Legislative Research Commission

Governance Of Education Data Security In Kentucky

Research Report No. 396

Prepared By

Marcia Ford Seiler, Director; Brenda Landy; Albert Alexander; Cassiopia Blausey; Thomas Clark; Deborah Nelson, PhD; Sabrina Olds; and Emily Spurlock

Governance Of Education Data Security In Kentucky

Project Staff

Marcia Ford Seiler, Director
Brenda Landy
Albert Alexander
Cassiopia Blausey
Thomas Clark
Deborah Nelson, PhD
Sabrina Olds
Emily Spurlock

Research Report No. 396

Legislative Research Commission
Frankfort, Kentucky
lrc.ky.gov

Accepted December 12, 2012, by the
Education Assessment and Accountability Review Subcommittee

Paid for with state funds. Available in alternative format by request.

Foreword

In December 2011, the Education Assessment and Accountability Review Subcommittee approved a research agenda for the Office of Education Accountability that included this review of the security of Kentucky's education information systems. The review found that Kentucky has many best practices in place, but needs improvement in some key areas.

Staff would like to thank the Kentucky Department of Education, the Commonwealth Office of Technology, and the Kentucky Auditor of Public Accounts for their extensive assistance with this study.

Robert Sherman
Director

Legislative Research Commission
Frankfort, Kentucky
December 2012

Contents

Figures

Summary

This study compared the protections in place to ensure education data security in the Commonwealth of Kentucky to those recommended by recognized data security authorities. The study found that while many important data security provisions are in place, the commonwealth lacks the comprehensive approach to data security necessary to prevent and respond to breaches. This concern is not unique to the commonwealth. Despite their essential roles, sensitive contents, and financial value, state education databases across the nation have weak security and privacy protections, according to a Fordham University study. In general, more value is placed on the acquisition and use of technology and education data than on protections necessary to ensure security.

Data security protections can reduce affordability and usability. As with any area of risk management, the potential threats must be weighed against the cost of risk reduction. While the ideal level of data security is unclear, it is important that the General Assembly and the public be aware of potential risks and the steps necessary to reduce them.

Ensuring the privacy of education data has long been a concern, but protections are more important than ever because of the proliferation of data collected and the variety of ways data are stored, transmitted, and used. The commonwealth has pursued an aggressive agenda to ensure that public education in Kentucky is supported by a broad and complex education technology infrastructure. The commonwealth is a recognized leader in adopting new technologies for education. While these technologies offer exciting potential for educators and students, they complicate data security challenges. Data systems are becoming more accessible and less centrally controlled, and data may be stored out of state or even out of the country, on computers shared by many other clients, with Internet access from anywhere in the world. At least half a dozen outside contractors access or store Kentucky's education information.

Education data systems are not commonly perceived as potential targets; indeed, the Kentucky Department of Education reports that it has not detected a significant, systemwide security breach in at least the past 20 years. Nevertheless, education systems are at risk for a number of reasons. These systems accumulate large amounts of personal information over long periods of time. Data include Social Security numbers, health conditions, and use of special education and other services. Financial systems store employees' personal, salary, and benefits information. The personal information in education systems is worth more than many people realize: Research suggests that personal data in Kentucky's student information system alone could be sold on the underground market for an estimated $1 million. Attacks on data systems can also be made at random for motives other than financial gain. In addition to risks from outsiders, those authorized to access systems are even more likely to cause security breaches, and while these insider incidents are usually accidental, they can expose confidential data to the risk of identity theft.

This report identifies specific data security concerns such as weak passwords, storage of personal data on mobile devices, and a large contract in which data ownership issues were not clarified. While these issues can each be addressed individually, they point to a broader need for a

comprehensive approach to education data security in the commonwealth. The accountability and authority for ensuring education data security are currently diffused among several entities at the state level. The General Assembly has given the Commonwealth Office of Technology statutory authority to oversee governance and implementation of technology, including data security, for state agencies. However, in practice, Kentucky's P-12 data systems are located and managed independently of the Commonwealth Office of Technology.

As for systems managed by school districts, the Kentucky Department of Education has taken the lead in advising and assisting districts in all matters related to education technology, including data security. However, there is no clear statutory authority to ensure that district-level data security plans are developed, implemented, audited, and enforced.

Recommendations

1.1. To improve the availability of information for security planning purposes, the General Assembly should consider legislation requiring notification of all nontrivial data security breaches, whether data are in electronic or paper form.

2.1. The Kentucky Department of Education should work with districts to ensure clear and consistent policies regarding the Individual Learning Plan "invite others" feature and to ensure that students are adequately protected from potential misuse of the feature.

2.2. The Kentucky Department of Education should continue to provide guidance, policies, and best practices to enhance data security at the district and school levels. While districts should be able to make decisions in noncritical areas, the Kentucky Department of Education should require minimum standards for critical areas, including strong passwords, review of security issues in contracts for technology services, the use of personal and mobile devices, and other emerging security issues.

3.1. If it is the intent of the General Assembly that the Kentucky Department of Education be excluded from the Commonwealth Office of Technology's governance, the General Assembly should consider amending KRS 42.728 to add the Kentucky Department of Education to the list of entities not subject to the authority of the Commonwealth Office of Technology.

3.2. The Kentucky Department of Education is currently developing a comprehensive security plan for the department. The plan should be reviewed annually and revised as necessary and should address planning and governance, implementation and management, monitoring and evaluation, and strategic corrective and preventive actions. Specifically, the plan should include, but not be limited to

- governance structures;
- clear and specific lists of security-related duties for each position that impacts security;
- a single, agency-wide security breach notification and response procedure;
- disaster recovery plans, including how they will be tested;
- policies regarding storage of confidential data on mobile devices and public cloud services;

- policies on acceptable use of social networking sites, such as Facebook and Twitter;
- procurement and contract management policies and procedures to ensure security;
- criteria for gauging compliance and the effectiveness of current security provisions;
- a requirement to annually present a brief summary to inform the Kentucky Board of Education of the status of education data security; and
- a requirement to provide dedicated training for employees and awareness campaigns for all system users regarding the importance of complying with security policies.

3.3. When presenting its biennial budget requests, the Kentucky Department of Education should request the personnel and funds needed to ensure adequate security, clearly explaining the risks that each expenditure is intended to address, so that the General Assembly can decide which risks to mitigate and which to accept.

Chapter 1

Introduction

Background

Education information systems are increasingly used for a variety of purposes. These systems store large amounts of personal data over long periods of time and are becoming more accessible and less centrally controlled.

Increasingly educators, researchers, and policy makers across the nation rely on information systems for a wide range of instructional, administrative, and operational purposes. Student information systems track attendance, program participation, and course and test performance. There are systems for financial management, assessment and accountability, college and career planning, and tailoring instructional materials and interventions to individual students. New and emerging uses include monitoring alternative education, identifying students at risk of dropping out, determining how well schools are preparing students for college and careers, and identifying teachers who excel or need additional professional development to address weaknesses.

These systems accumulate large amounts of personal information over long periods of time. A broad range of student data is collected, beginning as early as entry into Head Start and continuing through college graduation; workforce data will soon be added. Data include Social Security numbers, health conditions, and use of special education and other services. Financial systems store employees' personal, salary, and benefits information.

Education systems are becoming more accessible and less centrally controlled as states strive to make them more usable and affordable. Data may be stored out of state or even out of the country, on computers shared by many other clients, with Internet access from anywhere in the world. Most states use outside contractors for some data collecting and reporting needs. At least half a dozen outside contractors access or store Kentucky's education information.

Education systems represent a sizable investment; since 1990, Kentucky alone has invested well over $1 billion of local, state, and federal funds in education technology (US. Dept. of Educ. Statewide; Commonwealth. Dept. of Educ. *2007-2012*).

Despite their essential roles, sensitive contents, and financial value, state education databases across the nation have weak security and privacy protections. Education systems are at risk.

Despite their essential roles, sensitive contents, and financial value, state education databases across the nation have weak security and privacy protections, according to a study by Fordham University (Fordham).

The Kentucky Department of Education (KDE) reports that it has not detected a significant, systemwide security breach in the past 20 years (Couch). While this is very positive news, it should not be viewed as proof that there are no unmet security needs. A common misconception is that education information is at little or no risk because it is not a lucrative target, especially compared to personal financial data. On the contrary, education systems are at risk for a number of reasons:

- As financial institutions increase security, hackers are turning to easier, less lucrative targets and making up the difference in volume (Verizon).
- The personal information in education systems is worth more than many people realize. Based on estimates of underground market prices, Kentucky's student information system alone could be sold for an estimated $1 million (Symantec). Children's personal information is especially valuable because it can be used for several years before children are old enough to apply for credit and discover that their credit is already ruined.
- Many attacks on systems are made at random or for motives other than financial gain.
- While outsiders can breach security, those authorized to use systems are even more likely to cause breaches, and though usually accidental, insider incidents can expose confidential data to the risk of identity theft.
- Lack of evidence that a system was attacked in the past is no guarantee of its current safety. Security breaches are often not discovered for months or years. Moreover, security conditions change continuously, with cybercriminals constantly probing for vulnerabilities and devising new ways to misuse data.

Every organization needs an ongoing, actively supported, pervasive, and comprehensive security program.

For these reasons, every organization needs a security program that is ongoing, actively supported by senior management, pervasive throughout the organization, and comprehensive to avoid gaps.

Less clear is what level of security is desirable; there are tradeoffs among security, affordability, and usability. In an ideal world, every available security protection would be deployed to ensure the greatest possible security. In reality, however, some protections are so costly and difficult to use that they can, in effect, render a valuable system unusable. Overly burdensome protection might

hinder students from developing technology skills or educators from using information to improve efficiency and effectiveness. For these reasons, KDE has expressed concerns about the cost and burden of new security protections (Couch; Commonwealth. Dept. of Educ. *HB 341*).

The costs and burdens of protections must be weighed against the probability and consequences of breaches.

The costs and burdens of security protections must be weighed against the probability and potential consequences of security breaches. Cyber attacks are reportedly on the rise, as are the costs required to contain them; on average, a security breach cost $214 per compromised record in 2010 (Ponemon 5). These costs do not take into account intangibles, such as the public's loss of trust in the organization that experienced the breach.

Previous Study Of Education Data Security

The General Assembly has expressed concerns about education data security in the past. In the 2006 Regular Session, House Bill 341 required KDE to conduct a study of education security. The resulting document focused on three areas of unauthorized access to personal data: protection and prevention, preparation for notification, and notification. However, many aspects of that report are becoming dated as technology evolves and more and different types of data are collected (Commonwealth. Dept. of Educ. *HB 341*).

Authorization Of This Study

This study of the governance of education security was requested and authorized by the Education Accountability and Assessment Review Subcommittee in December 2011. It is part of the 2012 research agenda for the Office of Education Accountability (OEA).

Key Findings Discussed In This Report

Security assurance requires effective governance structures and a comprehensive, ongoing process that includes planning, implementation and management, monitoring and evaluation, and corrective and preventive actions.

- Security assurance requires effective governance structures and a comprehensive, ongoing process that includes planning, implementation and management, monitoring and evaluation, and corrective and preventive actions. Unfortunately, security experts find that security governance is weak in most organizations, and this may be true of many organizations responsible for Kentucky's education information security.

Apparent gray areas as to which Kentucky agencies ensure information security might change as a result of a new information technology (IT) initiative.

- There appear to be gray areas within Kentucky government as to which agencies have responsibility and authority to ensure information technology (IT) security. Changes might be on the horizon, given a new initiative to consolidate executive branch IT infrastructure under a chief information officer within the governor's cabinet, but it is unclear how this initiative will affect education data systems, if at all.

Kentucky is one of only four states that lack security breach notification legislation.

- Regarding some specific aspects of security, Kentucky is one of only four states that lack security breach notification legislation. Some security breaches may go unreported. Most of Kentucky's education organizations have security breach policies, but the policies vary widely among organizations and even among business units within a single organization.

The Kentucky Department of Education (KDE) has been improving data governance, but some recurring security issues could be prevented with more cohesive governance and an enterprise-wide, comprehensive information security program.

- For the past several years, KDE has been improving data governance structures and security policies, but much remains to be done. According to the auditor of public accounts (APA), some security issues that have recurred several years in a row could be prevented with more cohesive governance and an enterprise-wide, comprehensive information security program.

There are no routine security audits of Kentucky's student information system. There is uncertainty about future audits of the financial management system now that the equipment and software are owned by an out-of-state contractor and accessed through the Internet.

- Security is audited for relatively few education data systems. Some KDE systems are inaccessible to routine checks conducted by the Commonwealth Office of Technology (COT) to ensure compliance with state security policies. There are no routine security audits of Kentucky's student information system. The APA probes the security of selected machines involved in KDE's financial management and human resources system. However, it is uncertain whether these audits will occur in the future because this system is now "cloud based," with computer equipment and software owned by an out-of-state contractor and accessed through the Internet.

Contractors need stronger management and oversight with respect to security and data ownership.

- The management and oversight of outside contractors' security needs to be strengthened. Security and data ownership issues are inadequately addressed, especially in contracts written several years ago; contracts are not required to be reviewed again when they are renewed.

Each of Kentucky's 174 school districts establishes and enforces its own security policies. Even if security were perfect at the state level, security weaknesses in any one of these districts could pose risks to Kentucky's interconnected information systems.

- Each local school district establishes and enforces its own security policies. While advice and model policy documents are available from KDE and the Kentucky School Boards Association (KSBA), there is no comprehensive set of minimum security standards that districts must follow. As a consequence, even if perfect security could be achieved at

KDE and other state agencies, a lapse in security at any of Kentucky's 174 school districts could pose risks to Kentucky's interconnected information systems.

Study Method

While this study primarily examines KDE's information security, other agencies that collect and maintain education probably encounter issues discussed in this report.

This study primarily examines the security of information collected by KDE. However, it is likely that other agencies also encounter many of the issues and concerns discussed in this report. Education information is collected and maintained by a number of other agencies, including the Education Professional Standards Board (EPSB), Council on Postsecondary Education (CPE), the Kentucky Higher Education Assistance Authority (KHEAA), and the P-20 Data Collaborative, which is a joint venture of KDE, EPSB, and CPE.

The Office of Education Accountability staff reviewed statutes and regulations as well as the education, information technology, and policy literature to identify generally accepted security standards and best practices. Evidence about Kentucky's education data security included audit reports, interviews with key personnel, reviews of policies and procedures, and reviews of contracts.

OEA staff reviewed relevant state and federal statutes and regulations, as well as the education, information technology, and policy literature to identify generally accepted security standards and best practices. These standards and best practices guided staff inquiries into the security of each of KDE's education information systems. Evidence about Kentucky's education data security included

- audit reports and agency management letters written by Kentucky's APA;
- interviews and emails with key personnel at the APA, COT, KDE, KHEAA, KSBA, Office of Procurement Services (OPS), and the P-20 Data Collaborative;
- reviews of KDE's written security policies and procedures; and
- reviews of contracts and other information provided by contractors that store or access Kentucky education information.

Data Security And Governance Defined

Information security, cybersecurity, and information assurance all concern the security of information, especially when stored, used, or transmitted using electronic devices and the Internet.

Because of the global nature of information technology, similar definitions of security are used by most experts, including those in the US government and international organizations (US. Committee; US. Dept. of Comm. Natl.; ISO. *ISO/IEC 27000*; ISACA. *Cobit 5 for*). To distinguish security in the context of computers from physical security, experts may use such terms as information security, cybersecurity, or information assurance. While these terms have slightly different connotations, all concern the security of information, especially when it is stored, used, or

transmitted using computers, other electronic devices, and the Internet (US. Committee; US. Dept. of Comm. Natl. *Glossary*).

Security In The Context Of Information Technology

Security results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems.

The National Information Assurance Glossary for all US government agencies and contractors defines security as

> A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach (US. Committee 64).

Perfect security is not possible; the degree of security considered adequate takes into account the costs and reduced usability and productivity associated with security protections.

Adequate Security. Perfect security is not possible, and the degree of security considered adequate is not a technical decision but a policy decision, which takes into account the costs and reduced usability and productivity associated with security protections (US. Dept. National. *Glossary*).

Security entails managing risks to confidentiality, integrity, and availability of information and systems.

Confidentiality, Integrity, And Availability. Achieving the goal of information security protections—ensuring that the organization can perform its mission or critical functions—requires managing risks to confidentiality, integrity, and availability. These three conditions are so universally emphasized in information security definitions that they have been dubbed the "CIA triad."

Confidentiality means that information is accessed and disclosed only as authorized.

Confidentiality means that information is accessed and disclosed only as authorized (US. Committee 17). Whether a breach of confidentiality is as limited as the disclosure of information about one student to one unauthorized person or as extensive as the release of an entire data set on the Internet, every breach must be addressed because it exposes a security weakness that could be exploited. Breaches of confidentiality can lead to embarrassment, harassment or bullying, identity theft, or a loss of public trust in government.

Integrity means that information is modified or deleted only as authorized, and that non-repudiation and authenticity are assured.

Integrity means that information is modified or deleted only as authorized (US. Committee 38). Inadequate protection of data integrity could allow students to change their grades or allow employees or contractors to change data accidentally or deliberately, for fraudulent purposes.

Availability means that authorized users have timely and reliable access to information and systems.

Availability means that authorized users have timely and reliable access to information and systems (US. Committee 6). This is important given the billions of dollars that have been invested in federal and state information systems, which were deemed essential for accurate, prompt, and efficient administration of government services. If an attack on a system makes it unusable, tasks that depend on the system are delayed or carried out in some other way. This is not only disruptive but it also leads to security risks if frustrated users resort to less secure methods for completing a task. For example, when unavailability of the student information system kept school personnel from entering students' personal information through a secure connection to the system, some personnel have sent the changes through email, which is not secure (Lykins).

Other aspects of security include accountability, compliance, and ensuring the authenticity of those logging into a system.

Many other conditions are implicit within the CIA triad, including accountability, compliance, and ensuring the authenticity of those logging into a system.

Logical, Physical, And Managerial Security. To avoid confusion when discussing security, experts distinguish three categories:

- Logical security encompasses solutions involving software and hardware, such as antivirus software and firewalls. Many people think that these, alone, constitute information security.
- Physical aspects of information security include placing essential equipment behind locked doors and shredding paper or CDs that contain sensitive information.
- Managerial security, which is no less essential than the others, includes security planning, written policies, compliance monitoring, and training.

Data ownership, use, and control are important considerations, especially when outside entities collect or store education data.

Data Ownership, Use, And Control. The ownership, use, and control of data are especially important to consider when outside contractors store information on their own systems, sometimes mingled with their own content, such as proprietary assessments.

Educators often fail to consider data ownership, use, and control until a problem arises. For example, several companies that surveyed students at school about their career interests were fined by the Federal Trade Commission because, instead of sharing the information only with colleges, the companies sold the students' information for non-education-related marketing purposes (Golden; US. Federal. "Student"). In 2011, two US congressmen introduced a bill to limit the ability of ACT Inc. and the College Board to sell students' personal information collected in the course of administering the ACT and SAT exams (Hoover).

Schools are also required to protect students from risks associated with using the Internet, such as inappropriate content, online predators, and cyberbullying.

Protecting Students From Cyber Risks. Most security controls protect data and systems from users. However, schools are also required to protect students from risks associated with using the Internet, such as inappropriate content, online predators, and cyberbullying. The laws that mandate these protections are discussed later in this chapter.

Governance

Governance means that senior leadership provides strategic direction and ensures that objectives are achieved, risks are managed appropriately, and resources are used responsibly. Governance must be sufficiently flexible and agile to balance security with other critical goals.

Governance is the set of responsibilities and practices that senior leadership exercises in order to provide strategic direction and to ensure that objectives are achieved, risks are managed appropriately, and resources are used responsibly (ISACA. *Information*). However, IT security governance should not merely impose extra paperwork and delays; it must be sufficiently flexible and agile to balance security with other critical goals (Berson). A key role of governance is to change attitudes and behaviors about security, with top leadership saying often that security is important and requiring a comprehensive security assurance program, with monitoring and continuous improvement.

