

**Cyber Security:
Pay Now or Pay More Later
A Report on Cyber Security in Kentucky**

December 19, 2013



**ADAM H. EDELEN
AUDITOR OF PUBLIC ACCOUNTS
www.auditor.ky.gov**

**209 ST. CLAIR STREET
FRANKFORT, KY 40601-1817
TELEPHONE (502) 564-5841
FACSIMILE (502) 564-2912**

The Auditor Of Public Accounts Ensures That Public Resources Are Protected, Accurately Valued, Properly Accounted For, And Effectively Employed To Raise The Quality Of Life Of Kentuckians.

Table of Contents

Chapter 1	Cyber Security: Introduction by Auditor of Public Accounts Adam H. Edelen.....	1
Chapter 2	Background.....	3
Chapter 3	Summary of FY 2013 IT Audit Security Findings and Recommendations	14
Chapter 4	Finance and Administration Cabinet’s Commonwealth Office of Technology Chief Information Security Office Cyber Security Initiatives.....	25
Chapter 5	Conclusion – Need for Cyber Legislation.....	28
Appendices	1. Examples of External and Internal Threats	30
	2. Summary of APA IT Audit Security Related Issues Identified From FY 2011 through FY 2013.....	32
	3. Enterprise IT Policies	33
	4. National Conference of State Legislatures Heat Map.....	37

Chapter 1

Cyber Security: Introduction by Auditor of Public Accounts Adam H. Edelen

For the thousands of Kentucky parents whose children attend public schools, a recent cyber attack on the Department of Education's Infinite Campus website resulted in the inability to access their children's grades, homework assignments, and other information. Although the attack inconvenienced thousands of parents, it could have been much worse.

Cyber attacks on state and local government networks occur every single day. To get a sense of just how serious the threat is, we need to look no further than my office, which has already had more than 5,000 unauthorized attempts (i.e., potential attacks) to access our secure network this year alone.

We also can look at the recent devastating cyber attack in South Carolina that enabled hackers to access the tax records, bank account information, and Social Security numbers of 3.6 million residents. Sensitive information of hundreds of thousands of South Carolina businesses was also accessed. In an attempt to redress the situation, the state's elected officials offered all residents and businesses free identity theft prevention and credit monitoring services for a year – to the tune of almost \$30 million.

My primary role as state Auditor is to serve as the taxpayer watchdog. However, few know that I am also the cyber watchdog. This is something my office and previous administrations have been doing, mostly below the radar, for more than two decades. What's new, though, is the ever growing priority I and future auditors will need to give this role.

We know the bad guys are out there, and are trying to attack us every day. We must become more proactive about fighting the threat, or we risk becoming the next South Carolina. To fight that threat, we need to incentivize state and local governments to ensure everything in their power is done to protect citizens' data.

From tax returns and health records to credit card and banking information and more, our government possesses a vast amount of personally sensitive information. And yet Kentucky is just one of four states without a breach notification law that requires government to make notification when our personal information has been breached. Kentuckians do not currently have the right to be notified when government loses their personal information in a cyber attack. I believe we must change this and protect the privacy and identities of every Kentuckian.

Why is this so important? If a hacker breaches a network and obtains sensitive information, they will likely use that information for nefarious ends. If we are unaware that our information has been compromised, we're defenseless to take necessary actions. However, if the entity that has been attacked is obligated to make notification, a number of measures can be taken to ensure our identity isn't stolen, our bank or health records aren't jeopardized, and our lives aren't negatively impacted in any other way. We can ask our bank, for example, to notify us if they detect suspicious activity.

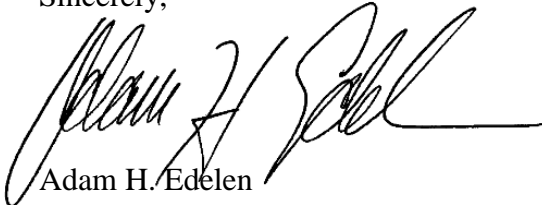
In short, breach notification laws grant us the right to be aware – to be vigilant. Without them, we are at the mercy of government, forced to hope the right thing is done by notifying us when our information is compromised. As your taxpayer watchdog, I've seen too many cases where systems that relied upon trust rather than accountability resulted in disastrous consequences. When cyber breaches occur, the entity on the receiving end of the attack may be embarrassed and inclined to sweep the incident under the rug. As your Commonwealth cyber watchdog, I view breach notification as a basic right.

Chapter 1**Cyber Security: Introduction by Auditor of Public Accounts Adam H. Edelen**

If it's good enough for 46 other states, then surely it's good enough for us. Although the Commonwealth Office of Technology, the agency responsible for the Commonwealth's technology systems, has internal policies requiring agencies to notify everyone affected by a cyber breach, something as critical as this must be enshrined in statute.

