Patch Management		1	
Total	**7**	**9**	**9**

Detailed observations and recommendations are provided in Section II – Detailed Results and Remediation Plans in the unredacted report.

During the engagement, Crowe identified the following controls that were successfully mitigating information security risks for the District:

- **Network Segmentation** – During the assessment, Crowe was connected to the same network segment as a basic user. Crowe attempted to access critical District applications but found that network segmentation restricted access from the user segment. This segmentation helps manage risk by reducing the likelihood that a threat originating on the user network would successfully be able to access critical District applications.

© 2021 Crowe LLP

- **Network Scanning Detection** – Throughout the assessment IT received multiple alerts and notifications pertaining to scanning that the audit team performed. In order to complete testing efficiently, Crowe leveraged tools and scanning approaches that generated more traffic and increased the likelihood of detection. It is important to note that in a real attack scenario, an attacker would move slower, generate less traffic, and be stealthier, which could make it more difficult to detect.

The most significant risks identified during our assessment include risks identified in Password Controls, Malicious Activity Detection and Alerting, Windows Security Patching, Guessable SQL Credentials, Internal Email Spoofing, Email Social Engineering and Anonymous Access to File Server.

In addition to the items summarized here, other items are also documented in later sections of the unredacted report. These items are issues that do not represent significant risk at this time but offer opportunities for LAUSD to further strengthen controls and processes.

Information security is an ongoing process and Internal and External Penetration Assessments cannot guarantee the security of a network. Since new vulnerabilities are discovered daily, LAUSD should continue with ongoing security assessments.

Crowe would like to thank LAUSD for this opportunity to report the results of this assessment and to thank LAUSD's personnel for their cooperation and assistance.

II. Summary of Scope

Crowe followed a structured assessment process to evaluate the security of the LAUSD internal & external network. The Crowe assessment team divided this process into the following phases:

IIa. Internal Penetration Assessment

Phase 1: Internal Network Target Identification

- Passively monitor network traffic to identify active systems and subnets on the network.
- Perform ICMP scans to identify active systems and subnets on the network.
- Query internal DNS servers to identify IP addresses.
- Perform TCP and UDP port scans to identify available services on the LAUSD network.

Phase 2: Internal Network Security Assessment

- Probe identified services to determine target configuration and vulnerabilities.
- Verify all identified potential vulnerabilities.
- Attempt to gain access to LAUSD systems and sensitive information by exploiting vulnerabilities.

For the identification and assessment of targets on the internal network, Crowe was provided with access to the internal network but was not provided by LAUSD with valid credentials or with other access to LAUSD systems.

Crowe worked with LAUSD to identify a sample of the internal subnets that would be representative of the entire network. Crowe used the list of sampled subnets as the basis for the technical assessment. Port scans and other scans were performed on these entire subnets and not merely on the active hosts identified by ICMP scanning and other measures.

IIb. External Penetration Assessment

Phase 1: Target Identification

- Perform Internet searches and search registration data to identify domains and Internet Protocol (IP) address ranges associated with LAUSD.
- Query domain name servers to identify additional IP addresses.
- Scan LAUSD-related IP address ranges to identify potential targets.
- Attempt to gather employee names and contact information from public sources.

Phase 2: Internet Target Security Assessment

- Probe identified services to determine target configuration and vulnerabilities.
- Verify all identified potential vulnerabilities
- Attempt to gain access to LAUSD network and sensitive information by exploiting vulnerabilities.

Phase 3: Security Awareness Assessment

- Attempt to obtain sensitive information through persuading users to execute malicious programs sent via email.
- Attempt to gain further access to the LAUSD network and sensitive information using information obtained from social engineering.

For the identification and assessment of targets on the external network, LAUSD did not provide Crowe with valid credentials or with other access to LAUSD systems.

III. Findings

This audit resulted in 38 Cyber Security findings that have been relayed in detail via our full Confidential Audit report to the Chief Information Officer of LAUSD. Those findings included some significant risks around passwords and credentials. Auditors were able to use social engineering to obtain LAUSD employee passwords and were further able to convince employees to unknowingly execute malicious codes. Auditors were able to gain access to certain sensitive information including a limited number of Social Security Numbers (SSNs).

IV. Recommendations

We made 38 Cyber Security recommendations that have been relayed in detail via our full Confidential Audit report to the Chief Information Officer of LAUSD. The Information Technology Division (ITD) agreed with all the recommendations and provided proposed mitigation plans to change or improve the control deficiencies and vulnerabilities identified in the audit and add specific IT Security personnel. Since the issuance of the draft report to ITD, action has been taken to address some of the vulnerabilities identified in the report.

.

V. IT Audit Team

The following personnel assisted the Crowe IT Audit Team in completing the LAUSD Cybersecurity Assessment and Penetration testing activities.

Name	Title	Organization
Katharine Monishi	Audit Manager	Office of the Inspector General (LAUSD)
Tony Li, CISA	Sr. Auditor	Office of the Inspector General (LAUSD)

© 2021 Crowe LLP

This report has been prepared by Crowe LLP in accordance with the terms of our engagement letter dated January 28, 2020. This report is furnished solely for the information and use of management and the Board of Education of Los Angeles Unified School District, and the report is not intended to be and should not be used by anyone other than these specified parties or entities.

Know about fraud, waste or abuse?

Tell us about it.

Maybe you are a school district employee, a parent or just a concerned citizen. Regardless, you can make a difference!

Maybe you know something about fraud, waste, or some other type of abuse in the school district.

The Office of the Inspector General has a hotline for you to call. You can also email or write to us.

If you wish, we will keep your identity confidential. You can remain anonymous, if you prefer. And you are protected by law from reprisal by your employer.

Whistleblower Protection

The Board approved the Whistleblower Protection Policy on February 12, 2002. This policy protects LAUSD employees who make allegations of improper governmental activity from retaliation or reprisal. To assure the reporting of any activity that threatens the efficient administration of the LAUSD, reports that disclose improper governmental activities shall be kept confidential.

General Contact Information

Office of the Inspector General
333 S. Beaudry Avenue, 12th Floor
Los Angeles, CA 90017
Phone: (213) 241-7700
Fax: (213) 241-6826
https://achieve.lausd.net/oig

Fraud, Waste and Abuse Hotline

(866) 528-7364 or (213) 241-7778
inspector.general@lausd.net