Information That Requires Extra Protection

Because systems are interconnected, no system should be without security protections. Extra protection is needed for some types of data.

Because information systems are increasingly interconnected, no system should be without security protections. However, extra protections should be in place to ensure the confidentiality, integrity, and availability of the personal and performance information of students and employees, financial information, and proprietary information. These are described and discussed in more detail in Appendix A.

Legal Obligations To Protect Confidential Information

A number of federal and state laws protect students' personal information, but Kentucky is one of only four states without legislation requiring notification of security breaches.

A number of federal and state laws require educational institutions to protect the privacy of students' personal information. These laws are detailed in Appendix B.

However, Kentucky lacks important legislation to require notification of security breaches. Although these laws may or may not prevent identity theft, there is a consensus that they do help improve security planning by increasing the availability of information about the nature and frequency of security breaches (Natl.). Security notification laws have been enacted in 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin

Islands. However, a limitation of many of these laws is that they cover only electronic forms of information; they do not require notifications when personal information is disclosed on paper (Privacy. Prevent). In recent years, efforts have been made to enact one federal law to ensure uniformity across states.

Recommendation 1.1

Recommendation 1.1

To improve the availability of information for security planning purposes, the General Assembly should consider legislation requiring notification of all nontrivial data security breaches, whether data are in electronic or paper form.

Kentucky law requiring careful disposal of materials containing personally identifiable information refers only to businesses, not to governmental or not-for-profit organizations. There are policies, procedures, and guidelines for state and local government, though these have less strength than statutes.

Another important piece of legislation concerns proper data disposal, such as the shredding of paper documents and the removal of files from discarded computers. Kentucky is among 29 states with laws that require careful disposal of materials containing personally identifiable information. However, the statute refers only to businesses, not to governmental or not-for-profit organizations (KRS 365.725; Natl. Conference. Data). The Kentucky Department for Libraries and Archives and COT offer state and local government agencies guidelines, policies, and procedures for safe disposal (Commonwealth. Commonwealth Office. *Sanitization*; Commonwealth. Dept. for Libraries and Archives. *Destruction*). However, these documents do not have the force that a statute would have.

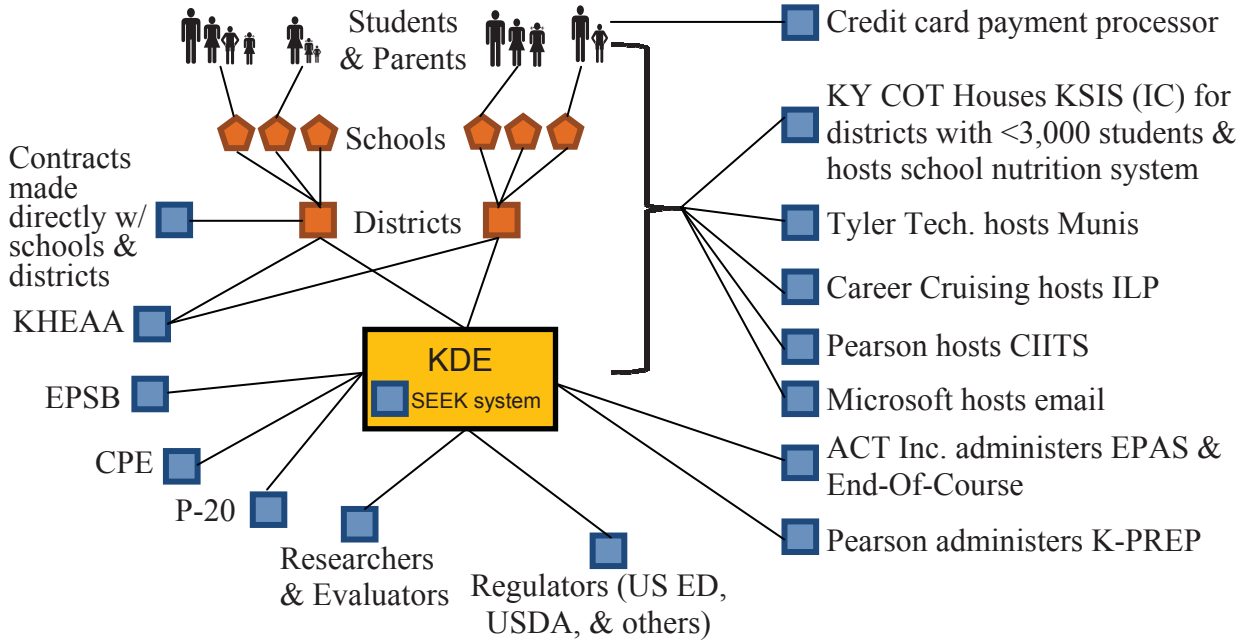
Key P-12 Education Information Systems

Nearly every instructional and administrative activity in Kentucky is involved in some way with a complex collection of interconnected systems. Data and systems located out of state offer greater protection from disaster but more potential risks to confidentiality.

Nearly every instructional and administrative activity in Kentucky involves some type of information technology. Figure 1.A illustrates the complexities of Kentucky's interconnected P-12 information systems. The bracket toward the right of the figure indicates which systems are shared across parents, schools, districts, and KDE. Listed on the right-hand side of the figure are KDE contractors that house (provide physical space) or host (house, operate, and maintain) data and systems. Most hosts are located outside of Kentucky and accessed using the Internet; such dispersed locations reduce the risk that a localized disaster will disable or destroy systems, but the dispersal can increase risks to confidentiality.

The following section briefly describes several of Kentucky's major K-12 information systems. More details are provided in Appendix C.

Figure 1.A
Collection, Storage, Access, And Transmission Of Sensitive P-12 Data
By Kentucky Educational Organizations And Contractors



Notes: KDE = Kentucky Department of Education; SEEK = Support Education Excellence in Kentucky; COT = Commonwealth Office of Technology; KSIS (IC) = Kentucky Student Information System (Infinite Campus); Munis = the financial management system used by Kentucky districts; ILP = Individual Learning Plan; CIITS = Continuous Instructional Improvement Technology System; EPAS = Educational Planning and Assessment System; K-PREP = Kentucky Performance Rating for Educational Progress; US ED = US Department of Education; USDA = US Department of Agriculture; P-20 = Kentucky's consortium for integrating data from preschool through graduate school; CPE = Council on Postsecondary Education; EPSB = Education Professional Standards Board; KHEAA = Kentucky Higher Education Assistance Authority.
Source: Staff compilation.

Student Information System

Kentucky's student information system (Infinite Campus, usually referred to as IC) contains data on all Kentucky public school students as well as data on teachers, courses, transportation, and schools. Some information is personal and confidential.

Kentucky's student information system—usually referred to by the contractor's name, Infinite Campus or IC—contains data on all Kentucky public school students as well as data on teachers, courses, transportation, and schools. Larger districts have on-site IC servers[1] while smaller districts use servers that are centrally housed at a secure data center owned and operated by COT.

For each student, IC contains the Social Security number, date of birth, home address, parent/guardian contact information, health conditions and disabilities, participation in educational and social programs (such as subsidized lunches and Medicaid), disruptive

[1] A server is a computer and software dedicated to providing services, such as access to data, to other computers in a network.

behaviors and disciplinary actions, course grades, test scores, and student locker combinations (Commonwealth. Dept. of Educ. *2011-12*).

Parents, students, teachers, administrators, and staff have various levels of access to IC.

Parents and students can view class schedules, attendance, and grades. Teachers use the system for recording students' grades and sending notices to parents and students. Administrators and staff use IC as a central location for recording and looking up information; coordinating services and programs; generating transcripts; and producing and sending numerous reports required to comply with state and federal regulations.

Munis Financial And Human Resource Management Information System

The Munis financial and human resource management system contains individual-level employee data that require confidentiality protections and aggregate or publicly available data that do not need confidentiality protections. All Munis data need integrity and availability protections. In a "software-as-a-service" arrangement, a contractor owns and manages Munis equipment and software, and districts access data through secure Internet connections for a fee. This arrangement is referred to as being in the "cloud."

To promote statewide consistency of financial information, all Kentucky districts use the Munis financial and human resource management system. Munis contains Social Security numbers and other personal and employment data, which require confidentiality protections. Its aggregate-level and publicly available data do not need confidentiality protections. However, all Munis data need integrity and availability protections.

Administrators and staff use Munis for record-keeping, budgeting, payroll, accounts payable and receivable, management of fixed assets, and a wide array of financial reporting.

In a "software-as-a-service" arrangement, a Dallas, Texas-based contractor owns and manages system equipment and software, and districts access data through secure Internet connections for a fee. This arrangement is referred to as being in the "cloud."

Support Education Excellence In Kentucky System

KDE developed and maintains the system for Support Education Excellence in Kentucky (SEEK), the formula used for allocating state funds to school districts.

Support Education Excellence in Kentucky (SEEK) is a funding formula used for allocating state funds to local school districts. The system used for storing the necessary input data and making calculations was developed by KDE.

Continuous Instructional Improvement Technology System

When complete, the Continuous Instructional Improvement Technology System (CIITS) will connect a wide array of curriculum, instruction, student, and teacher data.

The Continuous Instructional Improvement Technology System (CIITS) is a partially completed system that will eventually connect academic standards, electronic and multimedia instructional resources, curriculum, formative assessments,

instruction, and professional learning and evaluation of teachers and principals in one place (Commonwealth. Dept. of Educ. Continuous).

Once all components of CIITS have been implemented, CIITS will provide access to the individual student demographic, achievement, behavior, and program participation data contained in IC. In the future, CIITS will also contain teacher evaluation and professional development data.

Teachers use CIITS to access Kentucky's academic standards along with instructional resources for teaching those standards. Teachers may also share instructional resources they have designed. There are tools for scheduling and planning lessons and for creating and administering tests to students. Future phases of the project will support teacher and leader effectiveness and professional development.

Individual Learning Plan

The Individual Learning Plan (ILP) is a contractor-owned Web-based tool that helps students establish and work toward college and career goals.

The Individual Learning Plan (ILP) is a web-based tool created and hosted by Career Cruising to help students establish and work toward their postsecondary studies and career goals. Participation in the ILP is mandatory for students in grades 6 through 12 (Commonwealth. Dept. of Educ. ILP; Commonwealth. Dept. of Educ.).

The ILP contains much of the individual student demographic and achievement data contained in IC, plus career aptitude and interest test results and material that students provide about their career goals. Students can use the ILP to plan for their career, education, and life goals. Parents and guardians have access to the ILP. In addition, students can invite anyone within or outside of the system to view and comment on their information.

School Food Service Systems

The Child Nutrition Information and Payment System manages information about food service programs. Because the system stores only aggregate information, confidentiality is not an issue, but integrity and availability must be protected.

Child Nutrition Information And Payment System. The Child Nutrition Information and Payment System (CNIPS) manages information about food service programs. Because CNIPS stores only aggregate information, confidentiality is not an issue, but integrity and availability are important. The Division of School and Community Nutrition within KDE uses CNIPS to manage and reimburse over 1,000 food service providers.

Food service providers use CNIPS to file applications and submit claims to be reimbursed for the free and reduced-price lunches they provide.

"Point of service" systems in places where students obtain school lunches contain free and reduced-price lunch eligibility information, which the federal government considers highly confidential.

Point Of Service Systems. Eligibility for free or reduced-price lunches, which the federal government considers highly confidential information, is stored in "point of service" systems located at each site where children receive lunches. Food service providers use point of service systems to manage transactions and compile data to be reported, such as the number of lunches served.

Email And Communications Systems

Kentucky schools and districts use a free service called Live@edu, created and hosted by Microsoft. It provides free email and tools students and educators use for sharing calendars, online storage, and online collaboration space.

Kentucky's schools and districts use a free email system called Live@edu, which is created and hosted by Microsoft. In addition to providing free email service, Live@edu offers a suite of tools that allow students and educators to share calendars, online storage, and online collaboration space. By the end of 2012, Microsoft will transition its clients from Live@edu to its enhanced service called Office 365.

Security Threats And Protections

Security efforts should be driven by risk assessments and analyses of specific threats.

Security efforts should be driven by risk assessments and analyses of threats, which are defined as circumstances or events that

- involve the unauthorized access, destruction, disclosure, or modification of information or the denial of service of systems; and
- have the potential to adversely impact the organization (such as its operations, assets, reputation, or assets), individuals, or other organizations (US. Committee 75).

A common myth is that security is solely the job of IT departments, and that most security protections are highly technical. In reality, criminals increasingly target the "weakest link": people. This is especially true in education because students are less wary.

A common myth is that security assurance is solely the job of IT departments and that most security protections are highly technical. In reality, instead of targeting system software and hardware with technical attacks, cyber criminals are increasingly targeting the "weakest link" in security—people. For example, criminals are increasingly skilled at tricking users into clicking on email links that run malicious software. Such "social engineering" threats can bypass even the most sophisticated and expensive security technology. Insiders—those authorized to use systems—may cause more security issues than those attempting to gain unauthorized access. This is especially true in educational organizations, because students are less wary than the typical computer user. A recent study found that although young computer

users were more confident in their knowledge of security, they took more security risks and had more security problems than older users (Dimensional). The most important protections against social engineering threats are policies, procedures, training, and frequent awareness campaigns.

Security threats may be inside or outside the organization; accidental or deliberate; minor or extensive; and related to technology, physical access, or social manipulation.

Security threats come from inside or outside the organization, may be accidental or deliberate, may be minor or extensive and destructive, and may involve technology, physical access, or social manipulation. Appendix D describes some major types of threats and corresponding protections.

Estimating the probability and potential severity of threats is difficult because many breaches go undetected or unreported. Even when breaches are reported, there is no central agency to receive and analyze reports.

Ensuring sufficient security protections requires estimating the probability and potential severity of security risks. Yet this is not an easy task because security experts believe that many breaches go undetected or unreported. Even when breaches are reported, no single central agency receives and analyzes the reports. Depending on the circumstances, incidents may be reported to the local police department, the state attorney general's office, the Federal Bureau of Investigation, the Securities and Exchange Commission, the Federal Trade Commission, the Federal Communications Commission, the Social Security Administration, or other agencies.

Examples Of Education Data Security Breaches In Kentucky

Kentucky's schools and districts have experienced security breaches in recent years.

While public notice of security breaches is rare, there have been a few publicly reported instances in Kentucky involving elementary and secondary education records. Some of the incidents that have been made public are described below.

- In 2006, two high school students and one former student who gained unauthorized access to Jefferson County Public Schools' information system changed grade and attendance data and created a website on the system where they posted answers to tests (Harvey).
- In 2009, an employee of Bullitt County Public Schools employee accidentally sent an email message to about 1,800 school district employees that included the names and Social Security numbers of 676 employees. The email was a reminder to complete the district's open-enrollment process for health insurance (Privacy. Chronology).
- Also in 2009, someone erased both current and backup data on the website of the Graves County High School athletic department. The contractor hosting the website temporarily shut down all school websites it was hosting. Graves County had to piece together the data from several sources (WBKO).

- In 2011, approximately 6,500 ACT Explore test results for 8th-graders were mailed to incorrect addresses. The breach was discovered when parents began calling the district. Parents were asked to shred the tests. The exact cause of the mailing error is unknown (Privacy. Chronology).
- In April 2012, a Jessamine County student volunteering in the District Technology Office stole and used the password of a system engineer to view grades and other information without authorization (Young; Adams).

The Information Security Assurance Process

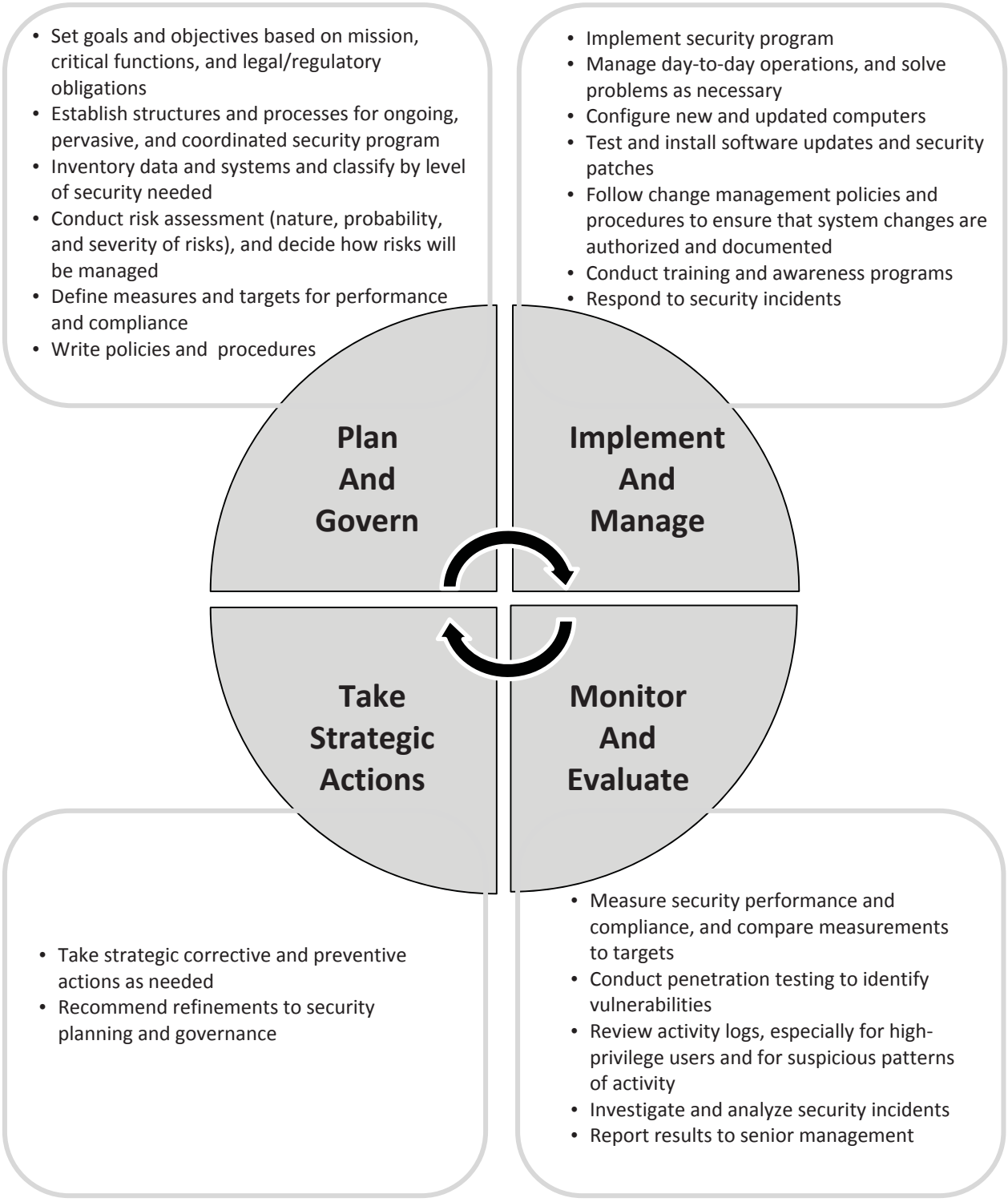
Every organization needs a security program that is ongoing, actively supported by senior leadership, pervasive, and well-coordinated. For continuous improvement, the program should cycle through four phases:
- Plan and govern
- Implement and manage
- Monitor and evaluate
- Take strategic actions

To combat numerous, constantly evolving threats to security, every organization needs a security assurance program that is ongoing, actively supported by senior leadership, pervasive throughout the organization, and well coordinated to avoid gaps. As Figure 1.B illustrates, organizations should strive for continuous improvement by repeatedly cycling through four phases:
- Plan and govern
- Implement and manage
- Monitor and evaluate
- Take strategic actions (US. Dept. of Homeland. *Essential*; ISACA. *Cobit 5 for*; ISO. *ISO/IEC 27000*)

Most organizations are struggling to progress from a tactical and compliance-driven process to a strategic risk-driven process. With most efforts concentrated in the "implement and manage" phase, IT staff work harder, with less lasting effect than if efforts were more balanced across all phases.

