LPA IT Security Audit Presentation

Background:

- We have done IT security audits for many years, in large part because the state lacks an enterprise-level approach to evaluate state agencies' IT security posture.
- In 2015, the legislature codified our IT security audit work into law.
- We select agencies to be audited based on a periodic risk assessment. The assessment is mainly driven by the inherent security risk that agencies have.
- The table below shows a list of 30+ agencies we audited since 2014.

**Agencies That Received an IT Audit
CY 2014 through 2018**

Area	Agency	Release date (a)
Ag and Natural Resources/ Transportation	Department of Agriculture	(Dec. 2015)
	Department of Wildlife, Parks and Tourism	(April 2015)
	Dept. of Transportation	(Oct. 2014)
Education	Kansas Board of Regents	(Oct. 2014)
	University of Kansas	(Dec. 2015)
	Kansas University Medical Center	(Sept. 2016)
	Emporia State University	(Sept. 2016)
	Wichita State University	(Sept. 2016)
	Kansas State University	(Dec. 2016)
	Kansas Department of Education	(July 2017)
	Fort Hays State University	(Dec. 2017)
	Pittsburg State University	(June 2018)
Corrections/ Public Safety	Department of Corrections	(July 2015)
	KS Comm. on Peace Officers' Standards & Training	(Sept. 2015)
	Kansas Bureau of Investigation	(June 2018)
	Kansas Highway Patrol	(Sept 2018)
	Kansas Department of Health and Environment	(Sept. 2018)
General / Financial	Office of the Bank Commissioner	(Oct. 2014)
	Department of Revenue	(Dec. 2015)
	Department of Administration	(April 2018)
KDADS/ Hospitals	Parsons State Hospital	(Dec. 2014)
	Department on Aging and Disability Services	(Sept. 2015)
	Kansas Neurological Institute	(Feb. 2015)
	Larned State Hospital	(July 2017)
	Department of Children and Families	*(est. Dec. 2018)*
	Osawatomie State Hospital	*(est. Jan. 2019)*
Labor/KHRC/ Commerce	Department of Labor	(July 2015)
	Department of Commerce	*(est. Dec. 2018)*
Legislative/ Elected Officials/ Boards	Dental Board	(Dec. 2014)
	Kansas Corporation Commission	(Dec. 2014)
	Kansas Insurance Department	(April 2016)
	Office of the Attorney General	(April 2017)

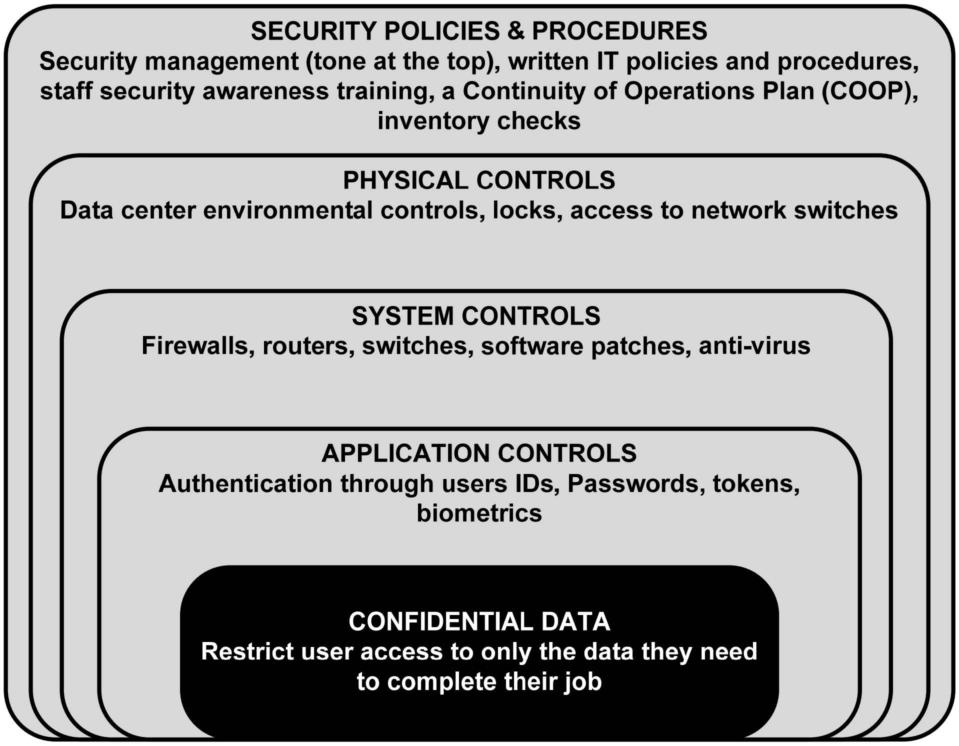
(a) The individual IT audits are permanently confidential. This date refers to the date of the LPAC meeting at which we present(ed) the findings.

- Our IT audit reports remain permanently confidential due to the sensitivity of the information.

- The state has established IT security standards to provide a mandatory floor for security controls. Several other organizations have published security standards, including the International Standards Organization (ISO), the National Institute of Standards & Technology (NIST), and the Center for Internet Security (CIS).

