KANSAS LEGISLATIVE
DIVISION of
POST AUDIT

A Performance Audit Report Presented to the Legislative Post Audit Committee

3 Year Summary of Security Controls in Selected State and Local Entities (2020-2022)

December 2022

Report Number: R-22-017

Introduction

K.S.A. 46-1135 authorizes our office to conduct information technology audits as directed by the Legislative Post Audit Committee. These audits are conducted on a three-year cycle. This three-year summary report answers the following question:

Do state and local entities adequately comply with significant information technology security standards and best practices?

Between January 2020 and December 2022, we conducted 21 audits on 20 entities (1 entity was audited twice during this timeframe). **Appendix A** lists the 16 state agencies and 4 school districts, their expenditures, and their FTE.

Our audit work generally evaluated 9 IT control areas. In 2022, we added a 10th control area because the Information Technology Executive Council (ITEC) revised and strengthened requirements for business continuity and disaster recovery planning in the prior year.

Within each IT control area, we generally measured an entity's compliance based on the state's IT security standards. Those standards are codified in ITEC policies 7230A and 5310, and state law. We also reviewed compliance with certain best practices. We did this because the state's standards had not been updated to include certain accepted industry standards. We reviewed between 37 and 51 applicable control items across audited entities.

To assess compliance, we interviewed staff, reviewed relevant policies and procedures, and evaluated relevant computer settings. We reviewed security awareness training documentation and other security controls. We used entity staffing information to evaluate certain deprovisioning, asset inventory, and account control processes. We also inspected data centers and performed or reviewed vulnerability scans on entities' computers. Lastly, we conducted or evaluated limited social engineering tests.

We issued reports to each entity throughout the three-year audit cycle. These individual reports are confidential under K.S.A. 45-221 (a)(12) & (45) because releasing that information could jeopardize the entities' IT security.

This summary report is based on the individually conducted audits and conforms to generally accepted government auditing standards. Some caveats follow:

- For each entity's audit, we limited our work to a handful of controls within each area in our audit plan. Because we did not evaluate a larger number of controls in areas such as boundary protection, access control, or system controls, there is residual risk that additional control weaknesses may exist.

- Physical distancing requirements due to COVID-19 limited our test work in certain areas during the past 3 years. As a result, we did not always conduct

physical inspections of data centers and work spaces (for clean desk or trash checks), and we cut back on certain asset inventory tests.

- Sometimes we relied on the entity or the Kansas Information Security Office to provide certain data, including their phishing test results and security awareness training records. We conducted testing on these data sets to consider the source data sufficiently reliable for our analyses.

- Some work required the use of samples. In some cases, we used judgmentally-selected samples. Although these results cannot be projected, the problem findings identified represent security threats which in and of themselves provided us with reasonable assurance that a problem existed. It is possible our work using samples showed compliance despite existing problems. As a result, our analyses should be viewed as an indicator of an area's status, and not viewed as absolute assurance.

Almost half of the 21 entities we audited between 2020 and 2022 did not substantially comply with applicable IT security standards and best practices.

Responsibilities and Initiatives

Under established security standards, state and local entities must protect sensitive information against data loss or theft.

- Many Kansas agencies collect tax, health, student, or other sensitive personal information on taxpayers and citizens. Examples include student records, tax returns, criminal records, and health care information. Several agencies maintain confidential information that have significant penalties for loss or disclosure.

- Kansans use state agency services and programs and depend on agencies to protect their personal information.

- Government agencies across the nation are consistently targeted because they maintain valuable information.

    - In May 2020, 2 ransomware attacks hit the Texas Department of Transportation. Officials said the FBI was alerted and is involved in the investigation. Texas has had prior ransomware attacks, including 1 on the Texas Court system, and a series of incidents in August 2019 affecting 22 local governments, with a collective ransom demand of $2.5 million.

    - In April 2021, the state government agency that oversees West Virginia's unemployment insurance program, learned its online database of job seekers and job openings was breached. The agency said it contacted everyone whose information may have been affected but didn't reveal how many people this included. Officials stated the database was secured soon after the breach was discovered.

    - In September 2021, the Alaska Department of Health and Social Services warned that a highly sophisticated cyber-attack exposed residents' personal data, including financial information.

