LEGISLATIVE BUDGET BOARD

Overview of State Agency Cybersecurity Costs

PRESENTED TO SENATE SELECT COMMITTEE ON CYBERSECURITY

LEGISLATIVE BUDGET BOARD STAFF **MARCH 21, 2018**

Department of Information Resources

The Texas Department of Information Resources (DIR) provides statewide leadership and oversight for management of government information and communications technology as well as cybersecurity controls.

> *The overall mission is to provide technology leadership, solutions, and value to Texas state government, education, and local government entities to enable and facilitate the fulfillment of their core missions. They facilitate and support government use of information and communications technology — everything from computers, Internet service, data storage, online applications, and much more — so that health, education, transportation, and other services are delivered to the citizens and businesses of Texas efficiently, economically, and innovatively.*

State Cybersecurity Controls

In order for State agencies to have a strategic roadmap for success, the DIR created the Texas Cybersecurity Strategic Plan for Fiscal Years 2018-2023 which states:

> *“In 2018, the Department of Information Resources Office of the Chief Information Security Officer worked with the Statewide Information Security Advisory Committee to create a statewide strategic plan that focuses on cybersecurity initiatives. The mission of the Texas Cybersecurity Strategic Plan is to assist public sector security personnel in improving their organization’s cybersecurity effectiveness through alignment with statewide goals. Although many organizations are mature in their cybersecurity efforts, continuous improvement is an important component of an effective cybersecurity program.”*

State Cybersecurity Controls

For FY 2018-19, DIR was appropriated $21.5 million in All Funds to provide security policy, assurance, education, and awareness; and assist state entities in identifying security vulnerabilities.

Additionally, DIR:

- Provides a monthly online Cybersecurity Newsletter;
- Hosts the Information Security Forum; and
- Establishes policy and governance security standards for agencies and institutions of higher education; which are closely aligned with the Federal Information Security Management Act.

Cybersecurity in the State Budget

Cybersecurity costs are embedded in various components of the budget, including:

- State Agency Staff (FTEs)
- Data Center Services (DCS)
- Centralized Accounting and Payroll/Personnel System (CAPPS)
- Capital Budgets
- Ongoing Maintenance (Daily Operations)
- Major Information Resources Projects

State Agency Cybersecurity Staff

The SAO’s classification schedule for FY 2018 lists the State's compensation and classification system, and provides information on employee salaries.

