



Maricopa County

Internal Audit Department

301 W Jefferson St
Suite 660, Phx, AZ
85003-2148
602-506-1585
maricopa.gov/
internalaudit/

To: Maricopa County Board of Supervisors

From: Ross L. Tate, County Auditor

Subject: Cybersecurity Assessment

Date: July 14, 2016

We have completed our FY 2016 Cybersecurity Assessment, which was performed in collaboration with the Office of Enterprise Technology (OET), with assistance from KPMG, LLP. This assessment was performed in accordance with the annual audit plan approved by the Board of Supervisors.

Our primary objective was to compare OET's Cybersecurity program and practices against industry recommended practices. To achieve our objective, we performed a Cybersecurity Capability Maturity Model assessment.¹

We found that OET's Cybersecurity program is aligned with industry recommended practices. Specifically, we noted that OET maintains mature capabilities in:

- Strategic planning and development, which has led to a comprehensive cybersecurity roadmap.
- Cybersecurity incident prevention and detection processes, which has led to the identification and remediation of significant threats to the County's infrastructure.
- Identification, prioritization, and communication of cybersecurity risks to County agencies, which has led to increased awareness around the subject of cybersecurity.

The assessment also revealed some process gaps, which are aligned to activities that OET is already in the process of executing, as summarized below.

- Finalizing draft cybersecurity policies for countywide adoption.
- Implementing the Governance, Risk, and Compliance (GRC) program and delivering security risk information to affected agencies.
- Completing the Service Management System project to enhance OET's asset management capabilities.

¹ The Cybersecurity Capability Maturity Model was developed by the United States Department of Energy in partnership with the U.S. Department of Homeland Security and is aligned with the Federal Cyberspace Policy Review.

A detailed report of findings and recommendations was issued to OET. Below we provide information describing why cybersecurity is important to the County, and an overview of our assessment results. For security purposes, this memo is restricted to high-level conclusions of the assessment.

Cybersecurity Background

Cybersecurity measures are implemented to protect information systems from unauthorized access, modification, and disruption. The practice of cybersecurity can be an overwhelming endeavor. Protecting all information technology assets equally is costly and ineffective.

In order to prioritize information technology assets, the U.S. Department of Homeland Security organized the country's vital interests into 16 critical infrastructure sectors. Each sector is considered so important that its incapacitation would have a debilitating effect on national security, the economy, and/or on national public health. The County operates, supports, or regulates 10 of the 16 infrastructures, as shown below.



Communication Facilities

Communication services are interconnected by satellite, wireless, and wireline providers who share facilities and technology to ensure interoperability. County first responders are highly dependent on reliable communication facilities.



Dams

The County services 22 dams that deliver critical water retention and control services. County dams are operated using systems that monitor potential flooding conditions.



Emergency Services

The Emergency Services Sector is the first line of defense in the prevention and mitigation of disasters. County emergency services agencies include Emergency Management, Sheriff's Office, Public Health, Public Works, and Flood Control.



Financial Services

The Financial Services Sector is frequently targeted for cyber-attacks. The County Treasurer manages County investments and banking services using sophisticated information technology systems throughout its operation.



Food & Agriculture

The Food and Agriculture Sector includes farms, restaurants, food manufacturing, and storage facilities. The County's Environmental Services oversees food safety using business applications that are integrated into its core processes.



Government Facilities

While most County facilities are public buildings; others are restricted. County facilities include courthouses, laboratories, structures that house critical systems, and the employees that operate them.



Health Care & Public Health Care

The Health Care and Public Health Care Sectors guard against terrorism, infectious disease outbreaks, and natural disasters. The County Department of Public Health uses numerous applications to keep County residents safe.



Information Technology

Well-executed controls over implementing, maintaining, and replacing County-owned information technology systems are vital to the safety of all other County-run, critical infrastructures.



Transportation Systems

County-maintained roads are critical to supporting national security and economic well-being. The County's Department of Transportation uses extensive systems to monitor safety requirements and road maintenance.



Water & Wastewater Systems

Attacks to the Water and Wastewater Systems Sector could result in illnesses and/or a denial of service. The County's Environmental Services Department regulates water and solid waste treatment using core business applications.

Cyber-Attack Methods & Damages

Some of the most common and successful cyber-attacks include:

- Exploiting identified system and web application vulnerabilities.
- Phishing emails luring victims to open malicious attachments.
- Stealing user IDs and passwords to gain unauthorized access to information systems.
- Denial-of-service attacks designed to interrupt online services.

These cyber-attacks can create significant reputational and financial damage. During 2015, data breaches cost organizations an average of \$217 per compromised record, including millions of dollars in technology costs and legal fees.²

To combat the risks associated with cyber-attacks, OET established a Maricopa County Cybersecurity Strategy using a Capability Maturity Model based on recommended practices identified by the National Institute of Standards and Technology (NIST). These efforts have led to a systemic and sustainable cybersecurity lifecycle that identifies, manages, and mitigates the risk of cybersecurity threats.

The program also provides leadership with a method to measure the effectiveness of investments made in cybersecurity. Furthermore, leadership is able to make high-level, risk-based decisions; and, as a result, the County has been able to make improvements to its cybersecurity portfolio.

Recent investments include increasing the number of cybersecurity personnel, implementing preventative security controls, improving IT processes and procedures, and providing security awareness to staff.

Assessment Results

We assessed OET's cybersecurity maturity within each of 10 domains.

- Risk Management
- Asset, Change, and Configuration Management
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Information Sharing and Communications
- Event and Incident Response; Continuity of Operations
- Supply Chain and External Dependencies Management

² 2015 Cost of Data Breach Study: United States, Ponemon Institute,
<http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF>

Cybersecurity Assessment

July 14, 2016

Page 5 of 5

- Workforce Management
- Cybersecurity Program Management

Within each area, we interviewed OET personnel, inspected documentation and system reports, and assigned a corresponding maturity rating. In addition, OET's desired maturity rating was determined and a plan was developed to reach the desired state. Overall, we found that OET's Information Security program is on track to meet its cybersecurity performance goals in accordance with OET's approved strategic plan.

This engagement was approved by the Board of Supervisors and was conducted in conformance with International Standards for the Professional Practice of Internal Auditing.

If you have any questions or wish to discuss items presented in this report, please contact Patra Carroll, IT Audit Supervisor, at 602-506-0345.