    - In February 2022, the Washington State Department of Licensing, which licenses around 40 categories of businesses and professionals had to shut down its online licensing system after learning of suspicious activity involving sensitive data from a quarter-million professionals.

- In October 2022, pro-Russia hackers claimed credit for state website disruptions in Colorado, Kentucky, and Mississippi. The disruptions were temporary and did not appear to involve data breaches. However, such events could negatively affect residents who may use their state web portals to apply for licenses or conduct other business.

State and local entities must balance their business needs against security risks.

- Generally, state agencies are not in the information security business. Their focus is on accomplishing their core missions such as collecting taxes, housing inmates, monitoring air and water quality and so on. Similarly, Kansas school districts' missions center on educating children from kindergarten through 12th grade.

- Implementing security controls takes staff, time, and resources. Security controls often can reduce staff speed or limit functionality. This creates a conflict between business needs and security risks.

- Entities must evaluate and understand their security risks to make informed decisions about which controls to put in place and how to go about it, all while carrying out their primary missions.

Several statewide initiatives are aimed at improving the state's information security.

- The Kansas legislature created the Information Technology Executive Council (ITEC) in 1998. ITEC has established security policies all state agencies must follow.

- The state's ITEC security policies are similar to other security standards including those issued by the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST). The state's standards require policies and procedures over physical controls, system controls, and application controls. Together they form a multi-layered approach to safeguard confidential data and are designed to help agencies create and maintain a strong security posture.

- In 2011, Governor Brownback initiated IT centralization through Executive Order 11-46. This order required all non-regent IT directors under the Governor's jurisdiction to report to the Executive Chief Information Officer. It was intended to increase the efficiency and uniformity of IT within the executive branch.

- The 2018 Cybersecurity Act (K.S.A. 75-7236 et seq.) aimed at reducing the risk of cybersecurity breaches within state agencies. Important features of the Act are as follows:

- **It pertains to most executive branch agencies with a few exceptions.** Elected office agencies, the Adjutant General's department, the Kansas Public Employees Retirement System, the regents' institutions, and the Board of Regents were exempted.

- **It created the Kansas Information Security Office (KISO) as a separate state agency to administer the Act.** KISO helps agencies develop cybersecurity programs in compliance with state and federal security standards. KISO also provides a cybersecurity training program at no cost to the agencies. KISO is led by the State Information Security Officer, who helps coordinate cybersecurity efforts between agencies.

- **It codified cybersecurity service costs.** The Act allowed agencies to pay for cybersecurity services from several sources, including fees. It also allowed KISO to charge agencies for certain security-related functions and required those fees to be used only for cybersecurity purposes.

- **It clarified that agency heads remain responsible for their agency's security postures.** Under the Act, agency heads have several specific responsibilities, including ensuring an agency-wide information security program is established and designating an information security officer. Agency heads also were required to participate in annual agency leadership training on statutorily prescribed cybersecurity-related topics, notify the CISO about breaches within 48 hours after discovery, and submit a cybersecurity report to the CISO every 2 years.

- The state's security policies get revised periodically to incorporate new or improved best practices or respond to technological changes.

    - In July 2019, ITEC revised the IT security standards. Prior to that revision, those standards were last updated in November 2014.

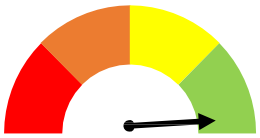
    - In September 2021, ITEC revised its business contingency planning requirements which were last updated in 2006. With this revision, ITEC also created specific requirements for disaster recovery.

- In July 2021, the Governor established a bipartisan Kansas Cybersecurity Taskforce. The taskforce was charged with developing a comprehensive plan to address potential cybercrime, and protect essential services on which Kansans and businesses depend. The taskforce published its final report in January 2022.