Security experts find that most organizations are still struggling to progress from a tactical and compliance-driven process to a strategic process based on analysis of risks. With most efforts concentrated in the "implement and manage" phase of the program cycle, IT staff work harder, with less lasting effect, than they would if efforts were more balanced across all phases of the security assurance process (Oltsik).

Figure 1.B
Security Assurance Process



Sources: Staff compilation based on US. Dept. of Homeland. *Essential*; ISACA. *Cobit 5 for*; ISO. *ISO/IEC 27000*.

This report focuses most attention on planning and governance for three reasons:
- This phase is critical to all the others.
- Deficiencies have been found in KDE's planning and governance.
- Few of Kentucky's education systems have been audited for security.

This report focuses most attention on the plan and govern phase of the process, for three reasons:

- Effective planning and governance shape the blueprint that is critical for all other phases; without this blueprint, even a perfectly secure environment would not stay that way for long.
- Several reviews and audits in recent years have found deficiencies in KDE's IT planning and governance (Commonwealth. Auditor. *Report*; Gartner).
- Few devices used for Kentucky's education systems are regularly audited for security, and OEA had neither the mandate nor the expertise to conduct such audits.

Chapter 2

Governance Of Kentucky's P-12 Education Data Security

Overview

Good governance ensures a sustained commitment and a comprehensive, well-coordinated strategy that is actively endorsed by senior leadership and developed with input from all areas of the organization. Governance is needed not only within individual organizations but also across organizations that share data and systems.

Good governance ensures a sustained commitment and a comprehensive, well-coordinated strategy to avoid security gaps and to keep up with evolving threats, technologies, and organizational structures. The security strategy must be actively endorsed by senior leadership and developed with input from all areas of the organization. All too often security assurance is an isolated duty for one unit within an IT department. Instead, it should be an integral part of IT governance in general, which in turn should be an integral part of the strategic governance of the organization.

Although the need for governance is often discussed in terms of the internal operations of one organization, it also extends across organizations that share data and systems, such as Kentucky's state and local education organizations and state government in general.

An assortment of legislation and agencies at the federal, state, and local levels impact the governance of Kentucky's education information security. Some responsibilities are scattered, and some efforts are not coordinated across agencies.

An assortment of legislation and agencies at the federal, state, and local levels have an impact on the governance of Kentucky's education information security. Responsibilities for some aspects of security are scattered across agencies. It appears that at least some agencies do not coordinate their security efforts. For example, at the federal level, security advice and checklists offered to states by the US Department of Education's Privacy Technical Assistance Center make little use of information from the federal government's leading authority on security, the National Institute for Standards and Technology.

Security experts find governance to be one of the weakest aspects of security in most organizations; as a consequence, security protections tend to be piecemeal and reactive, rather than proactive, with no comprehensive strategy to ensure the coverage of all gaps and continuous improvement. It appears that the organizations responsible for Kentucky's education security are no exceptions.

State and local governance of education information security are discussed below. A full discussion of security governance at the federal level is beyond the scope of this report.

Governance At The State Level

Some structures in Kentucky's executive branch may change as a result of an executive order issued by Governor Steve Beshear on September 24, 2012.

This section of the report discusses governance structures that existed through December 2012. Some structures in Kentucky's executive branch may change as a result of an executive order issued by Governor Steve Beshear on September 24, 2012. The order included an "IT infrastructure initiative," which will entail

- creating a Technology Advisory Council to improve coordination, accountability, and oversight of information technology across the executive branch;
- hiring a new chief information officer and elevating the position to the Governor's Executive Cabinet; and
- consolidating IT infrastructure services and associated support staff under the new chief information officer.

IT infrastructure services include

- computing equipment;
- server, storage, network, and desktop support;
- telephony;
- IT facilities and enterprise-level shared systems;
- IT security, disaster recovery, and business continuity;
- database administration;
- software licensing and related planning; and
- administration, procurement, and asset management.

The consolidation plan is intended to save money, reduce the risk of system failure, and lessen the number of privacy and security breaches while positioning the commonwealth to take advantage of emerging technologies and sourcing alternatives (Commonwealth. Finance). At the time of this report, no information was available as to how the IT infrastructure initiative would affect KDE, if at all.

Commonwealth Office Of Technology

The Commonwealth Office of Technology (COT) is meant to provide the commonwealth's single point of contact for all information technology matters. In addition to offering technical support and services, COT is responsible for overseeing and protecting state IT infrastructure.

The General Assembly established COT to provide, through its executive director,

> the Commonwealth's single point of contact and spokesperson for all matters related to information technology and resources, including policies, standard setting, deployment, strategic and tactical planning, acquisition, management, and operations (KRS 42.720 (1)).

In addition to offering technical support and services to all state agencies in the executive branch, COT is responsible for overseeing and protecting state IT infrastructure. Its roles and duties include

> [d]eveloping, implementing, and managing strategic information technology directions, standards, and enterprise architecture, including implementing necessary management processes to assure full compliance with those directions, standards, and architecture. This specifically includes but is not limited to directions, standards, and architecture related to the privacy and confidentiality of data collected and stored by state agencies (KRS 42.726(1)(d)).

The legislative and judicial branches and retirement systems are excluded from COT authority. School districts may also be outside of COT's authority.

The legislative and judicial branches, as well as the Kentucky Retirement System and Kentucky Teachers' Retirement System, are explicitly excluded from COT authority (KRS 42.728). As part of local governments, not part of the state's executive branch, school districts may be considered outside of COT's authority.

There are differences of opinion as to whether KDE is statutorily required to comply with COT policies and procedures.

Unclear Authority Regarding Education Technology. Representatives from COT told OEA that they interpret COT-related statutes to mean that KDE, like all agencies in the executive branch, is required to comply with COT policies and procedures. Agencies may enact policies and procedures that are more stringent than COT's. However, if an agency wishes to have less stringent policies, it should request an exception, and COT will work with the agency to determine acceptable alternatives (LeMay). Because school districts are local government entities, COT is usually not involved with district-level systems, even though districts are interconnected by state IT infrastructure.

Representatives of KDE told OEA that they believe KDE is not subject to COT authority and therefore not required to follow COT policies and procedures, though KDE does follow some voluntarily. To support this position, KDE's representatives stated that KDE is only administratively attached to the Education and Workforce Development Cabinet and pointed out a number of statutes that give KDE authority for education technology, including KRS 156.010(1)(a), 156.670, 156.671, 156.675, 156.690, and 157.061. However, most of these statutes concern KDE's relationship with districts, not with COT. The one statute that does grant broad authority for education technology is KRS 156.670, which directs the now-defunct Council on Education Technology[1] to draft a 5-year education technology master plan and have the

[1] The Council on Education Technology was dissolved after the repeal of KRS 156.666, but the council is still mentioned in this and other statutes.

plan approved by the Kentucky Board of Education and the Legislative Research Commission. KRS 156.670 is discussed further in the section of this report on KDE.

A relationship has evolved that allows KDE to operate essentially independently of COT.

Based on OEA staff's numerous discussions with COT and KDE, it appears that, despite COT's apparent statutory authority, a relationship between the agencies has evolved that allows KDE to operate essentially independently.

School districts and KDE seem to underutilize COT resources, such as its multiple layers of security, policies and procedures, knowledge gained from purchasing and managing many systems, and experience with being audited and acting on recommendations from those audits.

COT Resources Available To State And Local Agencies. Irrespective of statutory authority, COT seems to be an underutilized resource for school districts and KDE.

- Multiple layers of physical and logical security are provided for state agencies that choose to locate their systems within COT's infrastructure, but KDE is not among the agencies that consolidated. In 2012, KDE did move some equipment to a secure COT facility, but it still has many systems outside of COT's multiple layers of defenses. This means they are also outside of COT's routine checks for compliance with COT policies.
- The extensive set of COT policies and procedures could also be a better-utilized resource when KDE and school districts are developing their own policies and procedures.
- Given its volume of purchases and central role in managing many systems, COT could provide advice about the costs and quality of some of the latest IT products to augment information that KDE and districts gather on their own. For example, KDE had outdated information about the cost and usability of software that encrypts data on laptops, and COT was able to provide new information (Couch; Thomas).
- School districts and KDE could also learn from COT's own experience with being audited and acting on recommendations from those audits. According to COT's chief information security officer, COT underwent three types of third-party reviews of security in 2012. One was a complimentary Cyber Resilience Review that COT requested from the US Office of Homeland Security. A second review, paid for by COT, was an assessment by a private firm that compared COT's information security controls to widely accepted national and international security standards. The third was a National Cyber Security Review developed by the Department of Homeland Security to identify the level of maturity and risk awareness of state and local government information security programs. The three reviews made similar recommendations for strengthening security, and COT is working to implement the recommended changes (LeMay).

Commonwealth Technology Council

The Commonwealth Technology Council, representing all state cabinets, meets monthly to help maximize the business value of IT; provide comments and recommendations on IT policy, direction, planning and legislation; identify opportunities and conduct joint planning for cross-agency cooperation; and provide stewardship for other state IT programs and projects.

The Commonwealth Technology Council, made up of IT representatives from each cabinet of Kentucky government, meets monthly to

- assist the commissioner of technology in targeting and delivering IT resources for maximum business value for the commonwealth;
- provide comments and recommendations on policy, direction, planning, and legislation;
- identify opportunities and conduct joint planning for shared services implementation, sourcing, investments, and cost recovery; and
- provide stewardship for other state IT programs and projects (Commonwealth. Commonwealth. About).

Enterprise Architecture And Standards Committee

The Enterprise Architecture and Standards Committee is involved in direction, standards, and reviewing requests for exceptions.

The Enterprise Architecture and Standards Committee defines computer and network architectural direction, maintains IT standards, recommends revisions or new standards to the COT commissioner, and reviews business case exceptions from agencies (Commonwealth. Commonwealth. Governance).

Auditor Of Public Accounts

The auditor of public accounts (APA) does not provide governance but provides guidance in conjunction with its annual statewide audits.

While the APA does not provide governance, per se, the agency does provide guidance in conjunction with its annual statewide audits. The APA is independent of the state's administrative departments so that it can provide for disinterested audits of the accounts, financial transactions, and performance of all spending agencies of the state (KRS 43.050).

The APA's annual audits, including tests of security on selected computers, focus on Munis and SEEK.

Since 2004, the APA has audited KDE's financial records and the financial computer systems in which those records are stored. The audits, which include tests of the security of selected computers, focus on the Munis financial and human resource system and SEEK.

It should be noted that annual statewide audits do not include school district computers. Although each district has a financial audit by a local certified public accountant, the standard protocol for these audits does not include examinations of IT controls.

Annual audits do not include non-financial systems such as the student information system, CIITS, ILP, and school district computers.

It should also be noted that, because these annual audits focus on state agency finances, they do not include nonfinancial systems even though these contain highly sensitive personal data. Reviews of KDE documents found one recent audit of IC by a private company, but no audits for CIITS and ILP.

Although agencies are required to cooperate with the audit process, there are no clear requirements as to how, or even whether, agencies must act on recommendations that accompany the APA's findings. Audits of KDE's financial information systems show some weaknesses persisting for several consecutive annual audits.

One audit is not sufficient to ensure security because new security issues can emerge at any time, and old issues quickly reemerge if there is no systematic process to prevent them. Although KRS 43.990 requires agencies to cooperate with the audit process, no statutory language spells out how, or even whether, agencies must act on recommendations that accompany the APA's findings. Audits of KDE show some material weaknesses persisting for several consecutive years. One example is that software patches to correct security problems are not installed in a timely fashion; research shows this to be one of the top preventable causes of security breaches (Verizon). In these cases, KDE's written responses to the APA usually indicate that KDE is still working to correct the problem or that the recommendations are not feasible within budgetary, staffing, and technology constraints. Appendix F provides the APA's IT-related findings for KDE in fiscal year 2011.

While agreeing that security audits are advisable, KDE said that the cost of audits would far exceed the available budget.

While agreeing that security audits are advisable, KDE stated that good audits are very expensive—approximately $100,000 per audit—and that such annual costs are not feasible in the current budget climate.

Free "cyber resilience" reviews by the US Department of Homeland Security could offer some insights, though far less than true audits.

According to COT, the US Department of Homeland Security conducts free Cyber Resilience Reviews, which offer some insights, though far less than a true security audit (LeMay).

Office of Procurement Services

The Office of Procurement Services (OPS) within the Finance and Administration Cabinet oversees compliance with procurement statutes and regulations.

The Office of Procurement Services, an agency within the Finance and Administration Cabinet, is responsible for overseeing compliance with procurement statutes and regulations, an area of increasing importance given the large and growing number of contractors involved with Kentucky's education data.

For IT products and services, all agencies are supposed to use a standard requests for proposals (RFP) template and follow a process that includes review by OPS and COT.

For most IT products and services, OPS and COT work together to maintain a template for all agencies to use for creating requests for proposals (RFP). When an agency wants to make a purchase, OPS assigns a buyer in its office who sends the agency a template for drafting the RFP. The buyer reviews the agency's draft RFP for compliance with state procurement regulations and sends it to COT

for technical review. If COT has any concerns about the RFP, it informs OPS, which works with the agency to address the concerns. Then OPS sends out the RFP, receives responses, oversees the agency's evaluations of responses, helps to negotiate the contract, and drafts the contract for the agency and contractor to sign. The contract does not include new materials; instead, it pulls selected information from the RFP and references the RFP. At renewal time, OPS notifies the agency it is time to renew and reissues the contract with changed dates, but the contract is not usually reviewed again unless terms have changed (Williams. Telephone).

The RFP template does not address website end user agreements and terms of use, although these often provide important information about privacy and data ownership.

The RFP template does not request website end user agreements and terms of use, even though these often contain important information about privacy and data ownership. According to OPS, it would not be advisable to add such matters to the RFP template because a website is not a feature of most IT products and services. However, this practice may be changing as IT products and services increasingly use the Internet and Web interfaces to provide easy access to systems.

Although it is not a perfect process, Kentucky's precontract reviews by OPS and COT help state agencies avoid some security issues. However, as will be discussed later in this report, this review process does not extend to school districts. Also, if IT services are obtained using personal services contracts, there is less review by OPS and COT.

Kentucky Department For Libraries And Archives

The Kentucky Department for Libraries and Archives sets data retention schedules for data collected and stored by state agencies and public school districts. Most data are kept for 3 years.

The Kentucky Department for Libraries and Archives sets data retention schedules for data collected and stored by state agencies, including KDE, and local government agencies, including public school districts. The retention schedules detail, for each type of data the agency collects and stores, how long the data should be retained and what procedures should be followed for disposing of the data. Retention schedules are approved by the State Archives and Records Commission and posted online. Typically, data are kept between 3 and 5 years and then destroyed after any required audit has been completed. However, many types of data are kept indefinitely (Commonwealth. Dept. for Libraries. *Public* and *Department*).

P-20 Data Collaborative

The P-20 Data Collaborative gathers data into a single longitudinal data warehouse. Data are kept indefinitely. However, Social Security numbers and student IDs are replaced by identifiers that cannot be used outside of P-20, and the database is within COT's multiple layers of security.

The P-20 Data Collaborative is responsible for gathering data from Kentucky's education and workforce agencies into a single longitudinal data warehouse. P-20 keeps data for more than 3 years because it is charged with building a longitudinal database to support education research, evaluation, and innovation. However, as soon as P-20 obtains data from agencies, it removes any Social Security numbers and student IDs and replaces them with an identifier that is known only to the P-20 Data collaborative so that the data cannot be used by others for identifying individuals. The database is kept within COT's multiple layers of security defenses, in addition to security protections integrated into the database system itself (McGrew).

Kentucky Department Of Education

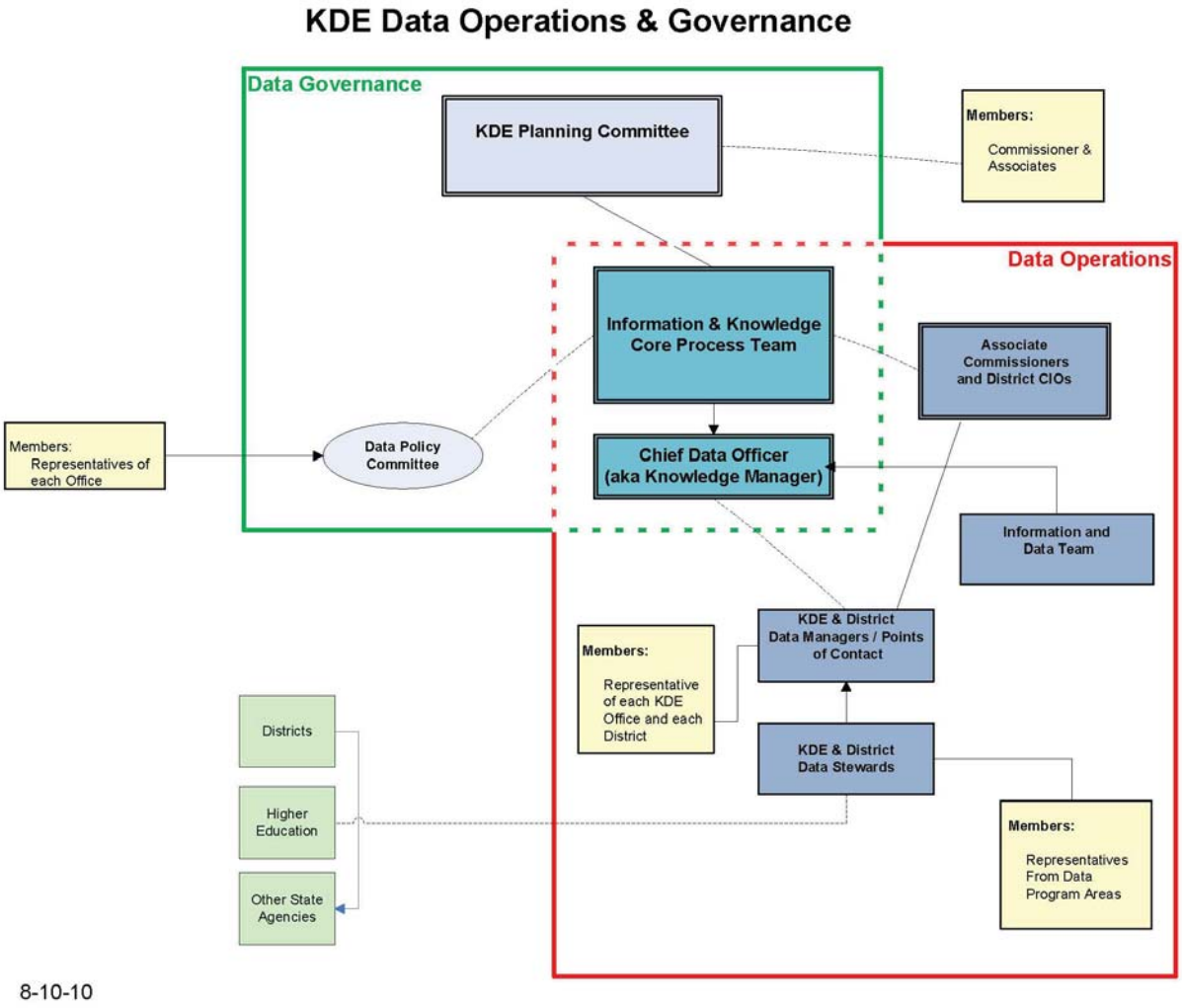
As the state agency primarily responsible for P-12 education, KDE maintains the largest amount of state-level P-12 education data. Because data security should be an integral part of overall IT governance, OEA requested information about KDE's IT governance. In response to this request, KDE provided the diagram shown in Figure 2.A. As the figure shows, the ultimate level of decision-making authority is the KDE Planning Committee, made up of the commissioner of education and heads of KDE's major business units.

The Data Policy Committee develops policies for the KDE Planning Committee's approval.