I am confident that during the 2014 legislative session, both parties can work together to provide Kentuckians with the protection they deserve in the face of the increasing cyber threat – a threat that our nation's Secretary of Homeland Security recently upgraded as being even more serious than terrorism. My goal will be to work with legislators on both sides of the aisle, as well as other stakeholders, to craft a cyber-protection bill that balances the practical realities of cash-strapped governments with the need to vigorously protect the citizen data held by our Commonwealth.

Sincerely,

A handwritten signature in black ink, appearing to read 'Adam H. Edelen', with a long horizontal flourish extending to the right.

Adam H. Edelen
Auditor of Public Accounts

Chapter 2

Background

Internal and External Cyber Security Threats

It is commonplace for employees to receive unsolicited emails that may contain malicious payloads

The National Institute of Standards and Technology (NIST) characterizes the source of cyber threats and defines a threat as any circumstance or event with the potential to cause harm to a system. Common threats to systems can be caused from natural, human, or environmental circumstances and may create mild to devastating consequences for an organization's systems. Human threats are possibly the most significant that must be considered. Though many examples exist of natural and environmental occurrences impacting systems with destructive outcomes, these threats are more predictable and may provide an organization time to prepare for such an event. However, human threats are always difficult to anticipate and only limited to the imagination of those determined to attack a system. When securing any system, an entity should always expect the unexpected and continually assess the environment for ever-changing threats.

Systems are routinely subjected to many types of probes, which are attempts by another computer to ask for information from the system, and could be initiated as precursors to an actual attack. It has become commonplace for employees to receive unsolicited emails that may contain malicious payloads intended to compromise computer systems or provide attackers with unauthorized access. Web servers are probed in an attempt to gain information about web pages that may accept input from outside, as well as looking at files on the website to determine whether sensitive or confidential information exists. Internet accessible systems are routinely probed seeking vulnerabilities that will allow unauthorized access. This information gathering process allows potential hackers to design and launch precision attacks.

The sources of external threats can come from next door or from across the world and the sources of internal threats can be just as unpredictable. These threats may originate from inside an organization's network rather than from outside. When designing cyber defenses, an organization often has an underlying false assurance that threats are primarily external, and, as a result, system security is designed to focus on external threats. However, malicious attackers are often users granted some level of authorized network access.

For example, many cyber attacks use email as their delivery system, so when an unsuspecting staff member, operating within the network, opens a malicious email, the payload begins an attack as though sitting at the email victim's keyboard. In effect, the cyber attacker has placed himself/herself inside the network and is acting under the victim's network identity.

Another example is war-driving, a method of searching for a wireless access point (WAP) connected to a network, to gain unauthorized access to the system. Many techniques exist to circumvent controls and gain access to a WAP and, consequently, access to the network. If the attacker is successful, a system could experience several issues, including denying users' access, deleting or modifying programs or data, and initiating or approving transactions.

Chapter 2

Background

Traditional perimeter defenses are no longer sufficient

Regardless of the means of attack, the techniques, motivations, and tools are often the same. Therefore, we cannot solely rely on traditional perimeter defenses such as firewalls to protect systems, but must also ensure security measures are taken regardless from where an attack originates.

Distinguishing the potential impact caused by an external versus internal attack can be difficult because of the potential opportunity for attack techniques to be launched from both. There are, however, a few distinguishing points worth mentioning:

- An external attack may be more disruptive because an insider usually wants to remain unnoticed.
- External attacks can be more disruptive due to the large numbers of bots, a software application that runs automated tasks over the Internet, which represent more machines than typically exist on internal networks.
- An internal attack is usually not noticed as quickly as an external attack because most security perimeter defenses (switches, firewalls, etc.) do not inspect internal traffic.
- Internal attacks are often more focused because an insider would be familiar with the environment and its target(s).
- Internal attacks are usually easier to launch because insiders are generally trusted, while external traffic is considered potentially malicious.

A listing of examples of external and internal threats can be seen at Appendix 1.

There are many ways to categorize and describe internal versus external threats. Categorizing threats assists in understanding the threat landscape but can also be taken too literally. There are several ways to maliciously attack a system and to unintentionally disrupt a system's security. Further, attacks can be launched from multiple locations. Being too focused on categorizations or a specific process can obscure the reality of the diverse means that can disrupt a system.

It is imperative to implement effective and practical policies to educate both the technical and non-technical staff about the risks likely to be encountered. Policies should provide staff guidance regarding the:

- Proper response to issues identified.
- Implementation of standard industry procedures for both perimeter and internal network security.
- Classification of data.
- Encryption of confidential and sensitive data.
- Regular review of system controls for compliance with agency established policies and standards.
- Performance of audits to ensure an acceptable level of risk is reached and that effective security defenses are established.