IT Security Audit Method

- At the start of each calendar year, the Legislative Post Audit Committee approved our suggested auditees. We selected agencies based on past audit results, the length of time that had passed since their last IT security audit, and other criteria.
- In 2021 and 2022, we added 4 K-12 school districts to our list of auditees, which the Committee approved. We surveyed larger school districts and selected from those who were most willing to undergo our audit.
    - It should be noted that the state standards we used (based on ITEC requirements or law) do not apply to Kansas school districts. We also learned that the State Department of Education had no IT security standards or requirements in place for school districts to follow. As a result, we decided to apply our audit plan as a best practice standard for the 4 districts we audited in 2021 and 2022. Our office also published a limited-scope audit in October 2021 to better gauge the IT security practices and resources for Kansas school districts more generally.
- As part of each audit, we evaluated roughly 45 individual control items across 9 areas. Area examples include security awareness training, account security, and vulnerability remediation. Most individual control items we evaluated came from ITEC policies or state statute. Lastly, our audit plan included a handful of best practices that were not codified in Kansas policy or law.
- To score entities' performance within each control area, we awarded between 0 and 3 points for each requirement or best practice we evaluated. Generally, we awarded 3 points for full compliance and 2 points when the entity was mostly compliant. We awarded 1 point when the entity had taken initial steps towards compliance, and 0 points if the entity had no process in place to adhere to the requirement. The resulting points in each control area were converted to a percentage which fell into 1 of 4 possible quadrants. **Figure 1** shows the possible results.

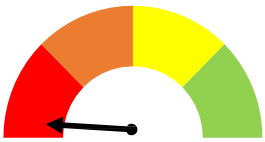
Figure 1. LPA categorizes Area and Overall Results within Individual IT Security Audits using compliance measures.



A green speedometer indicates 76%-100% compliance.
Within control areas, this means **minor/no control issues**.
Overall, it indicates **substantial assurance**.

A yellow speedometer indicates 51%-75% compliance.
Within control areas, this means **moderate control issues**.
Overall, it indicates **reasonable assurance**.

An orange speedometer indicates 26%-50% compliance.
Within control areas, this means **major control issues**.
Overall, it indicates **limited assurance**.



A red speedometer indicates 0%-25% compliance.
Within control areas, this means **significant control issues**.
Overall, it indicates **very limited/no assurance**.

Source: LPA methodology for IT security audits CY 2020-CY 2022

- Lastly, we assessed overall performance across the 21 audits using the results from all areas and opined on root causes for entities' overall performance within each confidential report.

IT Security Audit Results

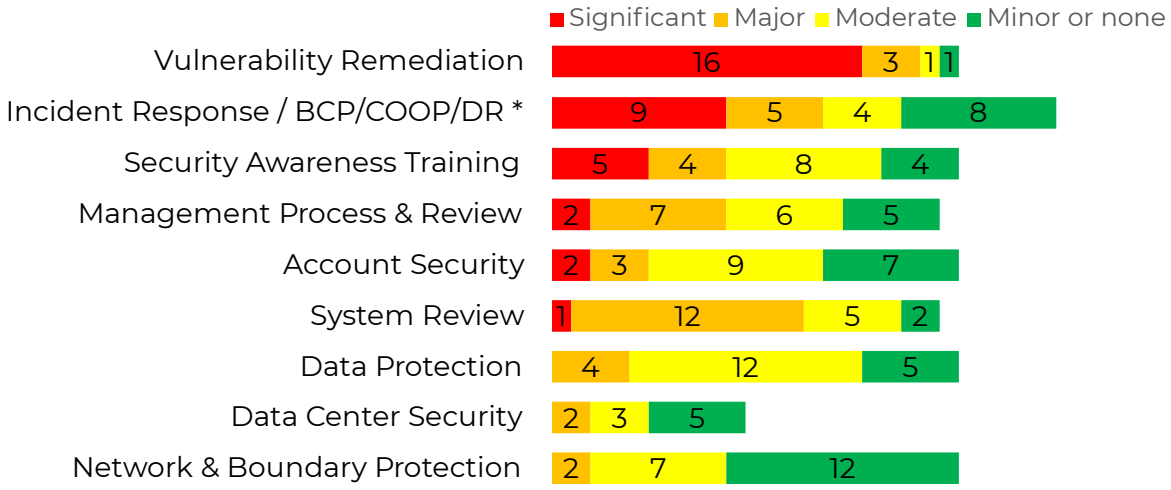
10 of the 21 entities audited in the past 3 years did not substantively comply with applicable IT security standards and best practices.