Governance Structures Within KDE. According to a 2009 document titled *KDE Data Governance*, the Data Policy Committee develops policies for the KDE Planning Committee's approval

> including, but not limited to steps to be followed for data policy development, roles and responsibilities, committees and committee charters that collectively describe how decisions are made, monitored and enforced regarding the management of KDE.

Figure 2.A
Kentucky Department Of Education Data Operations And Governance Structures



Notes: This figure shows the diagram as it was provided by KDE to OEA in 2012. In subsequent interviews, KDE mentioned some updates that need to be made, including the addition of a security program manager and the Technology Planning Council.
Source: Commonwealth. Dept. of Ed. *KDE Data Operations & Governance*.

Although a document titled *KDE Data Governance* does not contain detailed policies and makes no mention of KDE's security program manager, it does describe several roles.

Although the 2009 *KDE Data Governance* document does not contain or reference detailed policies, it does describe the following roles:

- Data steward, the owner of a data element or data field responsible for hands-on work related to data at KDE
- Data manager, a representative of an office within KDE who works in conjunction with the Data Policy Committee to coordinate the work of data stewards and use of data
- Chief data officer, responsible for training data managers and data stewards on data governance policies and processes, coordinating a "cross-office relationship" among data

managers and data stewards, and working with the Data Policy Committee to monitor the development of an enterprise-wide data dictionary, data collections, and data reporting events
- Office of Legal, Legislative and Communications Services, responsible for review of data policies as they relate to KDE statutes and regulations, language clarity, dissemination, and storage of policies
- Policy sponsor/associate commissioner, responsible for providing oversight in the development of data policies affecting appropriate program areas and for providing resources if the policy is approved for implementation (Commonwealth. Dept. of Educ. *KDE Data Governance*)

In 2011, KDE appointed a security program manager who is part of KDE's governance team. The *KDE Data Governance* document and the governance diagram should be updated to reflect these and any other changes.

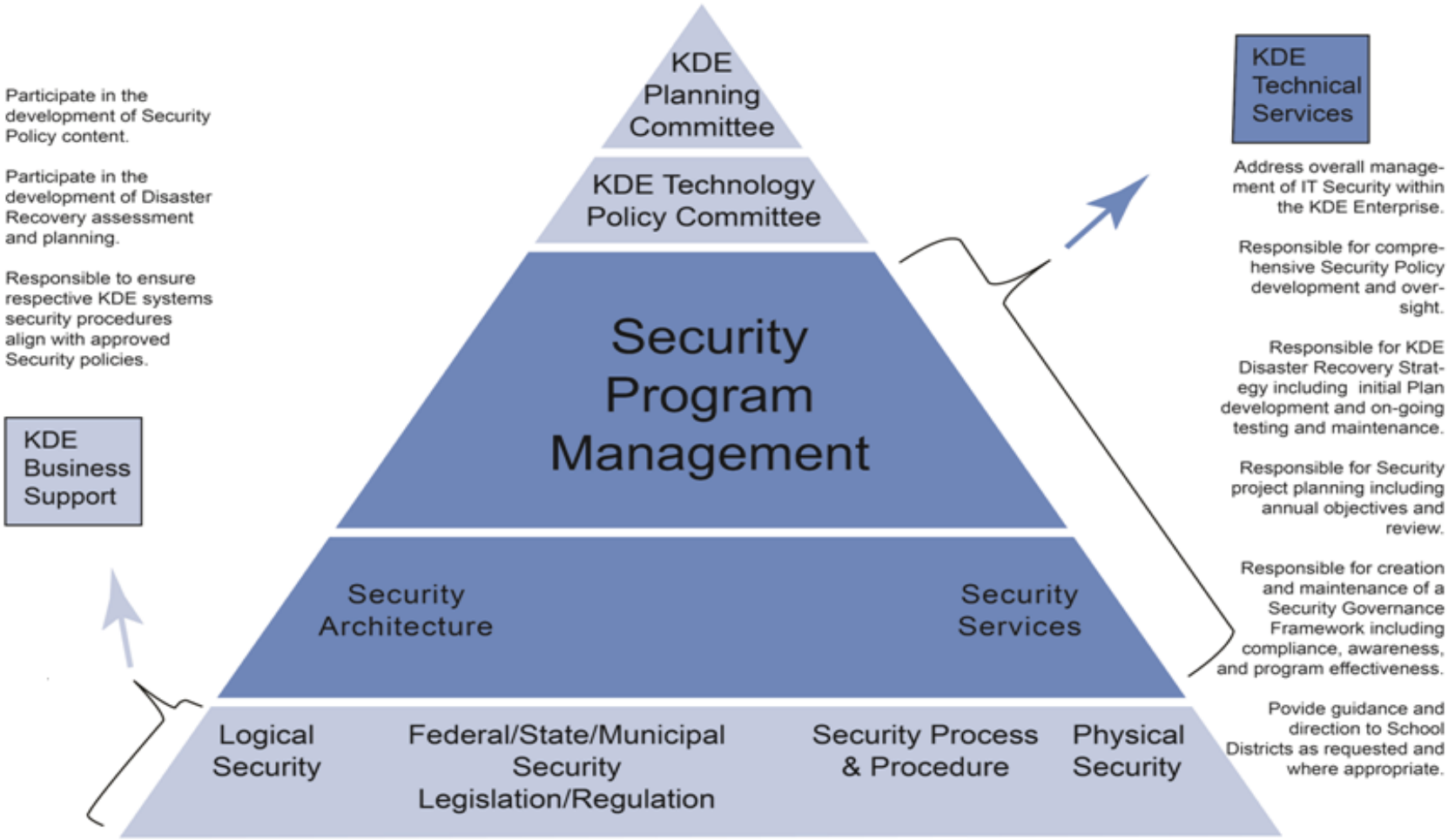
According to the APA, although KDE has been making gradual improvements in the way it governs IT, KDE still lacks a comprehensive IT policy to ensure adequate oversight. Each business unit is responsible for establishing and enforcing its own policies, including how to respond to security breaches.

According to the APA, although KDE has made gradual improvements to IT governance, it still lacks a comprehensive policy to ensure adequate oversight. This control deficiency has been found in the past six annual audits (Commonwealth. Auditor. *Agency*). In the latest audit (FY 2011), the APA found that each KDE business unit is still responsible for establishing and enforcing its own IT policies and procedures, but leaders of at least some units admitted to the APA that they have not yet established and implemented formal IT control policies, including how each unit will respond if there is a security breach.

The 5-year master plan, which is meant to guide all aspects of education technology, does not address security in much detail. A one-page diagram provided to describe KDE's security program was out of date and not entirely consistent with KDE's governance diagram, because the two diagrams were created in different areas of KDE.

Security Plan. A written security plan is important for ensuring that all levels and divisions of an organization have a shared understanding of the roles and responsibilities for security. Although KRS 156.670 requires a 5-year master plan to guide all aspects of education technology, the statute does not require, and the master plan does not address, security in much detail (Commonwealth. Dept. of Educ. KETS). When asked for its security plan, KDE provided a one-page diagram, shown in Figure 2.B.

Figure 2.B
Kentucky Department Of Education's Security Program Framework



Notes: This figure shows the diagram provided by KDE to OEA in 2012. However, in interviews, KDE mentioned a number of updates that need to be made: The KDE Technology Policy Committee no longer exists; its duties have been assumed by the Technology Planning Council. The Information and Knowledge Core Process Team now reviews recommendations made by the Technology Planning Council before the recommendations are sent to the KDE Planning Committee for approval. KDE created a Security Program Manager position in 2011.
Source: Commonwealth. Kentucky Department of Education. *KDE Security Program Framewor*k.

While Figure 2.B shows the diagram as it was provided by KDE to OEA in 2012, KDE mentioned a number of updates that need to be made to the diagram. The KDE Technology Policy Committee no longer exists; its duties have been assumed by the Technology Planning Council. The Core Process Team now reviews recommendations made by the Technology Planning Council before the recommendations are sent to the KDE Planning Committee for approval. The diagram does not mention the Security Program Manager position created in 2011.

There appear to be some disconnects between KDE's data governance and security policies. The KDE Technology Planning Council is not shown in the governance diagram (Figure 2.A) and did not sign off on the *KDE Data Governance* document. The Data Policy Committee is in the governance diagram but not in the security diagram. A KDE representative explained that the governance and security diagrams were created by different people in different areas of KDE.

While KDE's one-page security diagram is convenient and informative, it does not provide sufficient information to serve as a security plan. An extensive review of the literature found plans ranging from 50 to 200 pages in length.

The target date for KDE's security plan is the end of 2012.

The security program manager at KDE has been working to develop a comprehensive security plan and hopes to complete the plan by the end of 2012.

The state Board of Education did not sign off on KDE's data governance document, is shown in neither the governance nor the security diagram, and has given little attention to privacy and security issues in its meetings and strategic plan.

Limited Board Involvement In Security Governance. The Kentucky Board of Education did not sign off on the *KDE Data Governance* document and is shown in neither the governance diagram nor the security program framework. A review of the board's strategic plan and agendas for meetings in 2011 and 2012 found little attention to privacy and security issues (Commonwealth. Dept. of Educ. Kentucky Board of Education Agenda and *Kentucky Board of Education Strategic*).

According to security experts, although boards should be involved in security governance and consider security in all technology decisions, most lack adequate understanding of security and fail to undertake critical governance activities.

According to security experts, boards should be involved in setting the overall goals, priorities, and general direction of security strategy. Security should be a consideration in all of the decisions boards make about technology. They should receive annual briefings about the state of information security (ISACA. *COBIT 5: A Business* and *COBIT 5 for Information Security*). Unfortunately, studies show that boards give too little consideration to information security when making decisions. A 2012 study found that most boards of directors lack an adequate

understanding of the links between IT risks and other risks to the organization. Most fail to undertake critical governance activities, such as assigning key privacy and security responsibilities and reviewing regular reports on IT risks and incidents (Carnegie. Software. *Governing*).

Security experts recommend that policies be written, updated regularly, and readily accessible. Compliance should be monitored, and there should be consequences for noncompliance, ranging from additional training to disciplinary action, depending on the circumstances.

Policies And Procedures. Security experts emphasize that spoken reminders are not sufficient to ensure that all system users in all locations follow security best practices; policies must be written, updated regularly, and readily accessible to employees, contractors, and other system users. Compliance should be monitored, and there should be consequences for noncompliance, ranging from additional training to disciplinary action depending on the circumstances.

The most important document is the acceptable use policy, which explains how employees, contractors, and others may use information and IT equipment. It should include rules for email, the Internet, and mobile devices. Increasingly, experts also recommend rules for the use of public cloud storage and social networking sites, such as Facebook or Twitter.

The most important security document is the acceptable use policy, which explains, in nontechnical language, how employees, contractors, and others may use information and IT equipment. This policy should include, but not be limited to, rules for the use of email, the Internet, and mobile devices (ISO. *ISO/IEC 27002*). Security experts are increasingly advocating that the acceptable use policy also include rules for use of public cloud storage (a service that allows users to save documents on a company's computers and access those documents using the Internet) and of social networking sites, such as Facebook or Twitter.

Not all KDE managers agree that they must follow COT policies and procedures. The policies and procedures that KDE wrote are missing some important elements, including a KDE-wide security breach response and an adequate disaster recovery plan.

Although COT provides policies and procedures for state agencies, representatives from KDE said that not all KDE managers agree they must follow COT policies and procedures. Instead, KDE has been writing its own policies and procedures, and some important elements are missing from KDE's set. For example, KDE needs a written policy that either prohibits the storage of confidential data on mobile devices or requires that confidential data be encrypted. The head of KDE's IT unit said that KDE has a verbal policy against storing confidential data on mobile devices (Couch). However, KDE's written acceptable use policy assumes the opposite, urging employees to safeguard KDE devices from loss or theft, to prevent unauthorized access to confidential data (Commonwealth. Dept. *Acceptable*). The KDE mobile device policy focuses solely on who is eligible to have KDE-owned mobile devices and who must pay the monthly bills (Commonwealth. Dept. of Educ. KDE *Mobile*).

Most critically, there is no agency-wide written plan for responding to security breaches, and there is an inadequate disaster recovery plan (Commonwealth. Auditor. *Report*, 2011). A review

of policy documents provided to OEA by KDE also found no policies for the use of public cloud storage or social networking sites, and no list or keyword index that would tell employees which policy documents exist.

The intranet for KDE employees provides the acceptable use policy, the access control policies, and the *KDE Data Governance* document. However, the access control policy posted on the intranet was out of date.

According to KDE's Human Resources unit, KDE posts three documents on its employee intranet for employees' ongoing reference:

- The acceptable use policy covers the acceptable use of email, texting, instant messaging, Internet access, and network storage.
- The access control policy addresses account/user names and strong passwords, and access (wireless, remote, and physical) to KDE networks.
- The *KDE Data Governance* document lists some, but not all, of the roles involved in governing data (Lang).

In reviewing these three documents, OEA determined that the access control policy posted on the employee intranet was out of date.

In contract negotiations, pricing and product features are the key considerations. Some contracts make little or no mention of security and privacy. Contractors are not required to prove they are maintaining adequate security. However, most contracts were created several years ago, before security was a prominent issue. In 2011, KDE began requiring contractors to sign a statement that they will comply with the Family Educational Rights and Privacy Act.

Contract Management. Although many contractors access and store students' and employees' personal information, KDE reports that security has not been a key consideration in contract negotiations; pricing and product features were the top priorities. Some contracts make little or no mention of security and privacy of students' and employees' personal data. Contractors are not required to provide the results of periodic audits or other proof that they are maintaining adequate security. However, KDE pointed out that most contracts had been created several years in the past, before security was a prominent issue, and were not required to be reviewed or changed on subsequent renewals. In 2011, KDE's Procurement branch began to require contractors to sign a statement that they will adhere to the Family Educational Rights and Privacy Act requirements (Stratton).

The ILP was purchased using a personal services contract, which requires less review by OPS and COT. The contract did not address data ownership and did not reference the end user agreement.

The contract between KDE and Career Cruising for the ILP was a personal services contract, such as those used for legal services, and such contracts require less review by OPS and COT. Perhaps as a consequence, the contract for the ILP did not address data ownership or the cost to have data returned in a usable form if KDE chooses a new vendor. The ILP's end user agreement was not mentioned in the contract.

The end user agreement, to which students tacitly agree by using the ILP, grants the contractor indefinite rights to use information from the student's ILP. It does not rule out publishing, sharing, or selling students' information. When contacted by OEA, the contractor agreed that the wording was inappropriate and promised to work with KDE to change it.

A potentially serious student privacy issue arose as a consequence of not reviewing the ILP website end user agreement and not addressing data ownership and privacy issues adequately. The ILP's "Portfolio End User Agreement," to which students tacitly agree by using the ILP, has a clause that grants the contractor a "non-exclusive, non-terminable, royalty-free, world-wide license" to the student's work. This means that the contractor could keep and use the student's ILP contents forever and use it in unspecified ways; the wording does not rule out publishing, sharing, or selling the student's information. There was no mention of this clause in any of the parent materials posted on KDE's or Career Cruising's websites. It is unclear whether this agreement would be valid for students under the age of 18, especially given that students are legally required to use the ILP (704 KAR 3:305).

When OEA asked the contractor for clarification, the CEO said that the clause was standard legal wording for this type of Web application but agreed that it was inappropriate for the ILP and promised to work with KDE to change it (McQuillen).

The feature that lets students give others access to their ILPs should be carefully managed, to safeguard students. There is some confusion as to whether this feature is enabled automatically or only if a parent grants written permission.

Another area that requires closer examination is the feature of the ILP that allows students to give others access to their ILP. Without safeguards, a trusting student might give access to an online predator or other person who wants to misuse the information. School districts can disable the "invite others" feature for all students or just for those whose parents request it to be disabled, but OEA found some confusion as to whether the feature is initially turned on or off. The KDE website states that the feature is enabled except for parents whose children opt out, but a form developed by KSBA and used by many districts states that the feature will not be enabled unless the parent opts in by returning the signed form (Commonwealth. Dept. of Educ. ILP).

Recommendation 2.1

Recommendation 2.1

The Kentucky Department of Education should work with districts to ensure clear and consistent policies regarding the Individual Learning Plan "invite others" feature and to ensure that students are adequately protected from potential misuse of the feature.

Because a single user can bypass many protections, people are called the "weakest link." Regular dedicated training sessions should explain policies in detail, including why they are important, and should include opportunities for questions and answers. Ongoing awareness campaigns should provide reminders in multiple ways and multiple locations.

Training And Awareness Programs. Of all the factors that impact security, people are widely regarded as the "weakest link." Even a sophisticated technological security protection can be compromised by a single system user clicking on a link in a spam email or using a password that is easy to guess. Therefore, regular training sessions should explain security policies and procedures in detail, including why they are important, and should include opportunities for questions and answers. Ongoing awareness campaigns should provide reminders in multiple ways and multiple locations to reinforce this training (US. Dept. of Comm. Natl. *Building*; Quagliata).

Current training is relatively limited, being confined to new employee orientation and annual performance reviews, when security is one of many topics covered. Employees are required to sign a form agreeing to comply with the acceptable use policy.

Security training for KDE employees is relatively limited, being confined to new employee orientation and annual performance reviews, when security is one of many topics covered. The initial one-on-one meeting with each new employee includes a discussion of the acceptable use policy. Annual performance reviews include a rating of the employee's adherence to the acceptable use policy. Employees are required to sign a form stating that they will comply with the acceptable use policy when they are first hired and again each year during the annual performance review (Lang).

In monthly webcasts to district IT professionals and others who choose to attend, KDE's IT unit uses news stories about security incidents to remind attendees of the importance of security.

Activities to raise awareness include monthly webcasts directed to district IT professionals, and attended by many others who choose to tune in. In these webcasts, security incidents in the news are used as "teachable moments" to remind attendees of the importance of security. The commissioner of education is considering the possibility of talking about security during regular communications with all district superintendents.

Although KDE is quick to correct problems found in annual APA audits, these audits check only a small fraction of equipment. The APA recommends stronger governance and a comprehensive security plan to ensure that problems are identified and fixed proactively.

Security Issues Identified In Audits. The Auditor has found security problems at KDE in each annual audit, with some problems recurring in multiple years (Commonwealth. Auditor. *Report*). To their credit, KDE staff are quick to correct problems found in annual audits. However, annual audits check only a small fraction of the equipment used for education information systems. Problems with equipment that is not audited may never be discovered and corrected. There are no systematic procedures, monitoring, and evaluation for identifying problems and fixing them proactively. Representatives in the APA's office believe that these problems could be addressed with stronger governance and a comprehensive security plan.

Building on the wealth of existing standards and guidelines, instead of developing policies from scratch, can save organizations time and money and reduce the risk of security gaps.

There is a wealth of formal standards and less formal guidelines available in the literature that Kentucky's educational organizations could adapt to their needs. Building on these established documents, instead of developing a security program from scratch, often helps organizations reduce the time, costs, and risk of leaving gaps in security. Some widely recognized standards and guidance are discussed in Appendix G.

District-Level Security Governance

Some important security protections are left to the discretion of each of Kentucky's 174 school districts. It is likely that some lack the necessary expertise and resources to ensure adequate security. Gaps in just one district's security could endanger many interconnected systems.

Some important security protections are left to the discretion of each of Kentucky's 174 individual school districts. Examples include strong password rules, security breach notifications, policies for mobile and personally owned devices, and acceptable use policies. It is likely that some districts lack the expertise and resources to create and manage an adequate security program. Gaps in just one district's security could introduce malicious software or other threats that could endanger not only that district's information systems but also the many systems through which districts and state agencies are interconnected.

Because security audits are not required, it is impossible to assess districts' security controls. Moreover, districts may share confidential data with contractors.

Because routine security audits in districts are not required, it is impossible to gauge the effectiveness of districts' security controls. Moreover, a district may enter into contracts for a wide variety of services that entail sharing confidential student data.

The Kentucky School Boards Association offers policies and procedures, but districts are free to modify or disregard the policies.

