

# DET FACT SHEET: SECURE THE ENTERPRISE



## WHAT IS THE VISION TO SECURE THE ENTERPRISE?

Take an enterprise approach to preserving the confidentiality, integrity, and availability of state and residents' data through the innovative use of the right people, processes, and technology.

## FAQs

**What is the Information Security (InfoSec) Program?** The InfoSec Program is the collection of connected efforts inherent in the DOA DET 2013 Information Technology Strategic Plan to address physical and cyber risks in securing sensitive information, devices, and data channels managed by the State of Wisconsin.

**Who directs the Information Security (InfoSec) Program?** The program will be directed by a Steering Committee of decision-makers that will set strategic direction and prioritize the projects and resources.

## At-a-Glance

---

- 84% of intrusions take just minutes.
- 66% of breaches remained undiscovered for months.
- Breaches are spotted by an external party more than 69% of the time.\*

### How will the Information Security (InfoSec) Program be managed?

The InfoSec projects defined within the scope of the program will be led by project managers reporting to a program manager who will assure the resource priorities are implemented across the projects. This will be effected through:

- a program framework inclusive of the different security layers and areas,
- authority, accountability, and decision-making matrices,
- program-level work scheduling processes, resource planning methods, risk assessments, and estimating techniques,
- and program/project communications requirements and standards.

\* Verizon is a private industry. This data is from a 2013 Data Breach Investigations Report

“The past 15 years of security management have been characterized by a focus on improving the effectiveness of protecting information assets. In the coming years, the focus will increasingly shift to the efficiency and productivity with which this protection is achieved.” – Tom Scholtz, Gartner 2012

## SECURITY FRAMEWORK DIAGRAM

Policies

Controls

People

Information Security Program Management

Secure System Engineering

Information Security Awareness and Training

Business Continuity

Information Security Compliance

Information Security Monitoring

Information Security Incident Responses and Forensics

Vulnerability and Threat Management

Boundary Defense

Endpoint Defense

Identity and Access Management

Physical Security

Process

Technology