Chapter 2

Background

Overview of APA Efforts to Address Cyber Security Threats

The APA is tasked with annually auditing Commonwealth of Kentucky Executive Branch state agencies, which assists in the completion of the Comprehensive Annual Financial Report and Single Statewide Audit of Kentucky. Prior to planning each series of audits, the APA Financial Auditors assess the priority for significant IT systems operating in the Commonwealth having either a potential financial impact or potential non-compliance with federal regulations. The APA IT Auditors then determine the risks associated with each significant IT system and design audit procedures to test the security controls for each system and the network as a whole. Instances of insufficient security controls or inconsistent application of the established controls will result in specific recommendations to the responsible state agency.

IT risks and environments are dynamic and are constantly evolving. Further, all agencies and IT systems are unique, requiring specific and customized risk assessment and testing. Therefore, APA IT Auditors must adapt and keep informed of changing technology and the related risks through training and other professional development opportunities. The focus is an understanding of the current IT environment from a user and security perspective, as well as identifying ongoing IT enhancements and associated security challenges and concerns. APA IT Auditors refer to the NIST principles to ensure all relevant security concerns are addressed in the audit. Additional best practice resources are used in the APA IT audit process.

The APA uses multiple security scanning tools to identify security vulnerabilities on the Commonwealth networks. This process is continually revisited to ensure the most current vulnerabilities are identified. The APA also encourages audited agencies to perform their own periodic security scans to proactively resolve any identified security flaws or address vulnerabilities before they are identified by the APA scan.

Issues identified through the audit process are reported to agencies and recommendations, as well as best practices, are provided to assist the agency in addressing the concerns. In response to the issues, agencies are requested to provide an action plan developed to address issues reported. During the next annual audit, IT Auditors will perform follow-up procedures to test previously reported items to determine whether the issues were properly addressed and resolved. If items are not resolved, they are again reported in the current audit. The APA can release Auditor's Alerts that inform agencies of potential technology threats that could impact a broad spectrum of organizations.

Chapter 2

Background

Examples of Cyber Attacks on Multiple States

“It’s not a matter of if you will be attacked; rather, it’s a matter of when.” This is a common theme heard from cyber security experts when consulting with both businesses and governments in possession of sensitive or confidential data. While cyber attacks on banks and technology companies, such as Facebook and Twitter, tend to receive the most media coverage, governments have also been the target of countless malicious hacks. After all, from tax returns to health records, sealed court records to social security numbers, and credit card numbers to bank account information, governments hold an enormous amount of sensitive and confidential citizen and government agency data.

When attacks against public sector entities are successful, citizens begin to lose confidence in government’s ability to protect the data it stores. As the table below illustrates, successful cyber attacks on state agencies throughout the country are not uncommon. Over the last four years, security breaches involving health care data alone affected more than five million individuals as a result of dozens of attacks in at least 23 states. Note that Table 1 only includes attacks related to health care data that were reported and publicized. As a result, it represents a conservative estimate of the number of attacks and individuals affected.

Table 1: Government Entities Reporting Health Care Data Cyber Attacks

Name of Entity Reporting Health Care Data Cyber Attack	State	Individuals Affected	Date of Breach
Alaska Department of Health and Social Services	AS	501	10/12/2009
Wyoming Department of Health	WY	9,023	12/2/2009
State of TN, Bureau of TennCare	TN	3,900	12/23/2009
South Carolina Department of Health and Environmental Control	SC	2,850	2/17/2010
Utah Department of Health	UT	1,298	3/1/2010
State of New Mexico Human Services Department, Medical Assistance Division	NM	9,600	3/20/2010
California Department of Healthcare Services	CA	29,808	4/29/2010
Department of Health Care Policy & Financing	CO	105,470	5/17/2010
Carolina Center for Development and Rehabilitation	NC	1,590	6/24/2010
State of Delaware Health Plan	DE	22,642	8/16/2010
State of Alaska, Department of Health and Social Services	AK	2,000	9/7/2010
State of South Carolina Budget and Control Board Employee Insurance Program (EIP)	SC	5,596	11/18/2010
Texas Health and Human Services Commission	TX	1,696	3/10/2011
New York State Department of Health	NY	550	4/17/2011
Ohio Health Plans	OH	78,042	6/3/2011
Washington State Department of Social and Health Services	WA	3,950	7/1/2011
State of Tennessee Sponsored Group Health Plan	TN	1,770	10/6/2011
Missouri Department of Social Services	MO	1,357	10/16/11
Department of Medical Assistance Services	VA	1,444	11/02/11
Kansas Department on Aging	KS	7,757	1/11/2012