The KSBA offers some helpful policies and procedures for districts to use, but not all districts pay to use these services, and districts are free to modify or not use the KSBA policies and procedures.

KDE sets some standards for districts' software and hardware, but no specific security policies.

The uniformity of having all districts use the same financial management system and student information system has allowed KDE to mandate districts' software and hardware security standards, which are detailed in Appendix H. However, apart from giving districts best practices advice, KDE does not mandate specific security policies.

While KDE has traditionally stated that it lacks the authority to direct school districts on such issues as password requirements, in December 2012, KDE informed OEA that its position had changed. KDE stated that various statutes provide the authority to direct districts' security policies, including KRS 156.010(1)(a), 156.670, 156.671, 156.675, 156.690, and 157.061.

Recommendation 2.2

Recommendation 2.2

The Kentucky Department of Education should continue to provide guidance, policies, and best practices to enhance data security at the district and school levels. While districts should be able to make decisions in noncritical areas, the Kentucky Department of Education should require minimum standards for critical areas, including strong passwords, review of security issues in contracts for technology services, the use of personal and mobile devices, and other emerging security issues.

Lessons could be learned from looking at agencies that have similar challenges with dispersed locations and multiple levels of government. These include the Cabinet for Health and Family Services and the Transportation Cabinet.

When OEA asked COT and the APA whether other agencies might serve as useful examples, both credited the Cabinet for Health and Family Services with good security despite its size, complexity, and dispersed locations. Like KDE, the Cabinet for Health and Family Services has locations throughout the state and some systems outside of COT's multiple layers of security.

An example of the challenges encountered when coordinating security across state and local government boundaries can be observed in the ongoing work by COT and the Transportation Cabinet to implement the state's new vehicle information system, which is having an impact on every county clerk. Some IT contractors hired by county clerks inadvertently exposed some of the state's IT infrastructure; COT is currently working with the Transportation Cabinet and county clerks to ensure that county clerks have the system options they want, while ensuring security of the state's systems. It is proving to be a difficult task (LeMay).

New And Emerging Issues

Cloud Computing

With cloud computing, customers use a Web browser to access computer resources and applications that are owned and maintained by the cloud provider instead of going to the expense and effort of purchasing, installing, and maintaining their own computers and software. Perceived benefits include lower costs, less IT management burden, and flexible capacity.

With cloud computing, customers use a Web browser to access computer resources and applications that are owned and maintained by the cloud provider instead of going to the expense and effort of purchasing, installing, and maintaining their own computers and software. Cloud providers promise to lower costs and relieve IT departments of much of the burden of deploying and maintaining information systems. They can also allow customers to increase or decrease their computing capacity quickly, paying only for what they use. These perceived benefits have caused cloud computing to become one of the fastest growing markets in IT.

According to KDE, it is the first and largest state education department to use cloud computing. K-12 email systems have been moved to a cloud computing environment hosted by Microsoft, and Munis is transitioning to a cloud environment hosted by Tyler Technologies. According to KDE, moving to Microsoft's cloud email services has resulted in substantial cost savings; whereas COT charged $6 for each of Kentucky's 730,327 K-12 users, Microsoft's email services are provided to educational organizations at no charge. According to KDE estimates, similar email services would cost $53 million if provided by COT. Moreover, Microsoft offers a number of additional functions with the free email, including free storage space on its servers that would cost many millions of dollars if purchased from COT.

According to KDE, eventually, all P-12 systems will be moved to cloud computing providers, to take advantage of similar costs savings and enhanced functionality.

Kentucky's COT points out that many cloud security issues have yet to be addressed.

However, cloud computing raises a number of new security issues that have yet to be addressed. According to COT,

> cloud computing currently lacks security and privacy guarantees necessary to support much of government's internal functions. Some concerns that are not fully defined include, but are not limited to: the physical location of the data (U.S. vs. overseas), sanitation of equipment prior to disposal, security vulnerabilities of the applications themselves, security vulnerabilities of data in transit, and audit logging and regulatory compliance become very prohibitively complex. A lack of standards within the industry, at the present time, creates unacceptable levels of risks to the overall security of the Commonwealth's data (Commonwealth. Commonwealth. *2000* 3).

The APA expressed a number of concerns about cloud security, as well as questions on how systems can be audited when they are owned by others and located in another state or country.

Similar concerns appear in a document from the APA's office that suggests what questions an agency should ask before moving to a cloud provider:

- Where will the data reside?
- Who will have access to the data?
- How is the data segregated from other customers?
- What legal and regulatory compliance requirements must be met?
- What is the disaster recovery and business continuity plan for the cloud provider?
- Can we audit the provider ourselves?
- What are the change control procedures of the provider?
- How is access managed?

- What are the provider's security incident procedures?
- What support is available for investigations?
- What is the portability of the data?
- In SaaS [software-as-a-service] scenarios, how are the applications maintained?
- Does the provider maintain log data from IDS [intrusion detection system], IPS [intrusion prevention system], Firewall, systems, and applications?
- Is the data encrypted?
- Does the provider use virtualization?
- Does the provider use outsourced or subcontracted resources?
- What are the policies and procedures that assure secure destruction?
- How is the data protected? (Commonwealth. Auditor. *Cloud*)

As this document points out, another consequence of moving Munis to the cloud is that it raises doubts about whether Kentucky's auditor of public accounts will be able to conduct security checks as part of annual audits.

Although agencies must ask permission to use cloud services, they are generally not refused because each agency is regarded as the best authority on the level of privacy and security needed for that agency's data and operations. The agency's accountability for security is not transferred to the outside contractor.

For the above reasons, state agencies wishing to use cloud services must obtain a waiver from the Enterprise Architecture and Standards Committee. To date, agencies' waiver requests have been approved because the committee regards each agency as the best authority on the level of privacy and security needed for that agency's data and operations. However, COT emphasizes that an agency's accountability for security is not transferred to an outside contractor; the agency is still ultimately accountable for the security of its data and systems (Lile).

In 2012, COT issued a draft version of guidelines for records management in cloud environments; although it is not mandatory for state agencies to follow these guidelines, it is highly recommended (Commonwealth. Commonwealth. *Cloud*).

Mobile And Personally Owned Devices

Since the passage of the Kentucky Education Reform Act in 1990, Kentucky has embraced technology as a means of supporting efforts to ensure equitable access to education. However, some schools and families can afford less technology than others, and this inequitable access to technology is seen as an impediment to ensuring equal access to education. The economic downturn in recent years has increased these concerns. In 2012, the Task Force

on Student Access to Technology was formed to develop a strategy for overcoming some of these obstacles. One of the preliminary recommendations of the task force encouraged district initiatives to provide each student with a laptop, a so-called 1:1 policy. To spare districts the expense of buying laptops for all students, the task force favored allowing students to use any devices they already owned (a policy called "bring your own device" or BYOD). However, the task force had concerns about the security of these devices (Commonwealth. Task Force).

Allowing students and employees to use personally owned devices (a "Bring Your Own Device" or BYOD policy) may save money, boost satisfaction, and encourage employees to work more hours. Even without permission, users often insist on using their own devices.

KDE is encouraging districts to institute BYOD policies as a means of saving money on the purchase of workstations. Other reasons often given for BYOD policies include boosting user satisfaction and encouraging employees to work more hours beyond the school day. One of the most compelling reasons might be that, according to research, users often insist on using their own favorite devices even when the devices are forbidden. For this reason, one benefit of a good BYOD policy is to at least gather information about the types of devices in use.

Despite the potential benefits, personal and mobile devices introduce many new security problems. Many users do not go through necessary steps to secure their devices, and they often undermine security protections when downloading applications.

However, BYOD—and mobile and wireless devices in general—introduce many new security problems. Users have a great deal of control over the security of their devices. Many do not perform needed steps to secure their devices, such as disabling features that are not needed and adding passcode protection and screen locking. Even when an IT support professional helps them secure their devices, they often inadvertently undermine security when downloading applications.

Malicious software can breach confidentiality by collecting and transmitting information stored on a device. Some can tap into sensors to eavesdrop on spoken credit card numbers, detect passwords, or even see whatever is visible to the phone's camera.

Malicious software can breach confidentiality by collecting and transmitting information that is stored on a device. Moreover, some can tap into sensors to eavesdrop on spoken credit card numbers or detect passwords by sensing the vibrations of keystrokes. Researchers recently created and demonstrated malware that covertly taps into a phone's camera to see anything in view of the camera, which could compromise not only the confidentiality of information but also the privacy and safety of underage minors viewed by the camera (Templeman).

Many legitimate mobile applications collect and transmit personal information about users without their knowledge.

Aside from malicious software, many legitimate mobile applications collect and transmit personal information about users without their knowledge (O'Brien). Google and many advertisers have found ways to bypass privacy settings (Williams. "Court").

Rather than reduce IT costs, a BYOD policy can sometimes drive up costs because more support time is needed.

IT support personnel find it difficult to stay up-to-date on the evolving features of a wide variety of devices and applications. Rather than reduce IT costs, BYOD can sometimes drive up costs because more support time is needed (Osterman).

Mobile devices are far more likely to be lost or stolen.

Mobile devices are far more likely to be lost or stolen than stationary devices. A recent survey found that 69 percent of smartphone users had lost their phone at least once; on average, users lose their phones at least temporarily about twice per year (Lookout).

The first line of defense is managing attitudes and behaviors, with well-crafted BYOD policies, training, and awareness campaigns.

Protections. The first line of defense is managing human attitudes and behaviors with well-crafted BYOD policies, training, and awareness campaigns. Kentucky school districts that have introduced BYOD policies are striving to take this approach (Kentucky School).

Technological protections include giving personal devices no more than "guest" privileges when accessing networks, and providing a separate, protected workspace for personal devices.

One technological solution is to give personal devices attempting to access networks no more than the "guest" privileges that would be accorded to an outsider. Another is "containerization," a technology that creates a separate, protected workspace on a personal device (Mitchell).

Chapter 3

Conclusions

The specific security concerns raised in Chapter 2 point to a need for a comprehensive approach to security assurance, as discussed in Chapter 1.

Chapter 2 identified specific data security concerns such as weak passwords, storage of personal data on mobile devices, and a large contract in which data ownership issues were not clarified. While these issues could each be addressed individually, they point to a broader need for a comprehensive approach, as discussed in Chapter 1, including planning and governance, implementation and management, monitoring and evaluation, and strategic corrective and preventive action for continuous improvement.

As an education technology leader, Kentucky has focused more on fostering access and use than on protecting security, and statutes and regulations have not kept up with rapid changes. Accountability and authority for security are diffused and unclear.

While Kentucky is a leader in adopting innovative education technology, efforts have focused far more on fostering access and use than on protecting information security. The pace of change has outstripped some statutes and regulations. Accountability and authority for ensuring education data security are currently diffused among several entities. The General Assembly has given COT statutory authority to oversee governance and implementation of technology, including data security for state agencies. However, in practice, Kentucky's P-12 data systems are located and managed independently of COT. As for systems managed by school districts, KDE has taken the lead in advising and assisting districts in all matters related to education technology, including data security. However, there is no clear statutory authority to ensure that district-level data security plans are developed, implemented, audited, and enforced.

Recommendation 3.1

Recommendation 3.1

If it is the intent of the General Assembly that the Kentucky Department of Education be excluded from the Commonwealth Office of Technology's governance, the General Assembly should consider amending KRS 42.728 to add the Kentucky Department of Education to the list of entities not subject to the authority of the Commonwealth Office of Technology.

It is unclear who has authority and accountability for each of the activities that security experts agree are essential for ensuring security. Currently, some activities are done well while others receive inadequate attention.

It is unclear who has the authority and accountability to carry out each of the activities that security experts agree are essential to ensure security. Perhaps as a consequence, some security assurance activities are being done well while others receive inadequate attention. The sum total of evidence from OEA's interviews and

document reviews suggests that efforts are uneven across the four phases of the security assurance process.

- **Plan and govern.** Some effort is devoted to planning and governance of P-12 data security, but the accountability and authority for ensuring security are unclear, and some organizations lack comprehensive security plans.
- **Implement and manage.** Most efforts focus on implementation and management; in particular, a good deal of effort is devoted to technological solutions for ensuring logical security. Some efforts are directed toward managerial solutions, but there are gaps in policies, definitions of roles and responsibilities, training, and awareness-raising activities to remind system users what the policies are and why they are important.
- **Monitor and evaluate.** Relatively little effort is devoted to monitoring compliance and evaluating the effectiveness of current security protections.
- **Take strategic corrective and preventive actions.** Beyond the tactical actions involved in everyday management of security, it appears that little effort is directed toward strategic, continuous improvement.

Recommendation 3.2

Recommendation 3.2

The Kentucky Department of Education is currently developing a comprehensive security plan for the department. The plan should be reviewed annually and revised as necessary and should address planning and governance, implementation and management, monitoring and evaluation, and strategic corrective and preventive actions. Specifically, the plan should include, but not be limited to

- **governance structures;**
- **clear and specific lists of security-related duties for each position that impacts security;**
- **a single, agency-wide security breach notification and response procedure;**
- **disaster recovery plans, including how they will be tested;**
- **policies regarding storage of confidential data on mobile devices and public cloud services;**
- **policies on acceptable use of social networking sites, such as Facebook and Twitter;**
- **procurement and contract management policies and procedures to ensure security;**
- **criteria for gauging compliance and the effectiveness of current security provisions;**

- **a requirement to annually present a brief summary to inform the Kentucky Board of Education of the status of education data security; and**
- **a requirement to provide dedicated training for employees and awareness campaigns for all system users regarding the importance of complying with security policies.**

The amount of security considered adequate depends, in part, on the resources available and the degree of risk that an organization is willing to accept. What is important is to fully understand the risks and how each can be addressed, so that decisions are made with "eyes wide open."

The amount of security considered adequate depends, in part, on the resources available and the degree of risk that an organization is willing to accept. While many security assurance activities—such as having top leadership set a tone that security is important—can be implemented at little cost, others require more funds and personnel, and it is unclear how those additional resources would be provided. What is important is to fully understand the risks and how each can be addressed, so that decisions are made with "eyes wide open."

In discussions with OEA, representatives of KDE took the position that KDE has the primary authority and accountability for ensuring education security. Based on this position, it is logical for KDE to request the personnel and funds needed to ensure adequate security during the biennial budgeting process.

Recommendation 3.3

Recommendation 3.3

When presenting its biennial budget requests, the Kentucky Department of Education should request the personnel and funds needed to ensure adequate security, clearly explaining the risks that each expenditure is intended to address, so that the General Assembly can decide which risks to mitigate and which to accept.

Works Cited

Adams, Jimmy. "RE: status information security breach investigation." Email to Brenda Landy, Sept. 7, 2012.

American Institute of Certified Public Accountants. *SSAE 16. Statements on Standards for Attestation Engagements*. New York: AICPA, 2011.

Andress, Jason. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Kindle ed. Elsevier Science, 2011.

Berson, Alex, and Larry Dubov. *Master Data Management and Data Governance*. 2nd ed. New York: McGraw-Hill, 2011.

Carnegie Mellon University. Software Engineering Institute. CyLab Usable Privacy and Security Laboratory. Pittsburgh: Carnegie Mellon Univ. <http://cups.cs.cmu.edu/> (accessed Nov. 30, 2012).

---. ---. *Governing for Enterprise Security (GES) Implementation Guide, Article 1: Characteristics of Effective Security Governance*. Pittsburgh: Carnegie Mellon Univ., 2007.

---. ---. Symposium on Usable Privacy and Security. <http://cups.cs.cmu.edu/soups/2013/> (accessed Nov. 30, 2012).

Commonwealth of Kentucky. Auditor of Public Accounts. Agency Management Letter to Kentucky Department of Education. Frankfort: APA. For years 2006 through 2011.

---. ---. *Cloud Computing Concerns*. Frankfort: APA, 2012.

---. ---. *Report of the Statewide Single Audit of the Commonwealth of Kentucky*. Frankfort: APA. For years 2006 through 2011. <http://auditor.ky.gov/auditreports/Pages/OnlineAuditSearch.aspx> (accessed March 5, 2012).

---. Commonwealth Office of Technology. *2000 Software Domain*. Frankfort: COT, Jan. 2012. <http://technology.ky.gov/governance/Pages/architecture.aspx> (accessed July 10, 2012).

---. ---. About the Commonwealth Technology Council. <http://technology.ky.gov/about/Pages/CTC.aspx> (accessed July 10, 2012).

---. ---. Cloud Computing: Implications and Guidelines for Records Management in Kentucky State Government. Draft. Frankfort: COT, June 28, 2012.

---. ---. Governance. <http://technology.ky.gov/about/Pages/governance.aspx> (accessed July 10, 2012).

---. ---. *Sanitization of Information Technology Equipment and Electronic Media*. Policy no. CIO-077. Frankfort: COT, Nov. 1, 2005. <http://technology.ky.gov/governance/Pages/policies.aspx> (accessed May 3, 2012).

---. Department for Libraries and Archives. *Department of Education Records Retention Schedule*. Frankfort: KDLA, June 2011. <http://kdla.ky.gov/records/recretentionschedules/Pages/stateschedules.aspx> (accessed May 1, 2012).

---. ---. *Destruction Guidelines: Destruction of Public Records: A Procedural Guide*. Frankfort: KDLA, Aug. 2007. <http://kdla.ky.gov/RECORDS/RECRETENTIONSCHEDULES/Pages/default.aspx> (accessed May 1, 2012).

---. ---. *Public School District Education Records Retention Schedule*. Frankfort: KDLA, Aug. 2012. <http://kdla.ky.gov/records/recretentionschedules/Pages/LocalRecordsSchedules.aspx> (accessed Aug. 31, 2012).

---. Department of Education. *2007-2012 Education Technology Master Plan*. Frankfort: KDE, Dec. 2008. <http://www.education.ky.gov/KDE/Administrative+Resources/Technology/Master+Plan/Previous+Technology+Master+Plans.htm> (accessed Sept. 4, 2012).

---. ---. *2011-12 KDE Data Standards, District Policy and Procedures: Quick Reference Guide*.

---. ---. *Acceptable Use Policy*. Frankfort: KDE, Jan. 1, 2010.

---. ---. Continuous Instructional Improvement Technology System (CIITS) Public. Frankfort: KDE, July 18, 2012. <http://www.education.ky.gov/kde/instructional+resources/curriculum+documents+and+resources/continuous+instructional+improvement+technology+system+(ciits)+public.htm> (accessed July 18, 2012).

---. ---. Education Commissioner Releases Budget Analysis. Frankfort: KDE, April 9, 2008. <http://cpe.ky.gov/NR/rdonlyres/B1D74EA5-BE34-4F9C-A436-AA9D6196572B/0/5_CommissionerEdReport.pdf> (accessed Jan. 11, 2012).

---. ---. *HB 341 Data Security Study*. Frankfort: KDE, 2006.

---. ---. ILP Invite Others Option. KDE, April 24, 2012. <http://www.education.ky.gov/kde/instructional+resources/secondary+and+virtual+learning/ilp/ilp+invite+others+option.htm> (accessed June 1, 2012).

---. ---. *KDE Data Governance*. Frankfort: KDE Jan. 21, 2009.

---. ---. *KDE Data Operations & Governance*. Frankfort: KDE, Aug. 10, 2010.

---. ---. KDE Mobile Device Eligibility and Ownership Policy. Frankfort: KDE, April 1, 2010.

---. ---. *KDE Response - OEA Data Study – FINAL*. Frankfort: KDE, Dec. 12, 2012.

---. ---. *KDE Security Program Framework*. Frankfort: KDE, 2012.

---. ---. Kentucky Board of Education Agenda Book and Past Meeting Summaries. Frankfort: KDE. <http://education.ky.gov/KBE/meet/Pages/default.aspx> (accessed July 31, 2012).

---. ---. *Kentucky Board of Education Strategic Plan.* Frankfort: KDE, Oct. 6, 2010. <http://education.ky.gov/KBE/Pages/default.aspx> (accessed Jan. 23, 2012).

---. ---. Kentucky Education Technology System Expenditure Plan. For fiscal years 2006-2009.

