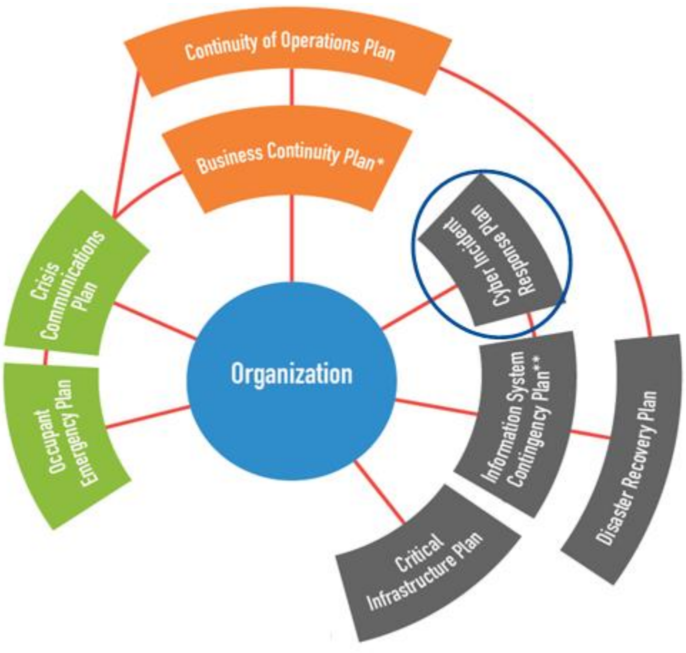
PERFORMANCE AUDIT – February 27, 2024

Information Technology Division Cyber Incident Response Plans

What We Found

The National Institute of Standards and Technology (NIST) defines a number of continuity and contingency plans. NIST identifies Cyber Incident Response Plans as a separate, discrete type of plan whose primary focus is identifying, responding to, and recovering from computer security incidents or events.



Continuity of Operations Plan
Business Continuity Plan*
Crisis Communications Plan
Cyber Incident Response Plan
Organization
Occupant Emergency Plan
Information System Contingency Plan**
Disaster Recovery Plan
Critical Infrastructure Plan

We identified 29 NIST recommended practices for Cyber Incident Response Plans and compared those practices to the Information Technology Division's current Cyber Incident Response Plans. These recommended practices fall into four areas:

- Plan Governance
- Plan Development
- Training and Testing
- Response and Recovery

What We Recommend

We identified areas for improvement and provided management in the Information Technology Division with our analysis and recommendations.

Management agreed with our recommendations.

Closed Record

We are not publicly disclosing the details of this audit due to the subject matter and security concerns. The full audit report is a closed record under RSMo §610.021(21).

Why We Did This Audit

Cyberattacks are widely recognized as one of the highest risks facing organizations. To mitigate risk, organizations develop various types of contingency and action plans to follow during and while recovering from an emergency or incident. Generally, emergencies and incidents can vary from natural disasters, such as a tornado, to cyberattacks such as ransomware, to the unforeseen.

The average total cost of a cybersecurity breach in the United States is over $9 million. An effective Cyber Incident Response Plan is also one of the most effective methods to reduce costs when a breach occurs.

Organizations with data breaches that had high levels of incident response planning saved $1.5 million compared to those with low levels of planning.

Objective

Do the Information Technology Division's Cyber Incident Response Plans incorporate cybersecurity recommended practices?

Background

The city's Information Technology Division, a division of the General Services Department, is responsible for responding to cyber incidents.

Cyber Incident Response Plans can help the city mitigate or reduce damages from cyber incidents.

KANSAS CITY
MISSOURI

Office of the City Auditor
Douglas Jones, CGAP, CIA, CRMA – City Auditor
21st Floor, City Hall, 414 E. 12th St.
Kansas City, Missouri 64106

816-513-3300
cityauditor@kcmo.org
@KCMOCityAuditor
KCMO.GOV/CITYAUDITOR