Chapter 2 Background

Name of Entity Reporting Health Care Data Cyber Attack	State	Individuals Affected	Date of Breach
South Carolina Department of Health and Human Services	SC	228,435	01/31/12
Iowa Department of Human Services	IA	3,000	02/06/12
Utah Department of Health	UT	780,000	03/10/12
Hawaii State Department of Health, Adult Mental Health Division	HI	674	9/25/2012
State of California, Dept. of Developmental Services	CA	18,162	11/10/2012
Cabinet for Health & Family Services, Department of Medicaid Services	KY	1,090	11/15/2012
Calif. Dept. of Health Care Services (DHCS)	CA	2,643	12/10/12
Utah Department of Health	UT	6,332	01/10/13
WA Department of Social and Health Services	WA	629	2/4/2013
Indiana Family & Social Services Administration	IN	187,533	04/06/13
Iowa Department of Human Services	IA	7,335	4/30/2013
Illinois Department of Healthcare and Family Services	IL	3,133	5/8/2013
California Correctional Health Care Services	CA	1,001	6/19/2013

Source: Auditor of Public Accounts based on information available from the U.S. Department of Health & Human Services.

The following examples of attacks on state government agencies from around the country illustrate the seriousness of the threat and the necessity of treating security with a sense of urgency. As detailed in these examples, the cause of security breaches varies widely. In many cases, they are the result of a malicious attack. However, other breaches are the result of negligence or mistakes by Information Technology (IT) administrators or other government employees.

- In 2011, the Texas Comptroller reported that sensitive personal information of approximately 3.5 million residents was posted publically on a state server for over one year.
- In 2012, a Utah Department of Health server was breached by eastern European cyber attackers. The server had poor authentication controls in place, which resulted in the theft of sensitive or confidential health records containing the information of 780,000 citizens. According to a study of the Utah incident by a strategy and research firm, the total financial loss to consumers and businesses could be as much as \$406 million. Although retailers and banks will be responsible for the majority of this loss due to having to deal with fraud schemes put into motion by the breach, consumers could realize up to a quarter of the total loss.

Total financial loss due to theft of health records may cost Utah over \$400 Million

Chapter 2

Background

- In 2012, the Wisconsin Department of Revenue exposed the confidential data of 110,000 people through a Microsoft Access database file, which was inadvertently placed on a public-facing website.
- In 2013, the Washington State Administrative Office of the Courts reported that up to 160,000 social security numbers and up to one million drivers' licenses were exposed.
- In 2013, a laptop containing the healthcare records for 18,162 developmentally disabled individuals was stolen from the car of an employee of the California Department of Developmental Services.
- In 2013, a laptop and flash drive with the unencrypted personal and medical information of 7,757 people were stolen from the car of an employee of the Kansas Department on Aging.
- In 2013, approximately 6,000 Medicaid patients were notified by the Utah Department of Health that their data was stored on a flash drive that was lost by a third-party contractor while traveling.

3.3 million bank account numbers, 3.8 million social security numbers, and sensitive information of 700,000 businesses exposed in South Carolina security breach

As serious as all of the above incidents were, the largest breach in recent years involving state government took place in South Carolina in November 2012. The case, which illustrates the ramifications that can occur after a serious breach, involved the theft of 3.3 million bank account numbers, 3.8 million social security numbers, and the sensitive information of 700,000 businesses from the South Carolina Department of Revenue. It was determined the breach occurred as a result of a state employee with authorization to these records falling victim to an email phishing scam. Phishing scams occur when someone with malicious intent sends a seemingly harmless email designed to get the recipients of that email to either provide personal information or unknowingly install a virus or other malicious software (malware) that can be used to obtain valuable data.

In South Carolina's case, it was more than a month after the employee opened the malicious email before anyone noticed. In the meantime, the hacker used the employee's stolen credentials to remotely access the department's system and scour the network to find the most sensitive data. Finally, over a two-day period, the hacker sent 74.7 Gigabytes of data over the Internet. The incident may never have been discovered had it not been for the United States Secret Service notifying South Carolina officials that they suspected an attack had occurred.

Chapter 2

Background

South Carolina paid \$12 million for more than 1 million individuals to receive credit monitoring services

Shortly after the breach was discovered, the South Carolina Governor announced that each person impacted by the breach was eligible to receive one year of free credit-monitoring services. To date, more than a million individuals have signed up for this service, costing South Carolina \$12 million. In addition, the Governor commissioned a study by an outside vendor, which offered a number of recommendations to strengthen the state's cyber security. The estimated cost of implementing these recommendations was an additional \$14 million. The study, as well as legislative hearings after the breach, determined that the Department of Revenue failed to encrypt much of its data despite warnings to do so from one of its former cyber security officers. The password encryption system that experts agree would have likely prevented the attack from occurring cost \$12,000 and has since been installed. The \$12,000 cost to have properly secured this data is minuscule compared to the \$12 million cost to address the security breach and the loss of public confidence in government.