---. ---. KETS Master Plan, v 1.3 DRAFT. Frankfort: KDE, July 2013.

---. Finance and Administration Cabinet. *Gov. Beshear Announces Three Smart Government Initiatives: IT Initiatives will save money and make service delivery more efficient*. Frankfort: FAC, Sept. 24, 2012. <http://finance.ky.gov/initiatives/ITinfrastructureinitiative/Pages/Overview.aspx> (accessed Oct. 1, 2012).

---. Task Force on Student Access to Technology. *Report of the Task Force on Student Access to Technology*. Draft. Nov. 2012.

Couch, David. "RE: Applicability of COT policies and procedures to KDE." Email to Brenda Landy, July 12, 2012.

Dimensional Research. *The Generation Gap In Computer Security: A Security Use Survey From Gen Y To Baby Boomers*. San Carlos: CheckPoint Software Technologies, June 2012. <http://www.checkpoint.com/press/2012/062012-check-point-survey-gen-gap-in-security.html > (accessed Aug. 1, 2012).

Fordham Center on Law and Information Policy. Children's Educational Records and Privacy: A Study of Elementary and Secondary School State Reporting Systems. New York: Fordham Univ., 2009. <http://law.fordham.edu/center-on-law-and-information-policy/14769.htm> (accessed Jan. 16, 2012).

Gartner, Inc. IT Assessment and Optimization Project: Final Report. Stamford: Gartner, May 2004.

Golden, Daniel. "College-Survey Firm Quietly Peddles Student Information to Big Marketer." *The Wall Street Journal*. Dec. 3, 2001.

Hackworth, Robert. "RE: Current status of response to SSWAK Audit Findings FY11." Email to Brenda Landy. Oct. 24, 2012.

Harvey, Scott. "Students charged with hacking JCPS computer system." *Wave3.com* (Louisville), Dec 17, 2007. <http://www.wave3.com/Global/story.asp?S=7509176> (accessed July 6, 2012).

Hoover, Eric. "Legislators Ask Testing Companies How They Use Student Data." *The Chronicle of Higher Education*. May 27, 2011.

ISACA. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows: ISACA, 2012. <http://www.isaca.org/COBIT/Pages/default.aspx> (accessed Jan. 15, 2012).

---. *COBIT 5 for Information Security*. Rolling Meadows: ISACA, 2012. <http://www.isaca.org/COBIT/Pages/info-sec.aspx> (accessed Jan. 15, 2012).

---. *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd ed. Rolling Meadows: IT Governance Institute, 2006.

ISO and International Engineering Consortium. *ISO/IEC 27000: Information technology—Security techniques—Information Security management systems—Overview and vocabulary. First edition 2009-05-01*. Geneva: ISO, 2009.

---. *ISO/IEC 27002: Information technology—Security techniques—Code of practice for information security management. First edition 2005-06-15*. Geneva: ISO, 2005.

Kentucky School Boards Association. "BYOD: Schools begin to adopt Bring Your Own Device policies." *Kentucky School Advocate*, Nov. 2012. <http://www.ksba.org/11-12BYOD.aspx> (accessed Nov. 20, 2012).

Lang, Lisa. "RE: questions for KDE's HR." Email to Brenda Landy, Aug. 6, 2012.

LeMay, Katrina. "RE: questions about COT authority with respect to agency security." Email to Brenda Landy. Nov. 20, 2012.

Lile, Janet, and Glenn Thomas. Meeting with Pam Young and Brenda Landy regarding waiver to allow cloud computing for Munis. Frankfort, July 10, 2012.

Lookout Mobile Security. Mobile Mindset Study. San Francisco: Lookout, 2012. <https://www.lookout.com/resources/reports/mobile-mindset> (accessed Oct. 31, 2012).

Lykins, Brian, Jenny Luscher, and Jenny Sparks. Interview with Marcia Seiler, Pam Young, and Brenda Landy regarding 2006 through 2011 audits of Kentucky Department of Education. March 16, 2012.

McGrew, Charles, Rich Miller, and Chris Brewer. Meeting with Pam Young and Brenda Landy regarding the longitudinal database maintained by the P-20 Collaborative. July 18, 2012.

McQuillen, Matt. Telephone conference call regarding ILP Portfolio End User Agreement with Marcia Seiler and Brenda Landy. Aug. 23, 2012.

Mitchell, Robert L. “Best BYOD management: Containment is your friend.” *ComputerWorld*, Aug. 29, 2012. <http://www.computerworld.com/s/article/9230476/Best_BYOD_management_Containment_is_your_friend> (accessed Oct. 15, 2012).

National Conference of State Legislatures. State Security Breach Notification Laws. Washington: NCSL, 2012. <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx> (accessed July 23, 2012).

---. Data Disposal Laws. Washington: NCSL, 2012. <http://www.ncsl.org/issues-research/telecom/data-disposal-laws.aspx> (accessed July 23, 2012).

O’Brien, Kevin. “Data-Gathering via Apps Presents a Gray Legal Area.” *The New York Times*, <http://www.nytimes.com/2012/10/29/technology/mobile-apps-have-a-ravenous-ability-to-collect-personal-data.html?_r=0> (accessed Oct. 2012).

Oltsik, Jon. *The ESG Information Security Management Maturity Model*. Hopkinton: RSA/EMC Corp., July 2011.

Osterman Research. Mobile Devices in the Enterprise: MDM Usage and Adoption Trends. White Paper. Black Diamond: Osterman Research, July 2012.

Ponemon Institute. *2010 Annual Study: U.S. Cost of a Data Breach*. Mountain View: Symantec, March 2011. <http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon> (accessed April 24, 2012).

Privacy Rights Clearinghouse. Chronology of Security Breaches: Security Breaches 2005-Present. June 11, 2012. <http://www.privacyrights.org/data-breach> (accessed June 12, 2012).

---. Prevent Identity Theft with Responsible Information-Handling Practices in the Workplace. 2009. <https://www.privacyrights.org/ar/PreventITWorkplace.htm> (accessed 2012).

Quagliata, Karen. “Impact of Security Awareness Training Components on Perceived Security Effectiveness.” *ISACA Journal*, Vol. 4, 2011. <http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Pages/JOnline-Impact-of-Security-Awareness-Training-Components-on-Perceived-Security-Effectiveness.aspx> (accessed Nov. 16, 2012).

Stratton, Tom. “RE: KDE student data privacy forms.” Email to Brenda Landy. Nov. 28, 2012.

Symantec, Inc. *Symantec Report on the Underground Economy, July 07–June 08*. Mountain View: Symantec, Nov. 2008. <http://www.symantec.com/content/en/us/about/media/pdfs/Underground_Econ_Report.pdf> (accessed June 5, 2012).

Tackett, Deanna. “RE: update on Auditor’s 2011 findings.” Email to Brenda Landy. Oct. 26, 2012.

Templeman, Robert, Zahid Rahman, David Crandall, and Apu Kapadia. *PlaceRaider: Virtual Theft in Physical Spaces with Smartphones*. Ithaca, NY: Cornell Univ., Sept. 27, 2012. <http://arxiv.org/abs/1209.5982> (accessed Oct. 31, 2012).

Thomas, Glenn. “RE: Applicability of COT policies and procedures to KDE.” Email to Brenda Landy and David Couch. July 13, 2012.

United States. Committee on National Security Systems. National Information Assurance (IA) Glossary. Fort George G. Meade: CNSS, April 26, 2010. <http://www.cnss.gov/instructions.html> (accessed Jan. 30, 2012).

---. Department of Commerce. National Institute of Standards and Technology. *Building an Information Technology Security Awareness and Training Program*. NIST Special Publication 800-50. Washington: NIST, Oct. 2003.

---. ---. ---. *Glossary of Key Information Technology Terms*. NIST IR 7298 Rev. 1. Washington: NIST, Feb. 2011. <http://csrc.nist.gov/publications/PubsNISTIRs.html> (accessed Feb. 1, 2012).

---. ---. ---. *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Special Publication 800-37, Rev. 1. Washington: NIST, 2010.

---. Department of Education. *Family Educational Rights and Privacy Act: Guidance for Reasonable Methods and Written Agreements*. Washington: DOE.

---. ---. *Intersection of FERPA and IDEA Confidentiality Provisions*. Washington: DOE, March 2012.

---. ---. Statewide Longitudinal Data Systems Fact Sheet. Washington: DOE, July 2009. <http://www2.ed.gov/programs/slds/factsheet.html > (accessed Sept. 4, 2012).

---. Department of Health and Human Services and Department of Education. *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records*. Washington: DHHS, Nov. 2008.

---. Department of Homeland Security. *Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development*. Washington: Sept. 2008. <http://www.us-cert.gov/ITSecurityEBK/> (accessed June 12, 2012).

---. ---. *A Roadmap for Cybersecurity Research*. Washington: Nov. 2009. <http://www.us-cert.gov/ITSecurityEBK/> (accessed Jan. 4, 2012).

---. Federal Trade Commission. Frequently Asked Questions about the Children's Online Privacy Protection Rule. Washington: FTC, Oct. 7, 2008. <http://www.ftc.gov/privacy/coppafaqs.shtm> (accessed May 1, 2012).

---. ---. "Student Survey Companies Settle FTC Charges: Data Collected For 'Educational Purposes' Also Sold To Marketers Who Targeted Kids." FTC press release. Jan. 29, 2003. <ftc.consumerdev.org/privacy/privacyinitiatives/promises_enf.html> (accessed June 21, 2012).

Verizon. *2012 Data Breach Investigations Report*. New York: Verizon, 2012. <http://164.109.37.243/Resources/> (accessed June 12, 2012).

WBKO. "Western Ky. School's Athletic Files Erased." Wbko.com, Oct 16, 2009. <http://www.wbko.com/news/headlines/64493747.html> (accessed July 6, 2012).

Williams, Martyn. "Court will reconsider Google's Safari privacy deal." *PCWorld*, Oct. 28, 2012. <http://www.pcworld.com/article/2013193/court-will-reconsider-googles-safari-privacy-deal.html> (accessed Oct. 28, 2012).

Williams, Stephanie. Telephone interview with Brenda Landy. Oct, 8, 2012.

Winnick, Steve. *Analysis of Final FERPA Regulations*. Washington: Data Quality Campaign, Dec. 9, 2011.

Young, Lu. "RE: status information security breach investigation." Email to Brenda Landy, Sept. 6, 2012.

Appendix A

Information That Requires Extra Protection

Personal Information Of Students And Employees

Federal statutes and regulations emphasize the need to protect the confidentiality of personally identifiable information, which includes

- personal identifiers, such as students' or school employees' Social Security numbers, student ID numbers, and fingerprints used as identifiers;
- names and addresses of students and their family members;
- other indirect identifiers, such as a student's date of birth, place of birth, or mother's maiden name;
- other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and
- information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates (34 CFR Section 99.3).

Although personal information is generally held confidential, schools may choose to release "directory" information, defined as "information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed." Examples listed in the federal regulation are student name and address; telephone listing; email address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full time or part time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors and awards received; and the most recent educational agency or institution attended (34 CFR Section 99.3).

Student Performance Information

In addition to confidentiality concerns, security measures must protect the integrity of student performance data, including course grades, test scores, and attendance records. Security breaches have allowed students to change their information and that of other students.

Employee Performance Information

Security controls must protect the confidentiality and integrity of information contained in personnel records of teachers, staff, and administrators.

Financial Information

Financial information includes revenues, expenses, account balances, purchase orders, invoices, and payment records. In public education, financial information is rarely kept confidential. However, securing its integrity is of vital importance to ensure that public funds are spent appropriately and efficiently. Inadequate security could allow records to be accidentally altered or destroyed or could allow the embezzlement or misappropriation of funds.

Proprietary Information

Organizations must prevent the loss, theft, or duplication of software, textbooks, and other proprietary information, which is defined as information associated with a company's products, business, or activities. Information is proprietary only if it was developed by the company and not available to the government or the public without restriction from another source. An organization that is negligent about protecting proprietary information can be sued for breach of contract or for loss of income to the company whose information has been stolen (US. Committee 56).

Appendix B

Legal Obligations To Protect Student Information

Federal Legislation

Family Educational Rights And Privacy Act. Most education information compliance efforts are driven by the Family Educational Rights and Privacy Act of 1974 (FERPA), which applies only to schools and districts receiving funds from the US Department of Education. Most private and parochial schools do not receive such funds and are, therefore, not subject to FERPA.

FERPA gives parents (or students once they turn 18) certain controls over the disclosure of education records. Federal program funding can be withheld from any education agency or institution that "has a policy or practice of releasing, or providing access to, any personally identifiable information in education records" without the written consent of parents or eligible students (20 USC sec. 1232g). The phrase "policy or practice" means that inadvertent disclosure of information is not considered a FERPA violation. A list of exceptions permits information to be released without parental permission to certain officials or groups, such as law enforcement agencies, state longitudinal data systems, and those carrying out interventions, evaluations, audits, or research on behalf of an educational organization. If a recipient of student data improperly rediscloses the data in violation of FERPA, revised FERPA regulations, effective January 3, 2012, require that this recipient be denied access to personally identifiable data for at least 5 years (20 USC sec. 1232g; 34 CFR Part 99).

Although the US Department of Education has the option to withhold funds or temporarily deny access to data, the preamble to the FERPA regulations states that these consequences would not be imposed until the organization has been given the opportunity to come into voluntary compliance. Moreover, the department has never actually withheld funds as a response to FERPA violations (Winnick).

Compliance with FERPA is necessary but not sufficient to ensure security. The US Department of Education emphasizes that FERPA "represents the floor for protecting privacy, not the ceiling," and recommends that organizations follow security best practices, some of which are specified in the department's guidance documents (*Family* 5).

Individuals With Disabilities Education Act Of 2004. The Individuals with Disabilities Education Act (IDEA) protects the privacy of information about students' disabilities or special education (20 USC 1400-1419; 34 CFR 300.610–300.627; US. Dept. of Educ. *Intersection*).

Health Insurance Portability And Accountability Act Of 1996. Privacy protections mandated by the Health Insurance Portability and Accountability Act (HIPAA) do not apply to health information contained within an education record if that record is covered by FERPA. Therefore, public schools rarely need to consider HIPAA. In any case, the privacy protections in both HIPAA and FERPA are similar (US. Dept. of Health).

National School Lunch Act. Because a student's eligibility for free or reduced-price lunch is an indicator of poverty, it is legally impermissible to disclose this information about an individual student without prior consent from the parent or guardian except for a few specific circumstances (42 USC 1758(b)(2)(C)(iii)).

Children's Internet Protection Act. The Children's Internet Protection Act of 2000 (CIPA) requires schools to monitor minors' online activities and to block or filter Internet access to visual depictions that are obscene, pornographic, or otherwise harmful to minors. This act applies not only to devices owned by the school but also to personally owned devices brought to the school, such as students' own laptops and cellphones. In 2011, the Protecting Children in the 21st Century Act added an additional requirement to CIPA: Schools must also educate students about online behaviors with respect to social networking websites, chat rooms, hacking, and cyberbullying (47 USC sec. 254(h)(5)(B)).

If a school does not comply with CIPA, it could be barred from receiving some funds and discounts for technology.

Children's Online Privacy Protection Act. The Children's Online Privacy Protection Act of 1998 (COPPA) requires operators of commercial websites to obtain a parent's permission before collecting personal information from a child under the age of 13. However, if a school grants the operator permission to collect students' information, the operator is permitted to assume that the school has already obtained the parents' approval (15 USC sec. 6502(b)(1)(A)(ii). When giving an operator access to student information, the school must consider its obligations under FERPA (US. Federal. Frequently).

State Statutes And Regulations

Kentucky Family Education Rights Act. The Kentucky Family Education Rights Act of 1994, codified in KRS 160.700 through KRS 160.730, mirrors the FERPA statute in most respects. However, it goes farther than FERPA, addressing not only rules for disclosure but also the responsibility for protecting information:

> [s]chool officials shall take precautions to protect and preserve all education records including records generated and stored in the education technology system (KRS 160.705(2)).

Education Technology. KRS 156.675 and 701 KAR 5:120 require the use of the latest available filtering technology to prevent the transmission of sexually explicit materials to or from schools and school districts. The Kentucky Department of Education must make this technology available without cost to schools or districts that request it and must notify all schools and districts that such software is available. In addition, each district must establish an acceptable use policy including parental consent for student Internet use, teacher supervision of student computer use, and auditing procedures for determining whether education technology is being used for accessing sexually explicit or other objectionable material.

Special Education. Confidentiality of special education students' records is addressed by 707 KAR 1:360. Section 2 requires that districts keep records of anyone given access to a special

education student's records, including the name of the person, the date of access, and the purpose for which the access was granted. Section 7 of this regulation requires parental consent before disclosing education records, except for specified purposes. The regulation goes on to spell out specific safeguards:

(1) An LEA [local educational agency, usually called a district] shall protect the confidentiality of personally identifiable student information at collection, storage, disclosure, and destruction stages.
(2) An LEA shall assign a staff member to assume responsibility for ensuring the confidentiality of any personally identifiable student information.
(3) An LEA employee collecting or using personally identifiable information shall receive training or instruction regarding the requirements of this administrative regulation.
(4) An LEA shall maintain, for public inspection, a current listing of the names and positions of employees within the LEA who may have access to personally identifiable student information (Section 8).

A district must inform parents when it no longer needs education records to provide special education services to the child and must comply if the parent requests that the records be destroyed. However, the district may retain a permanent record of the student's name, address, phone number, grades, attendance, classes attended, grade level completed, and year completed (Section 9).

The rights of parents are transferred to the student once the student reaches the age of 18, unless the student has been declared incompetent (Section 10).

Sanctions for not complying with state and federal regulations are addressed in 707 KAR 1:380, although a breach of confidentiality is not listed explicitly. Districts that are not in compliance are given time and assistance to come into compliance. If the district is still not in compliance after several opportunities to do so, special education funds may be withheld. Continued noncompliance may result in the withholding of SEEK funds.

Data Disposal. KRS 365.720 through 365.730 require careful disposal of materials containing personally identifiable information. However, the statute refers only to businesses, not to governmental or not-for-profit organizations. The Kentucky Department for Libraries and Archives and the Commonwealth Office of Technology offer guidance, policies, and procedures for proper disposal, but these documents do not have the strength of a statute.

Appendix C

Kentucky's Major P-12 Data Systems

System	Uses	Data Types	KDE Unit(s) Primarily Responsible	Contractor(s) (HQ location)	Where Data Are Stored—Primary And Backup)
Student Information System (Infinite Campus/IC)	Student record keeping, service coordination, transcript generation, compliance reporting	Students' Social Security numbers, birth dates, family contact information, course and test performance, health conditions, special education, disciplinary actions	Office of Knowledge, Information, and Data Services	Infinite Campus (Blaine, MN)	On-site servers at 63 districts with > 3,000 students. Site for smaller districts, KSB, and KSD: Commonwealth Office of Technology (COT)'s secure data center in Frankfort.
Munis	Financial management, payroll, accounts payable and receivable	Revenues and expenditures; employees' Social Security numbers, birth dates, salaries, and benefits	Office of Knowledge, Information, and Data Services	Tyler Technologies (Dallas)	Software-as-a-Service hosting in Yarmouth, ME [backup: Dallas]
Support Education Excellence in Kentucky (SEEK)	Management of state education funds allocated to districts	Aggregate district characteristics (average daily census, lunch eligibility, etc.), financial data	Office of Administration and Support, Div. of Budget and Financial Management	No contractor	Frankfort (KDE servers at COT data center-Cold Harbor)
Continuous Instructional Improvement Technology System (CIITS)	Lesson planning, assessment creation, content sharing	Standards, educational content (some proprietary); eventually will also include student performance data and teacher performance data	Office of Administration and Support; Office of Knowledge, Information, and Data Services	SchoolNet-Pearson (New York)	Cloud-based: New York [backup to be established Jan. 2013]
Individual Learning Plan (ILP)	College and career planning	Students' personal data from Student Information System (IC), career interests, work and volunteer experiences	Office of Next-Generation Learners, Division of Learning Services	Career Cruising (Toronto)	Cloud-based: Toronto, ON, Canada [backup: United Kingdom]
CNIPS	Meal reimbursements	Food service provider information, meal reimbursement claims	Office of Admin & Support, Div. of School & Community Nutrition	Colyar Consulting Group (Phoenix)	Frankfort (COT-Cold Harbor) [backup: Plano, TX]
Food service point-of-service systems	Meal pricing, transaction records	Individual student eligibility for free or reduced-price lunches,	N/A – districts contract directly	various	Individual district, school and food service provider sites

(Continued on next page.)