- Whether you look at the state's IT security standards or other sets of standards, they generally include several different categories which, if implemented correctly, produce a layered protection around an entity's most valuable data. This is shown graphically below.

Figure OV-2
Security Layers Should Be Used to Protect Confidential Data



SECURITY POLICIES & PROCEDURES
Security management (tone at the top), written IT policies and procedures, staff security awareness training, a Continuity of Operations Plan (COOP), inventory checks

PHYSICAL CONTROLS
Data center environmental controls, locks, access to network switches

SYSTEM CONTROLS
Firewalls, routers, switches, software patches, anti-virus

APPLICATION CONTROLS
Authentication through users IDs, Passwords, tokens, biometrics

CONFIDENTIAL DATA
Restrict user access to only the data they need to complete their job

Agencies rely on a wide range of IT security controls to help protect confidential data. Those controls exist in multiple layers to help provide numerous barriers to unauthorized access from both outside of and within an agency.

Source: LPA summary of common network security layers adapted from Cisco.

- The purpose of our IT security audits is to evaluate agencies' compliance for a *selection* of the state's established IT security standards.

- Because the state's standards have last been revised November 2014 and are quickly becoming out of date due to emerging threats and changing perspectives, we have supplemented our work with several best practice items.

General Findings for Key IT Control Areas

- **Security Policies & Procedures –** In this area, we evaluate whether agencies provide the mandatory security awareness training to staff. We also do several social engineering tests including simulated email phishing campaigns, clean desk checks, trash and door checks. When Henry in the legal department clicks on an emailed hyperlink to allegedly track an Amazon package or when Susie in HR provides a password over the phone to a supposed IT help tech staff, hackers could use the information to bypass whatever other controls are set up.

  LPA Finding: Many agencies do not conduct security awareness training. Additionally, our social engineering tests demonstrate staff do not sufficiently understand security protocols.

- **Physical Controls –** In this area, we evaluate whether agencies properly restrict access to their data center, which includes limiting staff with unescorted access rights, prohibiting generic badges, and implementing proper environmental controls to protect against water or fire damage.

  LPA Finding: A number of agencies have poor physical controls for their data centers. Identified problems range from allowing too many staff to access their data centers without identified need, issuing generic badges or not properly collecting data center badges or keys when staff leave the agency, and not implementing water, fire, temperature, or humidity controls.

- **System Controls –** In this area, we evaluate whether agency computers are up-to-date and supported. Vendors must constantly update operating systems and software to prevent newly discovered vulnerabilities from being exploited. Eventually, keeping those systems current becomes ineffective so vendors announce a day when they will stop releasing updates. At that point, the operating system or software is considered "unsupported." It essentially reaches "end of life." Agency IT staff must keep up with installing available security patches and change out OS and software once it becomes unsupported.

  LPA Finding: Many agencies fail to properly patch their computers or servers, essentially not keeping up with available security updates. Our test scans also frequently find agencies have computers with unsupported operating systems and *applications. This is worse because are no patches available and hackers can devise continuous and unknown ways to exploit these weaknesses to gain access.*

- **Access Controls (Application controls)** – In this area, we evaluate proper password and lockout settings. Even though the world is moving to biometric and multi-factor authentication, most state agencies continue to rely on singular passwords for users to "authenticate," or enter, agency network or specific applications because it is cheaper. Because of the risks, it is critical to set up strong access controls for singular passwords. Lastly, we evaluate whether agencies have shared accounts which allow multiple people to log into the same account.

  LPA Finding: Several agencies do not adopt strong password settings, increasing the risk of brute force attacks. Poor settings include short passwords without complexity requirements, no lock-out features after users type in a password too many times. Additionally, we often find agencies have shared accounts, often not even realizing it. This creates the risk of not being able to trace improper transactions to a particular individual.

Root Causes

- **Insufficient awareness of state security requirements.** We were surprised how many IT staff simply are not familiar with the state's requirements.

- **Inadequate top management support, understanding or emphasis.** This was often demonstrated by how "buried" or under-represented security was, and how little top management is briefed or involved in that area. We were surprised at the number of times agencies had prior security findings, indicating top management does not provide sufficient oversight to ensure the agency follows state standards and fixes known problems.

- **Lack of sufficient IT resources.** This was demonstrated by missing IT positions, long vacancies, not filling positions, and high turnover especially for CIO or ISO positions. Inadequate staff resources means employees put out fires to ensure business functions continue, rather than developing strategic plans for security. State pay that's not commensurate for necessary expertise, as well as overall budget constraints contribute to insufficient staffing or outdated equipment.

- **Lack of sufficiently knowledgeable staff**. We saw agencies parceling out security duties to people with insufficient training or understanding, and small agencies that did not know about security at all.

- **User pushback**. Security standards generally slow down or make business functions harder – for example, having to remember long, complex passwords. When the agency does not have a good representation of why those controls are necessary, user pushback can result in business needs winning over security.

- **Too must trust.** Generally, agency staff fail to think about insider threats and are not sufficiently skeptical that bad things can happen based on intended or unintended behavior by staff or contractors.

- **Poor communication across agency divisions.** This is more prevalent in larger agencies with separate or independent reporting functions to coordinate and implement security responsibilities.