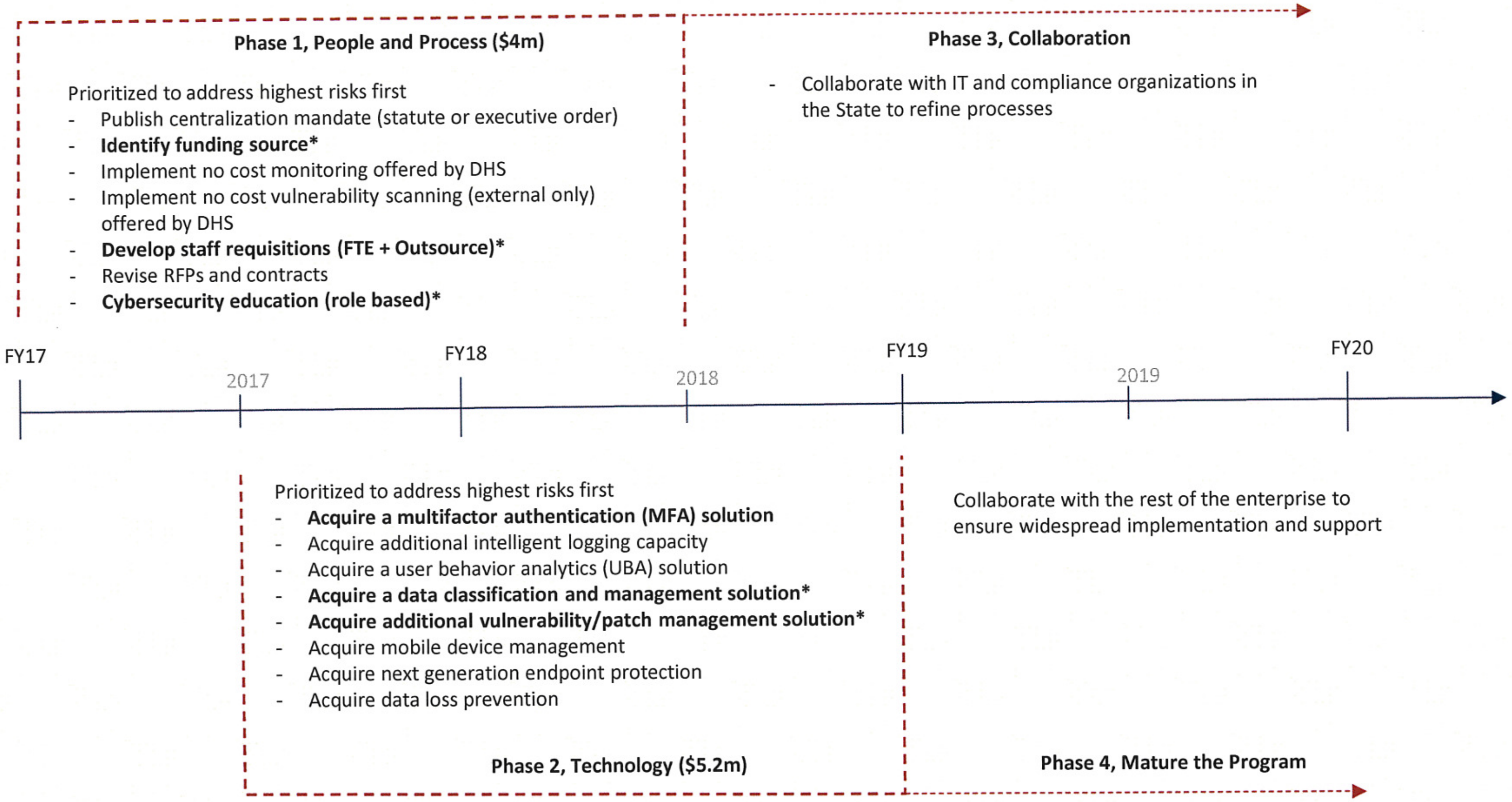
Kansas Executive Branch
Information Security Briefing

AD ASTRA PER ASPERA

Kansas

Phased Approach



Phase 1, People and Process ($4m)

Prioritized to address highest risks first

- Publish centralization mandate (statute or executive order)
- **Identify funding source***
- Implement no cost monitoring offered by DHS
- Implement no cost vulnerability scanning (external only) offered by DHS
- **Develop staff requisitions (FTE + Outsource)***
- Revise RFPs and contracts
- **Cybersecurity education (role based)***

Phase 3, Collaboration

- Collaborate with IT and compliance organizations in the State to refine processes

Prioritized to address highest risks first

- **Acquire a multifactor authentication (MFA) solution**
- Acquire additional intelligent logging capacity
- Acquire a user behavior analytics (UBA) solution
- **Acquire a data classification and management solution***
- **Acquire additional vulnerability/patch management solution***
- Acquire mobile device management
- Acquire next generation endpoint protection
- Acquire data loss prevention

Phase 2, Technology ($5.2m)

Collaborate with the rest of the enterprise to ensure widespread implementation and support

Phase 4, Mature the Program

* note: Repetitive LPA Finding

Top 1 of 5

Organizational Resources (Staff):

Implementing effective information security is dependent on People, Process and Technology. Gathering individuals with expertise in information security that can perform cybersecurity foundational functions is the most important deficiency to address in the State. These individuals must be brought together in a new organization with a clearly defined mission, and clear lines of authority. These people are necessary to make risk-based decisions on further priorities, to build critical processes, and to help educate and change the culture of the State. Once the people are in place, each of the core security functions will begin to mature and provide significant improvements in the information security posture of the state.

Presently, there are only two certified Information Security Officers supporting Executive Branch agencies.

STATE OF KANSAS
K I S O
INFORMATION SECURITY OFFICE

AD ASTRA PER ASPERA
Kansas

Top 2 of 5

Training:

The purpose of periodic security awareness training is to develop essential competencies, new techniques and methods that are so essential in facing possible security issues. Investing in awareness training solution can provide some level of maturity in incident response and help protect organizational resources; by adopting and promoting a robust Cybersecurity Awareness Training Program, organizations greatly increase their security-related risk posture.

Presently there are few programs that are effective and measurable, this is evidenced by through the repetitive number of findings in this topic area by the Legislative Post Audit.

Top 3 of 5

Technology – Multifactor Authentication:

Multi-factor authentication (MFA) is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). This technology is essential for those with elevated system privileges or for those with access to sensitive information.

For example, the breach of the South Carolina mainframe was due to compromised credentials of a system administrator (the admin fell victim to a phishing attack), the attacker was simply able to log in (something they know) and take the data. Had MFA been in use this would not have occurred because a second layer of security (some they have or are) would have prevented the breach.

Top 4 of 5

Technology – Vulnerability Management:

Vulnerability management is the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities", especially in software and firmware. Vulnerability management is integral to computer security and network security.

Vulnerability management is one of the key areas of focus recognized by numerous Legislative Post Audit (LPA) Security Audits over many years. Exploiting an existing vulnerability is second only to phishing in methods of compromise.

Top 5 of 5

Technology – Centralized Intelligent Logging:

Intelligent logging technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources (AV, DLP, FW, IPS, etc.). It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of this technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources – this solution is commonly referred to as Security Incident and Event Management (SIEM). Today, levels of logging from common sources are not sufficient if collected at all, and are rarely monitored.

For example, if an agency is not collecting this information, it would be impossible to identify a compromised system that is exfiltrating data.

Questions?

AD ASTRA PER ASPERA

Kansas