- As mentioned previously, we tested between 37 and 51 control items across 9 areas, generally averaging 43 items per audit.
- All entities had at least some control issues, ranging from a low of 15 to a high of 42 control items with less than full compliance. In other words, no entity passed with a clean review.
- 10 entities scored below 50% and received an overall 'limited' or 'very limited' audit assurance rating. Such entities can be thought of as not substantively complying with applicable audit standards and best practices. These 10

entities generally also had significant or major control issues in 4 or more control areas. The other 11 audits we conducted resulted in 'reasonable' or 'substantial assurance'.

- **Figure 2** shows the number of findings across all 21 audits (20 entities) by IT control area and severity.

Figure 2: Results of IT Security Findings Across 21 Audits



Source: LPA summary of IT security audits of 20 entities (one entity was audited twice) from January 2020 through December 2022.

* This category has more results than audits because ITEC created specific requirements for Disaster Recovery (DR) which we evaluated separately from Business Continuity Plan (BCP) / Continuity of Operations Plan (COOP) in 2022.

- As the figure shows, a handful of areas had the most significant security weaknesses. Those areas included vulnerability remediation, incident response/continuity of operations, and security awareness training.

- We also judgmentally selected and reviewed a specific IT system that maintained or processed confidential or sensitive data at most audited entities. This is shown in Figure 2 as "System Review." Findings in this area are discussed in greater detail later in the report.

- For ease of understanding, we counted the entity that received 2 audits during this time period as 2 entities in the sections that follow.

The security findings summarized in this report are similar to those in previous summary reports.

- Our audit work varies somewhat from year to year. Nevertheless, we consistently evaluate certain security areas we think are most important and part of a basic security process.

- State agencies and local school districts across the state continue to have similar IT security issues to those we've identified as far back as 2003. Results in this 3-year summary (CY 20-22) were generally similar to the results from the 2 previous 3-year reports (CY 17-19 and CY 14-16). Areas of greatest concern continued to be inadequate scanning and patching processes, security awareness training, data protection, and incident response and continuity of operations planning.

- We audited several agencies for the second or third time during the past decade. Some agencies improved their security posture from one audit to the next, while others had repeat findings. For example, 1 agency had poor data center controls, no asset inventory, and poor deprovisioning processes for departing staff in a prior audit, but showed marked improvements in this 3-year period. Conversely, another agency had failed our prior audit and during this 3-year period, with repeat findings in security awareness training and vulnerability remediation, among other issues.

A lack of proper top management attention and inadequate resources generally were the main reasons for compliance problems.

- Top management ultimately is responsible for an entity's information technology governance, risk management, and compliance. Despite, this, we often found top management had not set sufficient expectations or monitored compliance with security standards. We also found several entities lacked a strong security culture, based on repeat audit findings.

    - At 1 entity, we found IT management overestimated the effectiveness of its technical controls.

    - Several entities made conscious decisions to favor business activities over security. This was particularly true in deciding not to upgrade or fix security issues for failing IT systems, because those systems were said to be replaced sometime in the future.

    - Lastly, a lack of required IT security standards for Kansas school districts likely contributed to district officials not mandating stricter security controls.

- Inadequate IT security staff resources within IT divisions make it difficult to create or maintain a security baseline or retain institutional knowledge. Several entities had no or few security staff (including a dedicated Security Officer) to carry out IT security work even when those entities held highly sensitive data. In at least 2 entities, a key security position remained vacant for months. In several entities, we noted security resources were likely insufficient given the entity's size and federal compliance requirements. Conversely, entities that invested in IT resources and had sufficient, experienced staff generally had a robust security posture.

Most Significant or Most Common Security Weaknesses Across Entities

Most entities (90%) did not adequately scan or patch their computers to keep them secure.

- Over time, vulnerabilities in computer software are discovered that could allow someone to break in or otherwise harm an entity's network. Entities must periodically scan for known vulnerabilities. More importantly, entities must apply patches to keep their computers secure.

    - **Many entities did not scan their computers at all or performed only partial scans**. 5 entities did not perform any scans, and 3 more had paused certain computer scans for several months due to technical issues. Another entity could not provide past scan results for review. Several entity-provided scans we reviewed did not include all networked computers or servers. 1 entity's scanning product only identified Microsoft-related vulnerabilities. Lastly, our review of several entity-provided scans showed they were uncredentialed. Uncredentialed scans do not provide enough insight into computer vulnerabilities and can provide a false sense of security.