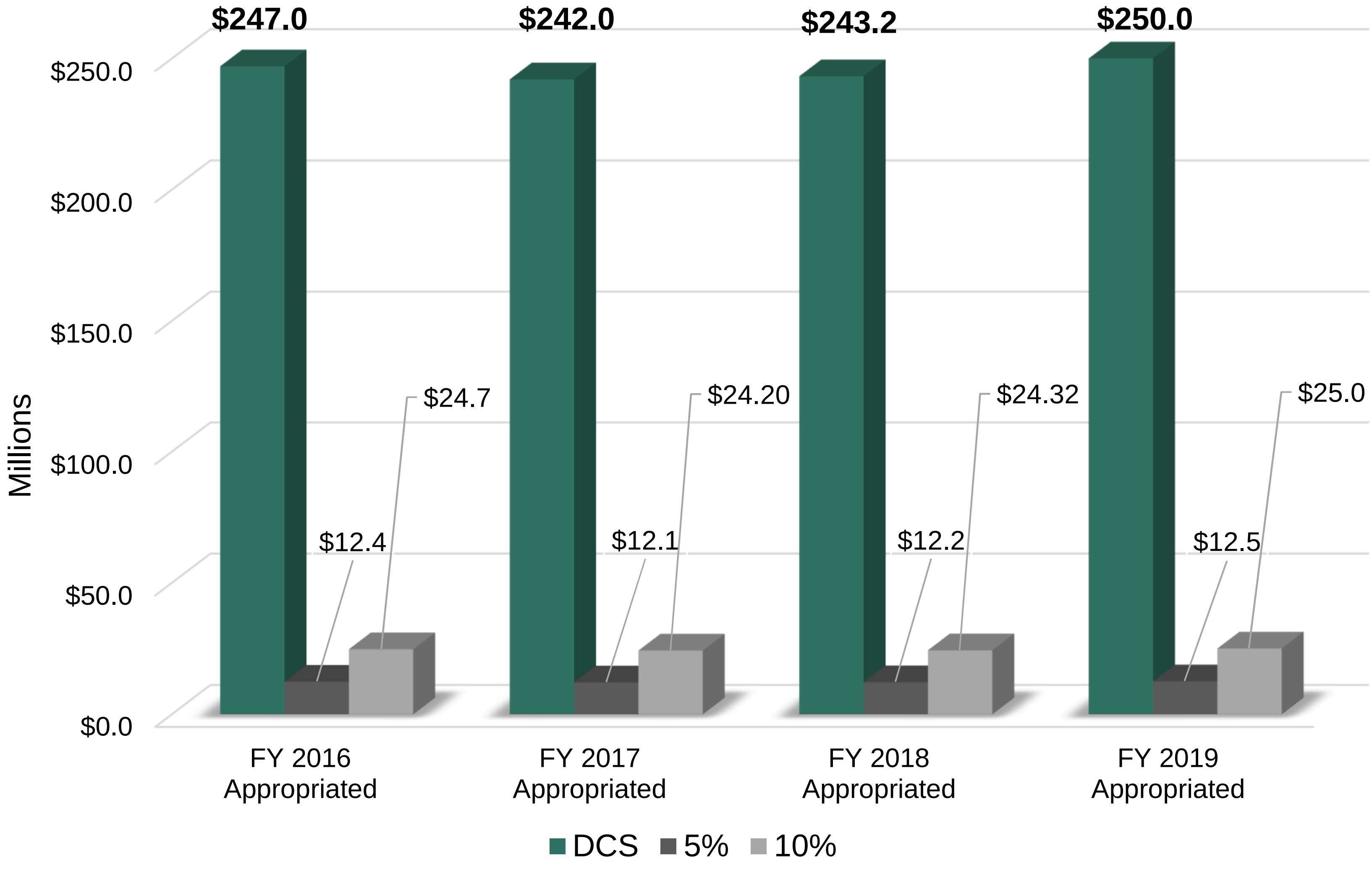
$8.0 million is expended annually on 180 agency employees whose responsibilities are primarily related to cybersecurity. These include, but are not limited to:

- Chief Information Security Officer
- Chief Cybersecurity Officer
- Cybersecurity Analyst (I – III)
- Cybersecurity Officer
- Information Security Officer
- Information Technology Auditor (I – IV) and
- Information Technology Security Analyst (I – III)