Data encryption to protect records would have cost \$12,000

The Auditor of Public Accounts (APA), as Kentucky's primary taxpayer watchdog, strongly encourages state and local agencies to take preventative efforts to implement strong cyber security policies and controls to reduce the risk of exposing sensitive and confidential data. The costs to pro-actively implement policies, controls, and security software into their procedures to reduce the risk of these incidents will far outweigh the loss of public confidence and the costs to clean up after an incident occurs. Governments can pay now to provide proper cyber security or pay more later after a breach has occurred.

Historical Events Reported Previously by IT Audit

The APA has identified and/or assisted in the investigation of multiple security breaches in state government over the last several years. Each of these events highlights the importance of implementing strong security controls over IT resources to mitigate actual or potential financial losses and data manipulation or destruction. In the absence of sufficient controls, these or other types of events could potentially be repeated.

The events discussed below can be categorized as:

- Existence of malicious software, also known as malware.
- Lack of sufficient password protection.
- Exposure of personally identifiable, confidential, or sensitive information.

Existence of Malicious Software (Malware)

Two examples below relate to the existence of malware on an agency's computer and the actions taken by individuals with bad intentions. Generally, malware attempts to take control of a computer, capture sensitive or confidential information, or cause the computer not to function as expected. Malware can be loaded onto a computer through various methods, including infected email messages, files, or websites.

Chapter 2

Background

Hackers stole over \$400,000 from Bullitt County Fiscal Court

- In 2009, the Bullitt County Fiscal Court had over \$400,000 stolen from a payroll account. This event was perpetrated by a foreign group of hackers that used a malware application on the Fiscal Court Treasurer's computer to identify her password to the county's online banking account. Using this information, the hackers were able to log onto the county's online banking account and create fake payroll transactions that transferred money from the Fiscal Court's account to their accomplices. There were a number of missing or weak controls in place, which, if functioning properly, would likely have kept this type of theft from happening.

Malware shuts down Kentucky county clerks' offices

- In 2007, more than 100 local government county clerks' offices throughout Kentucky were unable to issue drivers' licenses, renew vehicle registrations, or perform other functions because 77 county clerks' offices and other offices were infected with a specific type of malware. When this malware was detected, the Commonwealth Office of Technology (COT) instantly blocked the network connections from those offices in order to keep the malware from spreading to other government offices. It was determined the malware would have initially been detected if the county computers had installed up-to-date anti-virus software.

Lack of Sufficient Password Protection

This example relates to a situation where passwords were either not used or were not strong enough to keep unauthorized users from gaining access to the computer or application. Insufficient password controls can be caused by passwords being left as the manufacturer's default, no password being required, or the password policy not providing sufficient criteria detailing how to create a strong password that cannot be guessed or cracked with the help of specialized software.

- On July 29, 2003, the APA issued a news release revealing that a state agency network was breached by hackers. Agency computers were used approximately 6,000 times to visit and view pornographic websites or images, which were identified during a 4-day test period. During April 2003, and potentially prior to that date, French hackers entered the agency network through the agency Internet proxy server and used that machine to:
 - Store and distribute pirated new movies, music, TV shows, and new computer games.
 - Post and distribute pirated copyrighted French medical textbooks.
 - Host an Internet chat room.

Access to the agency network was traced to 33 routers/switches that did not have password protection controls in place. This exposed the agency and other connected state and federal computers to attack and exploitation. After gaining access to the system, hackers installed software and tools that gave them access to the passwords of core technology administrators and other agency employees.

Chapter 2

Background

Exposure of
Personally
Identifiable,
Confidential, or
Sensitive
Information

These examples relate to the unintentional release of information to the public or state employees that is considered sensitive, confidential, or is specifically attached to an individual. The exposure of these types of information could potentially put both the agency and the related individual at risk. Depending on the type of information released, the agency could potentially face a monetary fine, a loss of proprietary information, loss of public trust, and/or a heightened security risk to their facilities, staff, or clients. Further, an individual may be put at risk for identify theft, which could lead to multiple financial problems.

*Confidential data
posted on agency
website*

- In April 2012, a state agency upgraded its public website. During this upgrade, personally identifiable information (PII) was unintentionally posted to the website making it available to the public. When updating office contact information for the website, one of the agency offices provided a workbook that contained multiple worksheets. The first and third worksheets contained staff names and organizational units. The second worksheet contained names, social security numbers, birth dates, home phone numbers, and additional employee position data for current and former staff. Central level personnel responsible for reviewing and adding information to the website reviewed only the first worksheet, failing to identify the PII in the second worksheet. As a result, the workbook was published in its entirety on the agency's public website.