    - **Most entities did not adequately patch their computers**. Scans generally measured entities' computers based on the Common Vulnerability Scoring System (CVSS). The CVSS is a free and open industry standard to measure the severity of computer system vulnerabilities. A CVSS score of 7 or higher indicates a vulnerability is high or critical, as classified by the industry. Our review showed entities' average CVSS score for sampled computers often ranged in the hundreds. For example, 1 entity had an average score of 234 per machine (the scan included 139 machines across 2 different locations). Such results indicated entities did not properly patch serious Microsoft and 3rd party software vulnerabilities. Lastly, many entities' computers had CVSS-recognized vulnerabilities that dated back a decade or longer.

    - **Most entities also used unsupported software, applications, or operating systems**. When those products become too old to maintain,

vendors no longer release security updates for them. Those products are considered "unsupported." Our scans frequently found unsupported versions of Microsoft software as well as 3rd party software such as Adobe Flash Player, Acrobat, or Reader and Java. We also found unsupported internet browsers and operating systems such as Windows Server 2003, Windows 7, or Server 2008.

- Without a systematic approach to identify and patch known vulnerabilities and eliminate unsupported products, entities leave their computers open to attack from hackers. This increases the risk those computers are used to compromise the entity's network or even other entity systems.

More than half of the entities (57%) did not have adequate incident response and continuity of operations plans, or did not appropriately test them.

- An incident response plan lays out steps to isolate, contain, and remedy a security incident. Security incidents can be minor (e.g. staff accidentally sending a client's personal information to the wrong recipient) or major (e.g. network breach and subsequent ransomware).

- Continuity of Operations Plans (COOP) and disaster recovery plans outline an entity's strategy to remain operational and minimize downtime of critical IT systems when faced with a major disruption. We started evaluating COOP and disaster recovery plans separately in 2022 because related ITEC requirements were strengthened in Fall 2021. For purposes of this report, we combined information from the incident response and COOP/disaster recovery areas.

- Once plans are in place, entities should test them to ensure they work the way management intends and important information is not left out.

    - **Several entities did not have an incident response plan while others' plans were inadequate**. 1 entity only had a draft incident plan. Additionally, at least 4 entities had not tested their plan or had no documentation of a real incident being worked.

    - **Several entities did not have adequate disaster recovery or continuity of operations plans.** For instance, at least 3 entities did not have a disaster recovery or continuity of operations plan at all. 2 other entities had not updated their plans in over a year; those plans listed staff that had since departed. Several entities' plans were not yet finalized. A number of plans we reviewed did not have any information concerning entities' IT systems or were missing other required information. Lastly, at least 6 entities had not tested their plans at all or recently enough.

- Having adequate plans and testing them regularly helps staff get through security breaches or natural disasters. Without a plan, non-IT staff may not know how to identify and notify IT staff of an incident. Similarly, without incident response, disaster recovery and continuity of operations plans, IT staff could miss important containment, recovery, or communication steps when dealing with a serious disruptive event. Having incident response and recovery plans in place has become even more critical due to the higher likelihood of cyberattacks caused by the pandemic, geopolitical events, and sophisticated threat actors.

Almost half of the entities (43%) did not provide adequate security awareness training.

- Security awareness training educates employees on why security controls are necessary and where risks come from. One of those risks is social engineering—the art of manipulating, influencing, or deceiving people to circumvent internal controls and gain control over computer systems.

    - **Security awareness training processes were inadequate in a variety of ways.** Several entities did not have a dedicated training program at all or were missing key components. Many entities did not provide security awareness training to new employees who should receive training within their first 3 months on the job. 4 entities did not provide annual training to their staff at all. Other entities provided training for new and existing staff, but did not ensure employees consistently participated. Lastly, 5 entities exempted certain groups of employees - such as board members or staff without email accounts - from the training without documenting the exemption.

    - **Most entities failed simulated phishing email tests**. We tested 5 entities by sending simulated phishing emails claiming such things as notice of traffic violations, unread Twitter messages, or failed package deliveries. At 9 additional entities, we relied on the entity or the Office of Information Technology Services to perform similar tests. Of the 14 entities tested, click rates averaged 9.5%, and ranged between 1% and 26.5%.