Appendix C (continued)

System	Uses	Data Types	KDE Unit(s) Primarily Responsible	Contractor(s) (HQ location)	Where Data Are Stored—Primary and Backup)
Office 365 (formerly Live@EDU)	Email, document storage, collaboration space	Email messages and any content that users choose to attach to messages or store online	Office of Knowledge, Information, and Data Services	Microsoft (Redmond, WA)	Microsoft San Antonio Data Center [backup: Chicago, IL Data Center].
Assessment and Accountability	Statewide summative, college readiness, end-of-course, and English Learners assessments	Student level performance and demographic data	Office of Assessment and Accountability	Pearson (San Antonio); Univ. of Kentucky (Lexington); ACT, Inc. (Iowa City); WIDA Consortium (Madison, WI)	Frankfort (KDE-Cold Harbor); [backup: San Antonio (Pearson); Iowa City (ACT, Inc.); Lexington (Univ. of Kentucky); Madison, WI (WIDA)]

Source: Staff compilation of information from the Kentucky Department of Education.

Appendix D

Methods Used For Unauthorized Access To Data And Corresponding Security Protections

Technological, Social, And Physical Avenues Of Attack

Technological

Threats. Attackers, often working remotely via the Internet, find and exploit security weaknesses to gain unauthorized access to a computer system. Data can be intercepted during transmission. Malicious software, such as viruses, Trojans, worms, and spyware, may destroy or corrupt files, disrupt the normal operations of a system, and open security holes for hackers to exploit. Denial of service attacks overwhelm a system, making it unavailable to users (US. Dept. of Commerce. Natl. *Glossary*).

Protections. Technical protections include firewalls, proxy servers, antivirus software, careful configuration of new and updated machines, prompt and diligent installation of updates and security patches, encryption of data stored on portable devices, network intrusion detection and blocking software, and protections for communications and transmissions, such as secure socket layer and virtual private networks.

Social

Threats. Social engineering is the use of various methods to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear harmless but that are actually malicious. The most common example is phishing, sending authentic-looking emails to request information from users or to direct them to a fake website that requests information. While phishing involves sending emails widely and at random, spear phishing targets specific organizations or individuals using tailored information to lend legitimacy and encourage trust. The spear phisher sends email to addresses within a company, posing as someone who could be expected to contact that company and requesting information they may normally be expected to request. Information from social networks, such as Facebook and LinkedIn, can be used for tailoring spear phishing messages (US. Dept. of Commerce. Natl. *Glossary*).

Protections. The main defenses against phishing and other types of social engineering are training and awareness campaigns for both permanent and temporary staff, teachers and students, contractors/suppliers, and other system users. Policies and procedures are also key tools. Security should be promoted frequently, in several different ways, such as training sessions, posters, reminders on computer screens, and reminders in emails.

Physical

Threats. Physical methods of accessing data include theft of computers and printer hard drives, installing key loggers on personal computers to record the typing of passwords, taking confidential documents from printer trays, or finding carelessly discarded information in the trash or on old computers. When old computers are decommissioned, it is not enough to delete all the files. Deleting simply removes file names from a directory so that the computer can write new information over the old files, but until it does that, the old files are still there. Special "sanitization" procedures must be followed to render the information unreadable.

Protections. Physical protections include security guards at entrances, locked rooms for network servers, locked storage cabinets, careful disposal of discarded paper and electronic media that contain sensitive data, and extra care in guarding portable devices from loss or theft (Commonwealth. Commonwealth. *Sanitization*; Commonwealth. Dept. for Libraries. *Department* and *Public*).

Special Challenges Posed By Insiders

Threats. Although news stories often focus on hackers who attack systems using the Internet, security problems can also come from insiders. Insiders—those who are authorized to access at least some of the organization's data and systems—include staff, teachers, administrators, students, contractors, and suppliers. Breaches are often caused by mistakes, such as accidentally posting confidential information on a publicly accessible webpage instead of a secured location, printing Social Security numbers on the outside of mailings, or failing to thoroughly erase personal information from discarded computers or CDs. Insiders may deliberately breach security, taking advantage of their system privileges and physical access to information and computer equipment (US. Dept. of Homeland. *A Roadmap* 29-37; Privacy).

Protections. Three key principles for combating accidental and deliberate insider threats are:

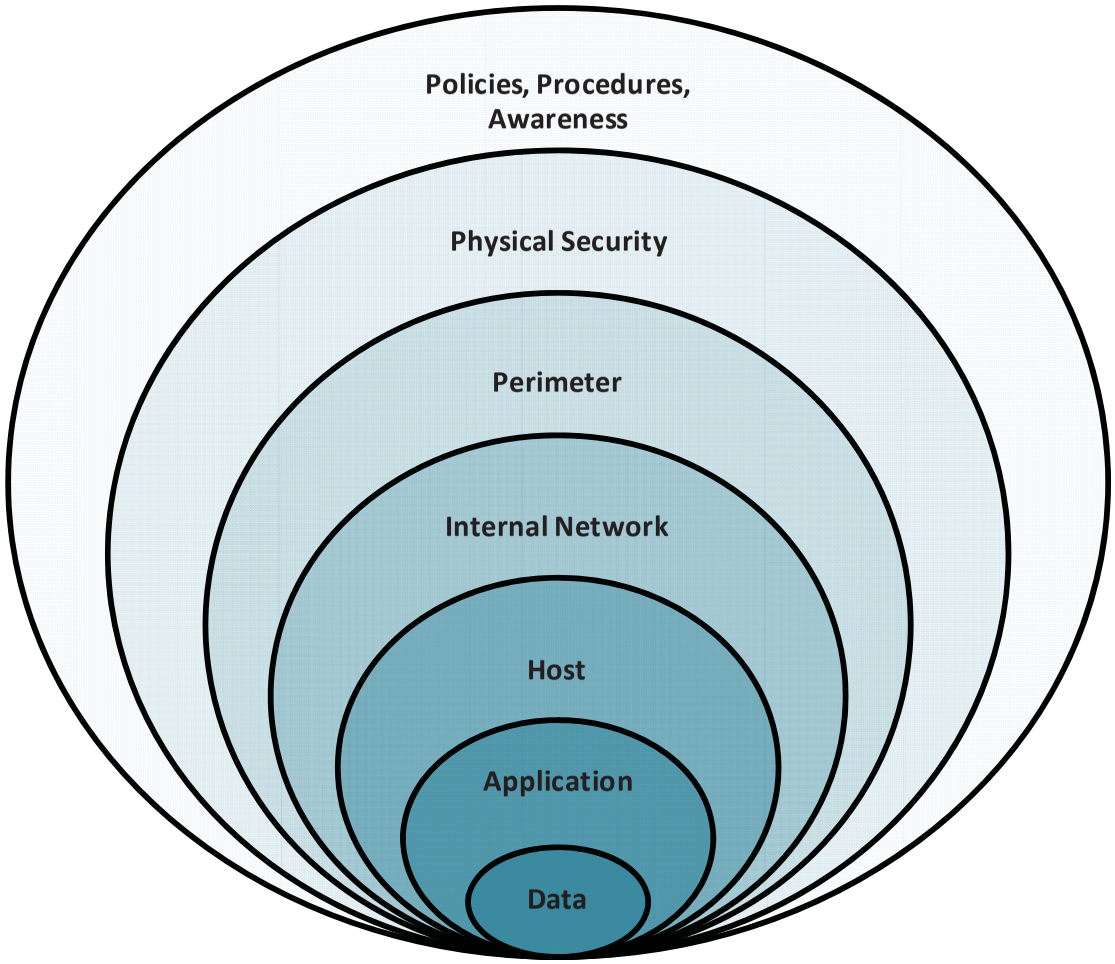
- Least Privilege: Giving each employee only the access and transaction privileges that are needed to carry out assigned duties;
- Need to Know: Restricting access to information to only those who need to know the information in order to carry out a required task;
- Separation (or Segregation) of Duties: Ensuring that no one person can carry out a sensitive process from end to end without requiring approval or double-checking by someone else.

Many security experts, including the Auditor of Public Accounts, recommend that logs be kept of system activities and that random samples of these logs be reviewed regularly for any suspicious activity, especially on the part of users who have the most privileges.

Defense In Depth

Most security experts recommend a "defense in depth" strategy that uses multiple layers of protections, as illustrated in Figure D.A.

Figure D.A
Layers Of Protections In A Defense-In-Depth Strategy



Examples of Protections in Each Defense Layer

Policies, Procedures, Awareness	Acceptable use policy, awareness campaigns
Physical Security	Locks, video monitoring, proper disposal
Perimeter	Firewall, proxy, penetration testing
Internal Network	Intrusion detection, logging, auditing
Host	Authentication, antivirus, password hashing
Application	Content filtering, data validation
Data	Encryption, backup, access controls

Source: Staff adaptation of information from Andress, 11-14.

Appendix E

Entities That Impact Governance Of Kentucky's Education Data Security

Federal	
Department of Education	Monitors FERPA, PPRA, and IDEA compliance
Privacy Technical Assistance Center	Provides information and guidance to education stakeholders on data privacy, confidentiality, and security practices
Family Policy Compliance Office	Investigates alleged FERPA and PPRA violations
Office of Special Ed. Programs	Monitors IDEA compliance
Department of Agriculture	Monitors National School Lunch Program compliance
Federal Communications Commission	Monitors CIPA compliance
Federal Trade Commission	Monitors COPPA compliance
Department of Commerce: National Institute for Standards and Technology	Sets technical standards for federal agencies, but these standards are widely used outside the federal government

State	
General Government Cabinet	
Auditor of Public Accounts	Audits financial information systems
State Chief Information Officer	New position created September 2012; unfilled at time of this report
Finance and Administration Cabinet	
Commonwealth Office of Technology	Oversees state's shared technologies and establishes IT security policies and procedures for state agencies
Commonwealth Technology Council	Provides input from all state cabinets on IT policy, direction, planning, and legislation; identifies opportunities for shared services, sourcing, investments, and cost recovery; guides state IT programs and projects
Enterprise Architecture and Standards Committee	Defines system architectural direction, maintains IT standards, recommends revisions or new standards to Commonwealth Commissioner of Technology, and reviews business case exceptions from agencies
Office of Procurement Services	Oversees requests for proposals/requests for bids, the evaluation of bids, and contract negotiations
Kentucky Higher Education Assistance Authority	Collects and manages information from high schools for the Kentucky Educational Excellence Scholarship (KEES)
Education and Workforce Development Cabinet	
Kentucky Department of Education	
KDE Planning Committee	Makes final decisions about IT and other matters
Information & Knowledge Core Process Team	Reviews recommendations of Technology Planning Council before they are submitted to the KDE Planning Committee
Technology Planning Council	Devises policies and procedures regarding technology, and presents recommendations to KDE Planning Committee

(Continued on next page.)

State (cont'd)	
Data Policy Committee	Devises policies and procedures regarding data, and presents recommendations to KDE Planning Committee
Technical Services	Manages infrastructure (for instance, networks and email) for KDE and districts
KDE Business Units	Manage several systems, such as the student information system
P-20 Data Collaborative	Manages state longitudinal data system
Education Professionals Standards Board	Manages teacher databases
Kentucky Department for Libraries and Archives	Establishes policies and procedures for retention and proper disposal of public records

Local	
School districts (174 districts)	Establish district and school policies and procedures; manage district and school information technology
Kentucky School Boards Association	Offers a policy and procedure service; 173 districts subscribe to policies service, and 147 subscribe to procedure service

Notes: In addition to the agencies listed in this table, a variety of agencies at the federal, state, and local levels receive and investigate reports about security breaches and other security-related issues. FERPA=Family Educational Rights and Privacy Act. PPRA=Protection of Pupil rights Amendment. IDEA=Individuals with Disabilities Education Act. CIPA=Children's Internet Protection Act. COPPA=Children's Online Privacy Protection Act. IT=information technology. KDE=Kentucky Department of Education.
Source: Staff compilation.

Appendix F

Auditor Of Public Accounts' IT-Related Findings For KDE, Fiscal Year 2011

The excerpts in this appendix are verbatim findings from the FY 2011 annual report of Kentucky's Auditor of Public Accounts. Statements in square brackets are updates that KDE provided to OEA about KDE's efforts to respond to these findings.

FINANCIAL STATEMENT FINDINGS
Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 11-KDE-25: The Kentucky Department Of Education Should Ensure All Agency Machines Are Properly Configured To Include Only Necessary Services

Our fiscal year (FY) 2011 security vulnerability assessment on machines owned by the Kentucky Department of Education (KDE) revealed 37 of 307 scanned central level machines, or approximately 12 percent, could potentially be mis-configured. A mis-configured machine could waste resource, entice an attack using ports that are unnecessarily open, have default services running, or allow excessive hypertext transfer protocol (HTTP) methods. The ports open on each of these machines should be reviewed to ensure they have a specific business purpose and that the services are properly authorized. Nine of these machines contained open ports addressed with the agency during the previous audit. An additional machine had an open port that was reported during the previous two audits. Of the 37 potentially mis-configured machines, 14 machines reported the potential use of a remote shell suite of programs.

For security purposes, detailed information that would identify the specific machines contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

System misconfigurations that allow unnecessary services can negate other security configurations established on the machine, increase potential security vulnerabilities, and provide enticements for intruders to enter the system. Specific to web servers, excessive HTTP methods provide additional avenues for system intrusion. The use of unsecured transmission programs also increases the risk of compromised data transmissions.

To assist in securing a network adequately, it is necessary to ensure all machines and web services are configured to only allow necessary services to operate. Only necessary business-related ports should be open. Default services should be disabled. Only the necessary HTTP methods (such as POST, HEAD, and GET) should be supported on agency web servers.

Recommendation

We recommend KDE take the necessary actions to ensure the noted services on each machine have a specific business purpose and are properly authorized. If the service is necessary, it should be reviewed to ensure it is properly authorized, licensed, and configured as well as

adequately secured. Default services should be disabled or removed from all servers. Any unnecessary services should be disabled or the associated ports should be closed. HTTP methods not required for the operation and maintenance of a web server should be disabled. If the remote shell suite of programs is being utilized, it should be replaced by a more secured shell suite.

Management's Response and Corrective Action Plan

KDE will review all KDE managed servers noted and take action to address. We will remove unnecessary and default services where possible. The UNIX hardware is limited and dated, which limits the ability to update the support tools, RTools. These are used on the UNIX environment supporting the MUNIS application.

There is a current KDE project to migrate the MUNIS application to another operating system and hardware platform. The districts are migrating over the next 18 months. RTools, which were specific to the UNIX platform, will no longer be needed.

[Update from KDE as of Oct. 24, 2012: "The move of MUNIS to the cloud will remediate this issue, which was focused on presence of a set of software tools on the MUNIS servers. Due to the limited nature of the hardware and the Dated OS required for the MUNIS application, these tools were unable to be updated, therein causing the finding during the APA audits. The tools are no longer needed in the cloud environment" (Hackworth).]

FINDING 11-KDE-26: The Kentucky Department Of Education's Office Of Knowledge, Information And Data Services Should Expand And Consistently Apply Logical Security Policies For The KETS Network And MUNIS

Our fiscal year (FY) 2011 audit of the Kentucky Department of Education (KDE) system controls revealed weaknesses related to the Office of Knowledge, Information And Data Services (KIDS) security surrounding the Kentucky Education Technology System (KETS) network and MUNIS. However, some improvements have been made since the prior year audit. Although KDE has developed an overarching Security Program, Acceptable Use Policy, and Access Control Policy to address appropriate use of resources within KDE, these policies do not specifically address IT responsibilities associated with the KETS network and MUNIS. At this time, there are no plans for a policy specific to KETS and MUNIS. Further, none of these address security controls specific to KIDS servers. Similar issues have been addressed to the agency during the past four audits.

KIDS management is responsible for central workstations and servers, as well as KIDS-related employee and contractor network access. Further, audit logging was enabled by KIDS for all UNIX and Windows-based servers; but, no security policy was formalized at the central level concerning procedures to periodically review the audit logs for users with high-level privileges.

All KDE users were granted Local Administrator rights on their workstations. This is considered unnecessary access for most KDE employees. Technical and support staff should be the only personnel with this level of access to prevent the accidental or intentional introduction of viruses or the loss of programs or data and to ensure workstations utilize only approved software.

In addition, an access request form was not developed for requesting and granting access to agency resources and applications. Currently, the KIDS Data Center Services team grants server access. The level of access is determined by the Division of District Support (DDS). Employees are required to sign Confidentiality Agreements upon hire. However, this form did not specifically identify the agency resources or applications to which the user requires access, did not list the level of access to be granted to the user, and was not required to be updated for changes in access. KDE intends to require access requests be processed through the KETS Service Desk in the future, although this is not currently a formal procedure.

The school districts primarily use the MUNIS financial system to manage their finances. In addition, certain financial and staffing reports exist that KDE uses from the districts for state and federal purposes. When districts are ready to forward files to KDE, a transfer utility program transfers the file to a Gateway server maintained by KIDS, and then the files are transported daily to a File Transfer Protocol (FTP) server and temporarily stored for pickup by the DDS staff. As MUNIS is a purchased system, specialized for Kentucky, select vendor staff also has access to the districts' MUNIS servers in the event that support is needed. For FY 2011, four new vendor support staff were identified with update access to district servers. A Confidentiality Agreement was not on file for one of the four users, or 25 percent. Further, KETS Service Desk tickets were not completed for these four MUNIS users.

During FY 2011, one new user account was established on the Gateway server and added to two security groups on the Gateway server. Appropriate documentation was provided supporting the account setup and addition to the security groups. However, we identified five disabled accounts on the Gateway server that remained members of one or more security groups on the server.

Although no new Jefferson County school district employees were granted access to the servers since FY 2009, we determined KDE still does not request Confidentiality Agreements or other supporting documentation for Jefferson County employees. During the FY 2010 audit, KIDS planned to establish an agreement with Jefferson County to ensure all Jefferson County employees with MUNIS access agree to an appropriate level of confidentiality. However, follow up performed during FY 2011 revealed this had not been done.

Although KIDS had not implemented a formal security policy related to specifically accessing MUNIS servers or software in the districts, an informal process was in place for KDE or KIDS staff to first obtain authorization from the school district before accessing the district's MUNIS server or software. A log was maintained at KIDS to track access to district servers by the root account. However, review of this log revealed that the activity being captured does not include the district server being accessed.

Without strong, formalized, logical security controls, the opportunity increases for unauthorized modification to financial and staffing reports as well as the likelihood of errors or losses occurring from incorrect use of data and other resources. Granting users local administrator rights to their workstations allows those users the ability to download and install unauthorized software as well as possibly pirated data.

Formalized security policies set the tone of management concern for strong system security and provide a security framework used to educate management and users of their responsibilities. System security should be administered in such a way as to ensure proper segregation of duties. System access should be limited to the level necessary for performing assigned duties, and system accounts should not be shared to ensure individual user activity could be tracked. Granting users system administration access to their computers increases the likelihood that unauthorized and unlicensed software could be installed and increases the chance of system attacks by viruses or other malware.

Further, access to servers that house critical financial and staffing data should be restricted to only necessary employees. Intruders often use inactive accounts to break into a network. If an account is not used within a reasonable period of time, the account should be disabled until it is needed. This minimizes the possibility that an unauthorized user will access the account. Accounts that are not anticipated as being used in the future should be periodically purged. Finally, system user accounts and audit trails should be reviewed periodically in order to ensure identification and tracking of user activity.