An employee realized the PII was available within two days of it being placed on the website and the workbook was removed within two hours of discovery. The agency worked with the website management vendor to ensure there were no remaining versions of the webpage available online. The agency confirmed the most frequently used Internet search engines deleted all versions of the webpage containing the PII six days after the workbook was removed. Access logs were also reviewed with the vendor to determine who had accessed the webpage while the PII was available. No suspicious website visitors were identified during this time period.

At the time of this incident, there was no agency level or state-wide policy or procedure in place to address this type of data exposure. In order to be proactive, the agency decided to notify the Office of the Governor, the Personnel Cabinet, and the Office of the Attorney General. The affected current employees were also notified by hand-delivered letter and former employees were notified by certified mail.

- Over the last five years, audits of agency machines available through the state's network found instances where access to saved files or documents was granted to any valid user within the state's network. In some cases, these files or documents contained information that would be considered sensitive, confidential, or personally identifiable information.

Chapter 2

Background

During the most recent fiscal year (FY) 2013 audit, we identified one state agency network domain with 40 machines that contained files or documents that the auditor could view. Two of these machines contained files that provided Internet Protocol (IP) addresses. We also noted a machine that provided IP and Media Access Control (MAC) address information, wireless router login information, an approved correctional facility inmate visitor listing, and 32 documents containing social security numbers. An additional machine was discovered that contained 55 documents with business IDs and passwords and a link to a website to update business data, as well as one document containing a social security number. These instances were immediately reported to the agency and corrective actions were taken by the agency to secure these machines.

20 Outlook public folders provided sensitive or confidential information

- In 2007, an audit of 1,600 Microsoft Outlook public folders available to be viewed on the state’s email system identified 20 public folders that were improperly managed, allowing calendar appointments, notes, emails, contact lists, file attachments, and tasks to be viewed by any valid users of the state’s network email system. Some of the items available within these folders included:
 - Social security numbers and names of certain state employees and private citizens.
 - Information related to certain correctional facilities’ parolees.
 - Information related to individuals in juvenile detention.
 - Transportation requests for children to attend medical appointments.

Additionally, over 3,400 emails were found in one email folder, many containing confidential information. An Auditor’s Alert was released at the end of this audit to address security controls over Microsoft Outlook public email folders.

- In 2005, a sample of computers sent to the Division of Surplus Property for release to the public revealed one computer contained confidential information, including the names, pictures, and social security numbers of thousands of state employees and other citizens who were issued access cards to state facilities.

Examples of Previous Recommendations Made to Strengthen Policies and Procedures

Over several years, the APA has provided a number of recommendations for strengthening controls and to reduce the risk of these types of events occurring. Some of these recommendations include:

- Install and keep anti-virus and spyware protection software current.
- Educate employees on basic security methods.

Chapter 2

Background

- Perform regular back-ups of data and storage in a secured off-site location.
- Keep software up-to-date with security/processing patches and versions.
- Ensure all software placed on an agency machine requires passwords for operation, if possible.
- Require all passwords to adhere to a complex syntax.
- Configure and monitor firewalls to control both traffic out of and into the agency network.
- Periodically perform vulnerability reviews to identify security weaknesses.
- Fix all identified security weaknesses.
- Avoid the use of remote access and, if used, implement controls to secure the system.
- Enable and monitor security features on wireless networking products.
- Require all agency staff to comply with the Enterprise Policy Chief Information Officer (CIO)-060, titled “Internet and Electronic Mail Acceptable Use Policy.”
- Develop procedures to approve the creation of public folders and ensure they are configured to be secure.
- Designate personnel to be trained and responsible for the establishment of email folders.
- Require agency staff to comply with the Enterprise Policy CIO-077, titled “Sanitization of Information Technology Equipment and Electronic Media,” which was superseded by the Enterprise Policy CIO-092, titled “Media Protection Policy” in October 2013.

Specifically related to the use of online banking services, the APA has also recommended the following general precautions to government agencies:

- Agency management should be aware of the online services, features, and security options that are available.
- Segregation of duties should be implemented.
- Changes to users’ access should be formally requested and approved by management based on the users’ job duties.
- Transactions should be reviewed regularly for unusual activity and investigated as necessary.
- Transactions should have multiple approvals and dual notification.
- A procedure manual for online banking should be developed and provided to staff.

As with all types of security, no single control or combination of controls exist that can totally secure systems or data; however, when agencies put in place controls, such as those discussed above, these precautions can reduce the risk of these types of events occurring and allow staff to quickly identify situations that do occur.