    - **Staff at several entities did not dispose of or secure sensitive information properly.** Due to physical distancing requirements, we were only able to do clean desk and trash checks at 6 entities. At 1 entity, we recovered sensitive information (name, date of birth, SSN) from locked, but overflowing shred bins. At another entity, we saw 2 passwords on whiteboards. Those were said to be used to set up Microsoft Office accounts and send protected files. At a 3rd entity, we found a document with an employee's name, birthdate, and employee ID sitting next to a printer located in a common area.

- Security awareness training is important because people are the weakest link in an entity's security posture. Entities use technical hardware and software to implement security controls at several levels. However, all it takes is for 1 employee to plug in a virus-infected flash drive, click on a phishing email link, or hold the door open for an unauthorized individual to gain access to physical premises to bypass technical controls in place.

Almost half the entities (45%) had significant management, contract, or policy-related weaknesses.

- Entity policies should describe rules for how staff should use equipment and the internet. In addition, Kansas law requires most executive-branch agencies to designate someone to oversee their security programs. Lastly, entities should incorporate language into IT-related contracts that protects both the entity and its data.

- We found entities had problems in all 3 areas.

    - 1 entity lacked a policy for personally-owned mobile devices used for work. Another entity's acceptable use policy did not address internet restrictions and lacked certain approval signatures.

    - At least 8 entities did not have documented risk management processes, while 2 others had a process but did not identify or update specific risks. Those activities help identify, track and follow up on risks to help make good decisions for the entity.

    - Several agencies did not designate someone to oversee their security programs. Security officer positions did not always report directly to executive leadership. Both are statutory requirements for most executive branch agencies and considered a best practice for others.

    - IT related contracts often did not include language to allow the entity to validate its contractor's security controls. Additionally, some contracts were missing clauses to ensure confidential data was returned or destroyed when the contract ended.

- When entities do not set clear expectations through polices or processes, it is more difficult to hold employees accountable for risky actions (e.g. using the internet inappropriately). Similarly, entities that use contractors should not simply assume the contractors will take the necessary precautions to protect the entity's sensitive data.

<u>Other Security Weaknesses Across Agencies</u>

Several entities (24%) had inadequate account security controls.

- Account security controls are designed both to limit and track who has access to an entity's network and data. One common control is to require account passwords to be a certain length or to contain letters and special characters (complexity). Another control locks out users from trying to log in to their accounts if they enter the wrong password too many times. This control prevents hackers from trying numerous passwords until they find one that works ("brute force"). Other controls require user accounts to be disabled or deleted when staff leave employment. 5 entities had significant or major problems in this area. Other entities also failed individual account security control tests.

    - **Several entities did not meet basic password setting requirements.** For example, 1 entity had no length or complexity requirements for account passwords, while another allowed 2- and 4-character passwords (without complexity) on their respective Windows and Apple computers. At least 2 entities did not require adequate account lockout settings to prevent brute force attacks.

    - **Most entities did not disable accounts belonging to former employees in a timely manner or at all.** For instance, 1 entity left 2 accounts of former employees open for more than 5 months (we tested 14 accounts). Several other entities had active accounts at the time of our audit, or did not disable accounts timely.

- Account security processes integrate with other controls, such as security awareness training and boundary control. When account security controls are weak, it is easier for unauthorized individuals to circumvent them and gain access to an entity's network and data.

Some entities (19%) did not adequately encrypt, back up, or destroy sensitive electronic data.

- Entities need to protect their data so that only authorized individuals can access it. Encryption is a sophisticated way to scramble electronic data so it can only be read by those who have the code to unscramble it. Additionally, entities should maintain an "air-gapped" copy of their data they can use in case their systems get compromised and networked data becomes unavailable. Lastly, entities should have up-to-date asset inventories, and ensure they destroy sensitive data on devices that are taken out of service.

- 4 entities with major findings had a combination of problems including no policies or suitable tools to ensure staff encrypt sensitive data when transmitting it outside the entity's network boundary (firewall), inaccurate or incomplete data asset inventories, and poorly documented or inadequate processes for disposing of old drives or computer hardware. All 4 entities also lacked complete offline (air-gapped) copies of their data. Most other entities had isolated findings in this area.

