Data Loss Prevention:
City's approach is sound but its practices should be strengthened

Audit Report – October 2018

Overall the City of Portland's approach to data loss prevention is sound, and the City is taking appropriate steps to manage and protect data it uses.

The audit did, however, identify some vulnerabilities and recommend actions the City can take to strengthen its data security program. Continued progress will help decrease the risk of data loss.

Why is data loss prevention important?

Data loss prevention is the practice of detecting and preventing unauthorized transmittal of sensitive or confidential information outside of an organization.

Data loss may occur physically or electronically and may be intentional or unintentional.

Recent headlines have profiled examples of data loss incidents that cost other organizations millions of dollars; and perhaps more important, these events increased the risk of identity theft for the people whose personal data was compromised, and the risk of financial loss and reputational damage to the organization.

Is the City protecting the data it uses?

The audit found the City's overall data loss prevention system was adequately designed and carried out with some exceptions. It identified weaknesses during assessments of the Bureaus of Technology Services and Human Resources and the City Archives and Records Management. The findings occurred in the areas of identifying and protecting data and detecting intrusions, such as:

- *Vulnerability scans* of City information systems were not performed completely and consistently;
- *Access controls,* such as password rules and authorizations to view data, were not followed in limited circumstances;
- *Policies and procedures* were out of date and did not align with the national cybersecurity framework the City follows.

Resolving those vulnerabilities will reduce the risk of data losses and move the City toward full implementation of the National Institute of Standards and Technology Cybersecurity Framework. The City's Technology Services follows this voluntary framework. It provides standards and guidelines to manage cybersecurity-related risk in the areas of identifying and protecting data, and detecting, responding to, and recovering from any data breaches.

What happens next?

We provided audit results to the Bureaus of Technology Services and Human Resources, and Archives and Records Management in separate reports. They include sensitive information about potential computer or system weaknesses, which are exempt in state law from public disclosure. The reports include in total 27 recommendations to strengthen the City's data loss prevention practices. Bureau managers provided responses to the detailed reports and generally committed to implementing the recommendations. We will follow up in one year to confirm that these improvements were made.

PORTLAND CITY AUDITOR
Audit Services

503.823.4005 | www.portlandoregon.gov/auditservices

What was the purpose of the audit?

The purpose was to assess if the Bureau of Technology Services' approach to data loss prevention was well-designed and implemented effectively. Testing centered on practices used by Human Resources to manage and protect data it uses, including data on paper, electronic and removable media.

The scope included the City's electronic network and financial system; specialized information technology systems and applications used, managed, or owned by Human Resources; and the City's electronic records system, which is managed by Archives and Records Management.

This audit was performed on behalf of the City Auditor by independent technical experts, Myers and Stauffer, under a contract managed by the Audit Services Division.

What were the audit steps?

- Reviewed access controls such as password settings and system lockout settings
- Reviewed processes and procedures for monitoring and logging access to systems
- Performed after-hours office walk through of Human Resources' offices to determine if systems, electronic media, and hardcopy records were properly secured
- Observed physical security controls for facilities used by the Bureaus being audited
- Observed tests designed to prevent and/or detect data loss
- Performed tests of samples of user accounts to determine whether system access and permissions were appropriately authorized
- Assessed controls for system authentication and authorization of access and access privileges
- Reviewed City policies and procedures for information technology security and data identification, and roles and responsibilities related to data loss prevention
- Interviewed management and staff at Technology Services, Human Resources, and Archives and Records Management
- Reviewed processes and procedures for identifying, marking, handling, securing, transporting, and securely disposing of electronic and hard copy media
- Assessed employee training on security and protection of restricted and confidential data and testing to determine whether training is provided consistently to all relevant staff

Archives and Records Management, which is a division of the Auditor's Office, was part of the scope of the audit because of its responsibility for the City's electronic records management system. Audit Services took steps to ensure that any potential threats to the independence of the audit were mitigated. For example, the Auditor had no contact with the consultants, and the City Archivist's response to the audit was delivered to Audit Services instead of the City Auditor.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate 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.

PORTLAND CITY AUDITOR
Audit Services