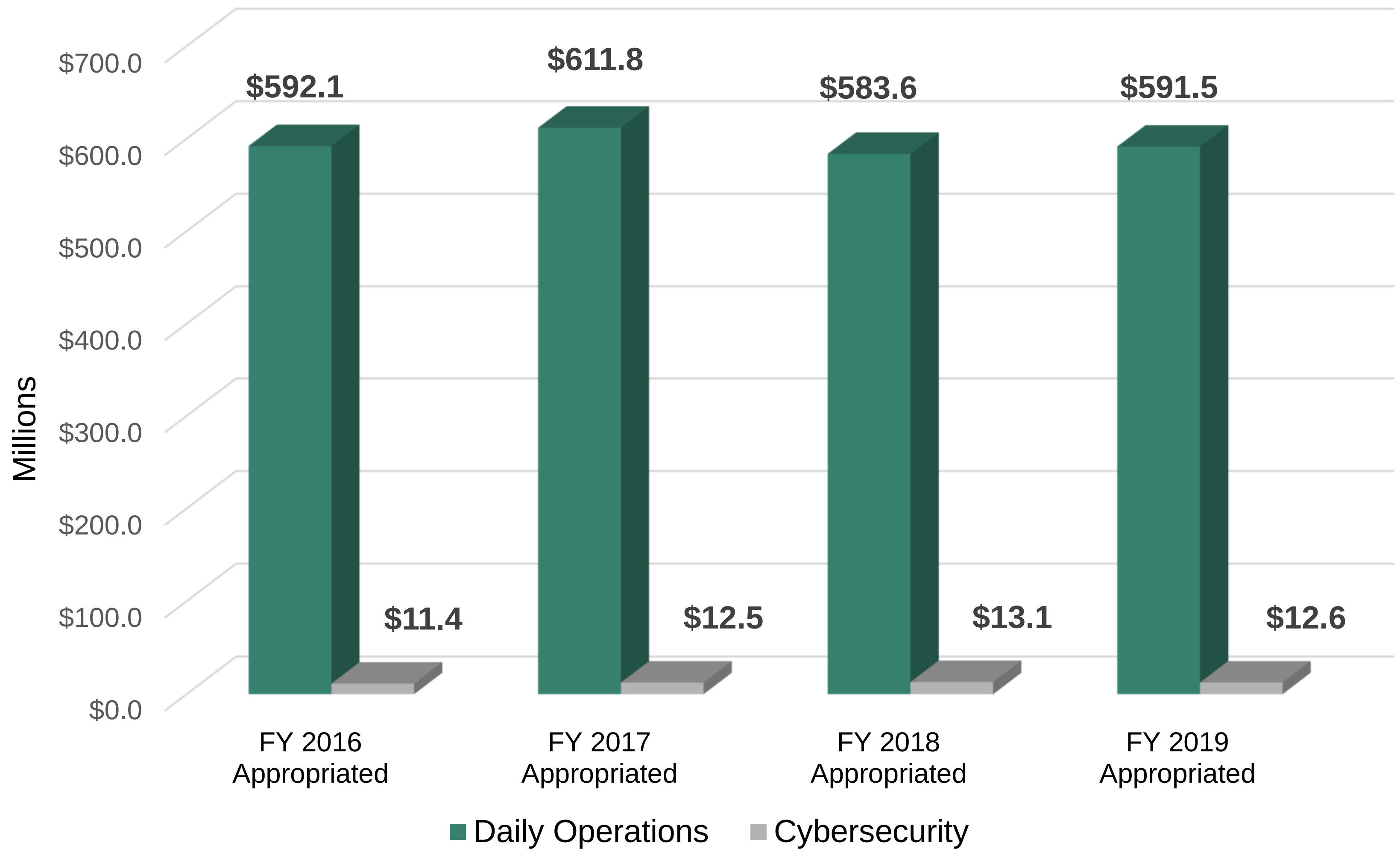
State Information Technology (IT) Budgets

- In FY 2016-17, agencies were appropriated $17.7 million for new cybersecurity projects.
- In addition to the $21.5 million appropriation to DIR for on-going cybersecurity services, in FY 2018-19 other agencies received $24.0 million for new cybersecurity projects and initiatives.
- Typically, cybersecurity is not a specified item in the state budget and is included within appropriations for related strategies, projects, and programs.
- State agency IT Operating Plans average $2.8 billion per year in FYs 2016 - 2019 for DCS, CAPPS, Capital Budget Projects, and Daily Operations.
- Cybersecurity projects are an estimated 2 percent of planned IT expenses, with the exception of DCS which is estimated between 5 and 10 percent.

Data Center Services (DCS) and Estimated Cybersecurity Costs



Daily Operations and Estimated Cybersecurity Costs



Major Information Resources Projects

- The Quality Assurance Team (QAT) is overseeing 79 major information resources projects with current estimated costs of $1.5 billion over the life of the projects.
- The majority of these are not dedicated cybersecurity projects, although several are being developed strictly for Cybersecurity Advancements and Data Loss Prevention within the agencies or with cybersecurity impacts.
- SB 533, 85th Legislature, requires a state agency assessment of proposed technical architecture for project to ensure agency is using industry accepted architecture standards in planning for implementation.

Impact of Security Breaches

- In FY 2013, the Health & Human Services Commission reported $2.3 million of staffing costs to respond to and recover from 1,948 security incidents.
- In FY 2016, the Department of State Health Services reported security incident costs of approximately $1.9 million.
- Other potential impacts and issues include:
  - Physical loss of devices or media containing data;
  - Incidents affecting IT infrastructure hosted by a third party;
  - Electronic leakage of data;
  - Personal data exposure;
  - Inappropriate IT resource use by employees; and
  - Viruses and malware.

LEGISLATIVE BUDGET BOARD

Contact the LBB

Legislative Budget Board
www.lbb.state.tx.us
512.463.1200