- Entities without backup data could face severe disruption should their primary data become unusable. Lastly, without adequate encryption, asset inventory and device destruction processes, entities risk their confidential data being accessed and used by unauthorized individuals.

A couple of entities did not adequately protect their network boundaries.

- A network firewall serves as a protective barrier between an entity's network (and the computers on that network) and the Internet. Entities must use updated firewall hardware and software, and should use firewall rules and exceptions to control who gets access to their network. Logging and reviewing abnormal network traffic are other important controls.

- 2 entities we audited lacked a combination of controls in this area. For example, several firewalls at 1 entity had reached end of life and were no longer supported. Its log settings prevented new information from getting captured once the server ran out of storage space, and the entity didn't have adequate network access controls in place. The other entity lacked firewall logs altogether and did not have network access controls either.

- Because a network firewall is often an entity's first layer of defense, it is critical that its software is up to date with the latest security patches. Robust practices for logging and reviewing anomalies allow entities to identify potential incidents early and recover more quickly from an attack. Network access controls help prevent unauthorized devices from gathering information about the network or introducing malware.

A couple of entities had poor access or environmental controls for their data centers.

- Entities typically use data centers to house their critical information systems. Data centers must have controls to limit who has unescorted access to them. They also must prevent or limit damage from environmental hazards, such as water, fire, temperature, and humidity.

- Physical distancing requirements due to COVID-19 prevented us from conducting data center inspections of each entity. However, 2 of the 10 entities we inspected had major findings.

    - For example, 1 entity acknowledged it did not perform background checks on staff with unescorted access to its data center. That entity also did not have an accurate, comprehensive list of staff with such access. Lastly, that entity's data center lacked water detection and humidity monitoring systems.

- The second entity had about 40 generic electronic badges that allowed data center access, in addition to the possible use of physical keys (both methods lack sufficient authentication). Its data center also lacked a dedicated water detection system. That entity also failed to collect and turn off electronic badge access for the former entity director who had not worked for the entity in over a year.

- Poor data center access controls increase the risk that individuals could lose, damage, or steal assets or data. Entities that use data centers with poor environmental controls risk data loss from fire or water damage. These problems could severely disrupt the entity's ability to provide services.

Review of Specific Information Technology Systems

Significant security issues existed within entities' specific IT systems.

- We also reviewed specific IT systems that maintained or processed confidential or sensitive data for almost all auditees. For those systems, we reviewed a limited number of account security, data protection, and vulnerability remediation controls similar to the entity-wide tests within our audits.

- Almost two-thirds of the entities we audited had major or significant security control weaknesses within their specific IT systems. Others had moderate issues. Only 2 entities had just minor issues in this area. Below are more details of what we found:

    - **Systems had poor account security.** We identified generic or dormant accounts at almost all entity systems. For example, at 1 entity we found nearly 400 of about 1,300 user accounts had not been logged into in at least 3 months. We also found over half of the systems we reviewed lacked sufficient segregation of duties. This meant that IT staff could move code between test and production environments without sufficient change controls.

      Many systems also had inadequate password settings, violating length and complexity rules. For example, at 2 entities, systems allowed users to select a 1-character password, falling short of the 12-character length requirement. Several other entities had systems that required only 5, 6, or 8-character passwords without complexity. Some of these systems also did not have a lockout feature.

    - **Systems lacked adequate data protection.** Over half of the systems we reviewed had accounts tied to users who were no longer employed by the entity that had not been disabled timely or at all. For example at 1 entity, accounts for 3 of 15 former staff who had left months prior to the audit were still active. We also found that the backup system data for 9 entities were not tested annually.

- **Systems generally were not sufficiently scanned and patched.** Several entities' systems were administered by contractors. For those, auditees had limited or no insight into the scanning and patching processes or health of the relevant computers. At 1 entity, we found the contractors' scans were uncredentialed. And 2 entities performing their own scans did not regularly scan their system servers as required.