The APA employs professional IT audit staff dedicated solely to the performance of annual IT audits of critical automated systems and data located in agencies throughout state government. The assessment of whether these systems and data are properly secured is a primary focus within each of these audits. Significant testing of systems and application programs, including performing electronic scanning of systems, is performed to identify the existence of potential weaknesses or vulnerabilities that unnecessarily increase the risk of unauthorized access or exposure to systems and sensitive or confidential data. When weaknesses or concerns are found related to policies, system configuration, security controls, or other vulnerabilities, specific recommendations are made to the agencies to assist in strengthening the security of the system, program application, or data.

The FY 2013 series of IT audits found several instances where the security of agencies' systems, program applications, data, or IT resources was not sufficiently strong to protect the agency from actual or potential theft, unauthorized access, or change. These instances involve many diverse control areas. Each control area is addressed separately to summarize the various concerns found, the significance of the concerns to the overall system security of the agency, and the recommendations provided to the agency to strengthen controls. See Appendix 2 for a Summary of APA IT Audit Security Related Issues.

Data Protection

In three agencies, management had not specifically identified which data items owned or housed in their agency networks would be considered sensitive or confidential. One agency had initiated a project to begin this data classification process, but the project was expected to take at least two years to complete. Further, because this process must be completed to determine the proper level of security to apply, sensitive or confidential data housed by these agencies is likely not protected in compliance with the minimum standards established by COT.

Recommendations

We recommend all agencies review the data they own, are responsible for, or house in their networks to specifically identify those items of data that should be classified as sensitive or confidential. The criteria for classifying data have been established within the COT enterprise "Data Classification" standard. Once the data classification process has been completed, the COT enterprise "Encryption" standard requires that all sensitive data be encrypted as a necessary added layer of protection.

Summary of FY 2013 IT Audit Security Findings and Recommendations

**Network
Neighborhood**

One state agency network domain, a logical collection of machines within a network, with 40 machines was found to contain files that were viewed by auditors. Since the domain resides on the Commonwealth's wide area network (WAN), users with access to the state's network could have potentially viewed these files. Two of these machines contained files that provided specific configuration information about various machines. We also noted a machine that provided configuration information, wireless router login information, an approved correctional facility inmate visitor listing, and 32 documents containing individuals' social security numbers. An additional machine was discovered that contained 55 documents with account IDs and passwords and a link to a state website that maintains current business data, as well as one document containing a single social security number. These instances were immediately reported to the agency and corrective actions were taken by the agency to secure these machines.

Recommendations

We recommend agency management ensure that access to all network machines be configured to properly restrict access to only those staff requiring access to the housed applications or data. Periodic reviews of domain machines should be performed to ensure only proper access is allowed. Further, we recommend sufficient training is provided to appropriate agency staff to ensure they are aware of the risk of housing sensitive or confidential data and the steps they should take to ensure this information is properly secured.

Incident Handling

At one agency, the availability of a payment application used primarily by Commonwealth residents and businesses to make payments to the Commonwealth had a technical issue that allowed the personal information of at least 27 individuals to be exposed to other individuals logged into the application at the same time. Although the agency worked in collaboration with COT and the vendor supporting the application to identify the technical issues that could have caused this situation to occur, it was found that the agency did not create and submit to COT all documentation required by the COT enterprise "Information Security Incident Response" policy related to security incident handling. The agency did not retain the documentation of the testing performed to determine individuals affected. Further, copies of the letters issued to these individuals were not maintained, which is required by the agency's records retention schedule. As a result, the auditors could not independently verify the actions taken by the agency to address the issue and notify the individuals.

Recommendations

We recommend agencies consistently develop all documentation required by the COT enterprise "Information Security Incident Response" policy. For future security incidents, we recommend that sufficient documentation is created and retained to support testing performed and determinations made by staff. Further, any correspondence with individuals affected should also be maintained in accordance with the applicable record retention schedule.

Summary of FY 2013 IT Audit Security Findings and Recommendations

Logical Security

Logical security issues were identified with one or more systems at nine agencies. Logical security involves, but is not limited to, restricting access to only authorized users, strong password settings, and appropriate levels of access granted to a user. It is imperative that individuals using systems are provided the minimum access necessary to perform their job duties and that management has previously authorized this access. These restrictions are necessary since these systems process data critical to the state, which is sometimes sensitive or confidential. Several different aspects of logical security concerns were identified, each of which will be specifically addressed below.

Policies

Within six agencies, we noted multiple instances where established policies and procedures governing access to critical agency applications were not formally documented or the existing procedures were inadequate or incomplete. Without formal, written policies and procedures, users or management may inadvertently put the agency at risk by not understanding the actions they can and cannot take in relation to the agency data and/or resources.

Recommendations

We recommend that all policies and procedures related to logical security over applications and networks be detailed, complete, and approved by management. These documents should be kept current and communicated to staff, in order to ensure all key staff members are aware of their responsibilities.