Recommendation

We recommend KIDS standardize security responsibilities for all KIDS employees and ensure critical programs and data related to the KETS network and MUNIS, as well as the servers housing such data, are properly secured. The agency should, at a minimum:

Develop formal procedures related to the management of locked and disabled accounts related specifically to the KETS network and MUNIS. These procedures should address the process of disabling or removing terminated employee accounts, as well as unnecessary generic accounts. Accordingly, a methodology should be developed so that a distinction can be made between accounts that can be safely removed versus accounts that must be retained on the server for performance reasons or audit trail history. These procedures should include the requirement for a periodic review of disabled and locked accounts to determine their necessity. If an account is deemed unnecessary, it should be permanently removed from the KIDS servers unless there is a pragmatic reason for maintaining the account, in which case it should be, at a minimum, disabled. All disabled accounts should be removed from current group membership on the KIDS servers.

Evaluate all security group assignments on the KIDS servers to ensure that all assigned users require membership in the assigned groups. Implement procedures to periodically review security audit logs with special attention being given to users with high-level privileges so that inappropriate use of resources can be further investigated, if the need arises.

Restrict Local Administrator rights to technical and support staff.

Finalize and implement plans to establish an agreement with Jefferson County to require a confidentiality agreement for all Jefferson County employees with access to KIDS servers.

Develop and implement a user access request form to explicitly identify access being requested to resources or data and all necessary approvals required. All users, both internal and external to KDE, requesting access to KDE resources or applications should be required to complete this form. The completed forms should be approved by appropriate management and should be maintained in the user's file as supporting documentation for their access. Until an access request form is established, KIDS should continue to use KETS Service Desk tickets to establish or alter access. These tickets should be maintained for audit purposes.

Ensure sufficient information is captured with the log used to track access to the district servers to allow the reviewer to determine the server on which the activity took place.

Management's Response and Corrective Action Plan

KDE will institute a unified process to ensure that MUNIS user accounts belonging to terminated employees will be deleted or disabled, except where the disabling of such accounts will interrupt normal operation. Due to the large number of services dependant on Active Directory for user access, including MUNIS, KDE has started a formal process to review and remove accounts.

KDE plans to develop a process to review the security group assignments of sensitive servers. KDE does not have adequate resources, staff or tools to regularly review security logs in an effective and efficient manner. Logs are retained short-term for review once an incident/issue is identified.

KDE continues to investigate current methods available to reduce the number of KDE workstations with Local Administrator rights.

The KDE is currently working on a solution to remove the need for district employees to have access to a KIDS server. In the meantime, KDE will establish a process with Jefferson County for the management of confidentiality agreements for all Jefferson County employees who have access to the referenced KIDS server. We will document the permissions granted and the approval and make them available.

KDE will continue to expand, enhance and standardize the electronic access control processes for permissions to network and critical applications.

We will continue to investigate new methods to capture the MUNIS district server identification within the district server access log. There is a current KDE project to migrate the MUNIS application to another operating system and hardware platform. Once complete, KDE staff will no longer be responsible for maintaining the district MUNIS servers.

[Update from KDE as of Oct. 24, 2012:

- "The move of MUNIS to the cloud will alleviate several issues pointed out in this finding – specifically those related to MUNIS and server user accounts.
- The server to which Jefferson County staff had access has been decommissioned.
- KDE understands the risk involved with providing KDE staff with Local Administrator rights, and I am working with our Security Team and our Desktop Support to investigate

solutions which will allow KDE staff as much of the functionality they require as possible, while increasing our security stance" (Hackworth).]

FINDING 11-KDE-28: The Kentucky Department Of Education's Office Of Knowledge, Information And Data Services Should Expand And Consistently Apply Program Modification Procedures

Our fiscal year (FY) 2011 audit of the Kentucky Department of Education (KDE) system controls revealed the program modification process developed by the Office of Knowledge, Information and Data Services (KIDS) is not sufficient to ensure only authorized changes to the Information Technology (IT) environment, which includes the Municipal Information System (MUNIS), are made. Similar issues have been noted for the past five audits; however, some improvements have been made since the prior year audit.

KIDS developed and implemented a formalized Change Management Policy and Procedures Manual. This manual stipulates changes made to the IT environment must be documented on a properly completed and approved Request for Change (RFC) form. However, the manual does not specify the individuals responsible for performing testing of a proposed change or migration of a change to production. The current informal process has members of the MUNIS Support Team and one MUNIS vendor employee responsible for testing MUNIS-related changes. On the approval of the Project Manager, MUNIS-related changes are moved into production by a member of the MUNIS Support Team. This informal process could lead to a segregation of duties issue between the request for change, development of the change, testing of the change, and promotion to production. It could also lead to a failure to complete any one of these tasks.

Over the past five years, we have recommended the implementation of digital signatures on the RFC forms. However, due to budgetary constraints, KIDS does not anticipate moving to this technology. Since the RFC forms are submitted and approved electronically through a simple process of typing an individual's name in the approver's field, there is not sufficient information maintained within the documentation to substantiate who provided an approval for a change. Also, KIDS had not developed a listing of authorized Requesters/Owners who can request a change to the IT environment.

Additionally, our review of five KDE utilities revealed 231 lines of code changed within one utility program affecting processing. An associated RFC form was provided; however, it did not reflect approval from the second line supervisor or the date in which testing was performed. Further, the description of the change was vague and did not adequately describe all the changes made.

Finally, an examination of eight RFC forms related to changes to the MUNIS system since our prior year review revealed five forms were missing at least one of three required approvals. Also, the testing section of two of these forms was incomplete. The other three forms were properly completed; however, the testing was designated as being completed by the MUNIS Support Team. Since this team is made up of three individuals, there is no way of knowing who actually performed the testing and moved it to production.

Failure to properly apply and monitor change control procedures increases the risk that incorrect or unauthorized changes could be made to critical applications and, potentially, be moved into the live production environment.

Program modification control procedures should be consistently applied in order to ensure that only appropriately authorized changes to critical applications are made and implemented within the production environment. All program modifications are to be requested on a Request for Change form. They should be monitored and thoroughly documented, with procedures established to log all program change requests, review and approval processes to be followed, and supporting documentation to be maintained for the process. Changes to KIDS utilities should also be included in the change management process.

Recommendation

We recommend an expansion of the KIDS Change Management Policy and Procedure manual to identify specific individuals or groups responsible for performing changes, testing changes, authorizing promotion of changes, and moving changes into production. All change management controls should be consistently applied to critical system software and utility programs.

All changes should be requested and approved using the RFC form. Since KIDS does not plan to implement electronic signatures, individuals responsible for approving the RFC form either should be required to print, sign, and date the RFC form or provide e-mail correspondence indicating approval which can be linked to the RFC form in order to validate approvals and avoid segregation of duties issues.

Finally, the requirement for support related to changes to the utility programs should be expanded. In the event a major change is made to a utility program, KIDS should perform a comparison of the old and new versions of the utility code to determine which lines specifically were changed and provide an explanation of the necessary changes. In instances where a minor change to a utility program is required, KIDS should provide a summary of the changes made. This can be done for each module or section of code changed. Each time a change is made to a utility program, a brief overview of the change should be documented in the 'Revision' section of the source code.

RFC forms as well as other supporting code compare or change descriptions should be maintained for audit purposes.

Management's Response and Corrective Action Plan

There is a current KDE project to migrate the MUNIS application to another operating system and hardware platform. Once complete, onsite vendor staff will no longer be responsible for maintaining utility codes. KDE will review the KDE/KIDS Change Management documentation and add the following improvements:

Identify groups responsible for performing, testing, and approving changes for critical system software and utility programs.

KDE will more explicitly document the RFC approvals.

Identify and track major changes to utility code for critical systems in the Revision section of the code.

[Update from KDE as of Oct. 24, 2012: "As stated in our reply to the FY 2011 audit findings, 'onsite vendor staff will no longer be responsible for maintaining utility codes' once the MUNIS application completes its transition to the cloud. However, the recommendation to more explicitly document RFC approvals was a point well-taken, and has been under revision" (Hackworth).]

FINDING 11-KDE-29: The Division Of School And Community Nutrition Should Develop Formal System Documentation To Support Processing Performed By The School And Community Nutrition Payment Application

Our fiscal year (FY) 2011 audit of application level logical security revealed the Kentucky Department of Education's (KDE) Division of School and Community Nutrition (DSCN) did not maintain current, technical documentation describing the processing performed by the School and Community Nutrition (SCNP) Application. This issue has been addressed with DSCN for three consecutive years.

The SCNP application, which was developed by and is currently maintained by the Commonwealth Office of Technology (COT), went into production in 1982. Updates and expansions of services were made to the application over the last 29 years, most recently in October 2010. Discussion with COT personnel during the FY 2009 audit revealed no technical manuals existed documenting the design or functionality of the system. They did indicate a series of binders had been maintained containing notes documenting how to perform different tasks within the application; however, many of the notes were identified as being outdated or obsolete. For FY 2011, documentation had been developed by COT in relation to the last system upgrade. This included numerous use cases, which provides a basic understanding of current business processes.

DSCN includes on their website the Online Reporting System User Guide and Application and Agreement User Guides for the various programs supported by DSCN. These are updated annually and provided to Sponsors during mandatory annual training. These documents provide a general overview of business processes and procedures associated with submitting claims and applications/agreements, but they do not provide a technical overview of system processing. During FY 2010, DNHS staff also provided to the auditors a Nutrition and Health Services (NHS) Technology Manual; however, it was determined at that time to be several years out of date. Further, this manual was not updated during the FY 2011 audit.

For FY 2011, DSCN hired a business analyst who will be responsible for formulating clear, comprehensive, and well-organized business rules of the existing system. This project was expected to begin in January 2011. At the time in which fieldwork was completed, technical documentation still needed to be compiled and organized as a reference manual.

We are aware DSCN has issued an RFP to facilitate a full upgrade/replacement of the legacy SCNP application. Within the requirements for the system, the vendor must provide several documents at initial implementation including functional and technical specifications as well as user guides.

Lack of documentation increases the likelihood of erroneous or incomplete processing. It further increases the likelihood of unauthorized data modification, destruction of assets, and interruption of services.

Proper documentation should be maintained for each critical program in production in order to, at a minimum, identify the purpose of the programs, the origin of data, the specific calculations or other procedures performed, and the output of data or reports.

Recommendation

We recommend DSCN continue working with COT to develop documentation that provides an understanding of critical programs or jobs currently running in production. The documentation could include a network diagram; user and operational manuals; and flowcharts, diagrams, or descriptive narratives of functional areas. Information normally collected in design documents includes a technical description of the program, sources and location of files used by the program, and the processing steps for main functions. This documentation should be used during the planning of the new SCNP application for cross-walking procedures from the old to the new system.

Management's Response and Corrective Action Plan

Discussions have been held with COT on the state of the current system documentation. COT has researched what documentation is available; including any documentation generated through past development efforts. COT's findings revealed that some documentation is available on the mainframe. When a job is updated this information must be updated and moved to production with the job. This documentation includes the job description, job frequency, description of the most recent change, input and output data sets, and reports generated from the job. Based on this inventory plans will be made to ensure sufficient documentation is available on critical programs in production.

The former Technology Manual incorporated many different areas that are irrelevant to SCN's current operations, including phone setup, use of the copier, etc. Portions of the Technology Manual pertinent to the current online application system were extracted and transformed into a mainframe user manual. The manual includes the most comprehensive step-by-step instructions and accompanying code definitions to date. The user manual will be beneficial to current staff as well as assist with the transition to the new system.

[Update from KDE as of Oct. 26, 2012: "I feel that these are resolved with our new system" (Tackett).]

FINDING 11-KDE-30: The Division Of School And Community Nutrition Should Enable System Auditing That Will Provide Documentation To Allow For Appropriate Monitoring Of Security Violations On Its School And Community Nutrition Payment System

Our fiscal year (FY) 2011 audit of application security over the Kentucky Department of Education's (KDE) Division of School and Community Nutrition's (DSCN) School and Community Nutrition Payment (SCNP) Application revealed historical transactions, including those related to security, are not logged or tracked within the system. The United States Department of Agriculture (USDA) Southeast Regional Office (SERO) of Food and Nutrition Service (FNS) had a finding related to this issue since FY 2007. This is the third consecutive year that this issue has been addressed to DSCN.

The SCNP application, which was originally developed and is currently maintained by the Commonwealth Office of Technology (COT), retains the date of the last update to claims and approvals, as well as the user Id of the person that made the update. However, it does not identify what information was changed. Further, the system does not retain a historic version of transactions.

Additionally, users with an access level of '1' are given full control over claims, sponsor and organization screens, applications, agreements, approvals, system access, and bank balances within the application. Since the system does not maintain a history of changes to security levels, it is not possible for the system administrator or management to review changes to a user's security level within the system. DSCN has reviewed staff duties and developed a proposed list of changes to access security levels to promote greater segregation of duties within the SCNP application. However, during FY 2011 fieldwork, COT had not completed the necessary configuration changes to accommodate these improvements.

We are aware DSCN has issued an RFP to facilitate a full upgrade/replacement of the legacy SCNP application. With this planned system change, DNHS does not believe it is feasible to enable security auditing on the current SCNP application. However, they hope to implement a formal review process over corrected claims submitted by central-level staff by March 2011.

Failure to adequately monitor security events and transaction logs could result in failure to identify suspicious activities that may be occurring on the system.

Without effective monitoring of event and security logs, the risk of inappropriate transactions being processed by the system increases. A logging and monitoring function within an application and consistent review of the results enables early detection of unusual or abnormal activities.

Recommendation

As DSCN is in the process of developing a new SCNP application, we recommend DSCN work in conjunction with COT to ensure the proposed security level changes within the currently SCNP application are incorporated to improve segregation of duties and, thereby, system security. Until a new system is in place, DSCN should implement a formal review process to

ensure all corrected or revised claims and approval changes are appropriate and being made by authorized central level staff.

An appropriate level of management should perform regular reviews of changes being made by central level staff within the SCNP application. This review should be documented and retained for audit purposes.

Further, we recommend DSCN ensure audit logging is a requirement for the new system. Once the new system is implemented, DSCN management should review the event and history logs on a regular basis. Identified security violations should be thoroughly documented to ensure they are resolved in a timely manner. This review should be documented and retained for audit purposes.

Management's Response And Corrective Action Plan

A formal review process to ensure corrected/revised claims are appropriate and being made by SCN staff has been implemented by SCN. COT provides a spreadsheet of claims modified by SCN staff in the prior month. The monthly audit review worksheets are being reviewed by an SCN administrator. Business requirements for the new system include maintaining of an audit log of past versions and the user ID associated with the change. In addition, the vendor notes the proposed system tracks statistics that may be related to suspicious access activities such as repeated failed login attempts and attempting to access functions the user is not authorized to perform.

[Update from KDE as of Oct. 26, 2012: "I feel that these are resolved with our new system" (Tackett).]

Sources: Commonwealth. Auditor. *Report*, 2011, 107-121; Hackworth; Tackett.

Appendix G

Widely Recognized Information Security Standards And Guidance

National and international groups of security experts collaborate to develop and continuously update systematic sets of standards that organizations can follow to achieve optimal levels of security. Globally, the most widely adopted set of standards is put out by ISO in collaboration with the International Electrotechnical Commission; the standards are often referred to as the 27000 series, reflecting how the documents are numbered (ISO. *ISO/IEC 27000*).

Another widely adopted standard is COBIT (Control Objectives for Information and Related Technologies) which is maintained by ISACA. Unlike the ISO/IEC 27000 series, which focus narrowly and deeply on security, COBIT provides less detail about security but integrates it into a broad framework that helps overall governance of information technology. Organizations often combine COBIT and ISO because each has unique strengths and uses.

The National Institute of Standards and Technology developed Federal Information Processing Standards (usually referred to as FIPS) and other standards for US government agencies. These standards are useful for other organizations outside of the federal government, because they are rigorous and because compliance with these standards is a condition for doing business with the federal government (US. Dept. of Commerce. Natl. *Guide*).

To guide audits of financial information systems, the American Institute of Certified Public Accountants developed Statement on Standards for Attestation Engagements (SSAE) number 16, which addresses security controls of these systems; SSAE16 replaces the widely used standard SAS 70 (American).

Although the above-mentioned standards say what should be done to protect security, they say little about how these duties should be distributed among various departments and positions within an organization. Unclear delineation of duties could allow gaps, inconsistencies, and redundancies. To address the lack of role-based security standards, the US Department of Homeland Security worked with experts from academia, government, and the private sector to develop a high-level framework that specifies which functions within the organization should be responsible for each of the duties described in the leading national and international standards (US. Dept. of Homeland. *Essential*).

There are advantages and disadvantages to adopting a formal set of standards. The main disadvantage is the cost (in time and money) of adopting standards. However, contractors and subcontractors are often required by their clients to comply with multiple sets of security standards, which suggests that adopting standards may not be as onerous as many organizations believe it would be. Another disadvantage is that the standards would be too inflexible and difficult for some organizations to adapt to their unique circumstances and needs. An advantage of adopting formal standards is that they are very helpful for ensuring comprehensive and systematic security measures. They lower the risk of security breaches, and if security is breached, the organization’s diligence in adopting standards can reduce the risk of lawsuits.

Governing best practices are discussed by a number of organizations, including the US Department of Education, the IT Governance Institute, ISACA, and the Carnegie Mellon Software Engineering Institute.

In recent years, the US Department of Education has offered grants to help states build longitudinal integrated education data systems. The burgeoning of these state databases raised concerns about privacy, especially for student information. In 2010, the department created the Privacy Technical Assistance Center, which provides technical briefs, issues briefs and white papers, a security checklist, a data governance checklist, and a checklist for written agreements with third parties that have access to data. These documents are far less detailed than the formal standards discussed above, but they provide some guidance tailored to educational organizations.

Usability is considered one of the most difficult and important problems in information security (US. Dept. of Homeland. *A Roadmap*, 90-98). In addition to devoting a laboratory to usability, Carnegie Mellon University's Software Engineering Institute organizes an annual Symposium on Usable Privacy and Security (SOUPS) that brings together researchers from around the world to share innovative alternatives for security protections that frustrate or confuse users, such as the need to create, change, and remember many complex passwords (Carnegie. Software. Cylab and Symposium).

Appendix H

District Hardware And Software Security Standards Required By The Kentucky Department Of Education

The list below was provided by KDE in response to a draft of this report.

IP Addressing: Every school district uses a pre-defined range of private IP addresses (not broadcast on the Internet) that make the internal district networks essentially invisible to the rest of the internet.

Anti-Virus/Malware/Spam/Spyware Protection: Every school district is provided with McAfee EPO, a standard policy set (along with any additions they require) and centrally managed DAT file updates to the District EPO server. Districts manage end user and district owned server clients/provisioning, deployment and updates.

Active Directory/Global Policy Orchestrator: Baseline GPO rules are created by KDE. Districts can create additional GPO profiles and manage assign user and group accounts according to their policies. Baseline directory structure is provided, districts can add to, or arrange directory objects and containers to meet their organizational structures.

Threat Management Gateway/Proxy/Web Filtration: KDE requires a web filtration/proxy system in accordance with SB 230. Districts can use the KDE supported product (Microsoft Threat Management Gateway 2010) or may make a waiver request for a similar product that meets or exceeds the requirements set by the state statutes. A baseline firewall configuration for TMG is supplied by KDE. No specified block list, whitelist, or blacklist is supplied by KDE. Those lists and category blacklists are managed and activated by the districts.

District Located Firewall to Internet: KDE supplies and manages the KEN network equipment at each district locale. This connectivity includes a Checkpoint firewall on HP hardware. The systems are managed by KIDS personnel and Avaya Services. Firewalls are centrally managed and follow a common configuration practice with minimal variations.

Nessus Vulnerability Scanning: As districts add or alter public facing services (such as web servers), KDE offers a scanning service to verify OS and applications are compliant to updates and patches. This is strictly by request of the district.

Source: Commonwealth. Dept. of Educ. *KDE Response*.