  Lastly, recent vulnerability scans we conducted or reviewed as part of our audits often showed system servers had numerous vulnerabilities, indicating inadequate patching processes. For example, the servers at 1 entity had an average CVSS score of 126 per machine (even after excluding low and medium vulnerabilities). This translates to 13-18 critical or high vulnerabilities per machine. That same scan identified unsupported operating systems and software, such as Microsoft Windows Server 7 or Server 2008 R2 instances.

- **Almost all entity systems we reviewed lacked risk and security assessments**. Most entities had not assessed or documented risks to their systems and lacked security plans that would document how risks were being mitigated.

- These audit results show security weaknesses exist not only at an entity-wide basis, but more importantly on systems that hold some of the most sensitive data these entities administer. Without proper account security, data protection, and systematic approaches to identify and patch known vulnerabilities and eliminate unsupported products, entities face increased risks of security incidents affecting those systems.

Conclusion

Our IT security audit work over the past 3 years revealed significant weaknesses in several security control areas across the 21 entities we audited. Auditees consistently struggled in 4 areas: vulnerability remediation (scanning and patching computers), incident response and continuity of operations planning, security awareness training, and specific IT system compliance. These themes are consistent with issues we identified in our prior IT summary reports. Problems appear to be the result of 2 main issues: insufficient management oversight and lack of adequate IT resources.

State and local entities could face significant consequences if hackers are able to access an entity's network or confidential data because of poor security controls. A significant security breach could disrupt an entity's mission-critical work and their reputation would be sorely damaged. A breach also could require costly customer credit report monitoring and could create legal liabilities or financial penalties for school districts or state agencies.

Although the state has taken steps to strengthen security by passing the Cybersecurity Act (in 2018), centralizing IT positions and services through the Office of Information Technology Services (OITS), revising certain technology policies, and establishing the Cybersecurity Task Force, more needs to be done to create a stronger security posture within state agencies and school districts. This is especially important as the shortage of IT security professionals appears to be worsening.

Recommendations

We did not make any recommendations for this summary audit. All 21 entities we audited during the past 3 years received individual recommendations to fix the problems identified. Based on the initial responses to the audits, entities generally planned to remediate most findings. We conducted follow up work the following calendar year to check on entities' progress. Results from our follow-up work for audits conducted in 2020 and 2021 showed that entities said they had fixed a little more than half of the findings. Auditees said the remaining findings were still in progress of being fixed (34%) or not started or refused (14%). Follow-up work for entities audited in 2022 will take place in Fall 2023.

Appendix A - List of Audited Entities 2020-2022 IT Security Audit Cycle

This appendix includes the list of 20 entities we audited between January 2020 and December 2022 (1 entity was audited twice during this period). The list includes each entity's expenditures and FTE.

Agency Name	2021 FTE Staff	2021 Expenditures
Department of Transportation	2,250.3	$ 2,294,100,000
Kansas Dept. for Aging and Disability Services	316.0	$ 2,159,800,000
Department of Labor (b)	485.9	$ 2,021,800,000
Kansas Public Employees Retirement System	98.4	$ 1,910,600,000
Kansas State University	3,651.1	$ 668,000,000
Wichita State University	1,790.4	$ 571,000,000
University of Kansas Medical Center	3,443.8	$ 461,100,000
Blue Valley School District #229	2,902.0	$ 346,300,000
Kansas Board of Regents	62.5	$ 327,200,000
Kansas Department of Revenue	1,049.2	$ 109,200,000
Emporia School District #253	823.7	$ 74,900,000
Department of Agriculture	329.0	$ 53,900,000
Seaman School District #345	565.3	$ 51,800,000
Great Bend School District #428	513.1	$ 43,800,000
Judiciary (not including district courts)	187.3	$ 38,200,000
Parsons State Hospital	477.2	$ 29,400,000
Office of the Attorney General	174.4	$ 25,800,000
Topeka Correctional Facility	261.5	$ 20,200,000
Kansas Racing and Gaming Commission	99.5	$ 7,500,000
Board of Healing Arts	61.0	$ 6,000,000

(a) Rounded to the nearest $100,000
(b) Statistics for the Department of Labor are unusually high due to COVID-19.
Source: Governor's Budget Report, FY 2023, Volume 2 and Kansas Department of Education Data Warehouse (unaudited)