Lack of Supporting Documentation

Within eight agencies, we noted some users did not have sufficient documentation on file to support the level of access granted to a system. The missing or incomplete documentation included items such as authorization emails, confidentiality agreements, or access request forms. Some request forms were incomplete or lacked the required approvals. Without complete documentation supporting the access request and approval by management, there is an increased risk that users will be provided inappropriate or excessive access to view or change data.

Recommendations

We recommend policies governing system access processes be updated and maintained so that IT staff are aware of the procedures in place to grant system access. Also, internal forms should be completed in their entirety to ensure appropriate access is granted to authorized individuals and to minimize any confusion regarding the level of access to be provided. Any supporting documentation such as emails, forms, etc., should be maintained as required by records retention schedules and in a central location for ease of review and necessary update.

Summary of FY 2013 IT Audit Security Findings and Recommendations

Inappropriate
Access

In seven agencies, we identified some users that were granted a higher level of access than was requested or was unnecessary based on their job duties and users who were granted multiple individual accounts without having a specific job requirement. Some security roles were established that permitted assigned users to perform multiple, differing job duties that, for proper segregation of duties, should not be performed together. Instances were identified where all agency users were granted administrator rights to their own machines, which give the user the ability to affect all machine settings or authorization levels. This access could potentially expose the network to applications that use a significant amount of the processing resources or contain harmful or malicious content.

Recommendations

We recommend IT staff only grant or assign the minimum level of access required for an employee to complete his/her job duties. Administrator access rights to individual machines should be limited to system administrators or IT security staff to limit the potential for downloading and installing unauthorized software.

Revocation of
Access

Documentation for system users who left state employment was also reviewed to determine whether their access to systems was revoked in a timely manner. In three agencies, we identified some users who retained access after employment separation. In some cases, the systems to which the users retained access also required a network logon, which had been deactivated. Access retained by employees who have left state employment increases the risk of intentional or unintentional misuse, manipulation, or destruction of data.

Recommendations

We recommend agencies remove or deactivate all user account access to their systems at the time an employee leaves the agency. Further, we recommend the agency implement a formal review process to ensure all user accounts are appropriately authorized. If this review reveals a user no longer requires network or system access, then the access should be removed or disabled immediately. Adequate documentation, such as a properly completed access form or email, should be maintained to support the removal of access.

Security Options
Configuration

We identified instances within one agency where the password associated with database security profiles did not match the COT enterprise “User ID and Password” policy for how passwords were to be structured. In addition, we found instances where the access to server accounts were not locked due to the excessive age of passwords, which was not in compliance with the COT enterprise policy requiring passwords to be changed within 30 days. For example, a user account was identified whose password was over 17 months old. If passwords are not changed frequently, it allows a potential attacker a longer period of time to try to access the account.

Summary of FY 2013 IT Audit Security Findings and Recommendations

Recommendations We recommend the agency develop a process for documenting the request for and the approval by management of password changes for any accounts that require a different password structure or length of time than established in the COT enterprise “User ID and Password” policy or agency-specific policy. Further, management should be made aware of and should consistently enforce these requirements.

**Vulnerability Scan
Performed to Test
System Security**

Annually, auditors perform a scan of agency devices to identify weaknesses, focusing on those machines where agency critical information is processed or stored, printers, and machines identified in the prior year audit as having control weaknesses. A scan is an automated audit test that uses multiple electronic security-related tools to evaluate the settings, configuration, and controls established on various machines to determine whether those machines are properly secured. We request listings of critical machines from each audited agency and use the various automated security tools to perform the scans of potentially hundreds of machines. As discussed below, the security concerns found by performing scans were:

- Server configuration.
- Authentication to devices.
- Software version control.
- Agency vulnerability assessments.

**Server
Configuration**

In eight agencies, several IT devices were found that were not securely configured. Some agencies failed to develop written procedures for the original configuration or for monitoring configuration changes to new desktops, laptops, mobile devices, and printers. Specifically, we found:

- Ports, points of access to a device, that were open with no apparent business purpose, some of which were known to be a frequent access point used by malicious software or malware.
- Ports typically used for web services that did not connect to a website currently in operation.
- Configuration settings within web services that could allow a user unnecessary control over data being allowed into and sent out from the device.
- Devices that provided the software product name and version that was running, which is more information than should be revealed.
- Multiple ports used to transmit data over the network in an insecure fashion were noted.

System misconfigurations increase potential security vulnerabilities and provide enticements for intruders to enter the system. Improperly secured services could allow unauthorized access to sensitive or critical system resources.

Summary of FY 2013 IT Audit Security Findings and Recommendations

Recommendations We recommend management ensure that all new agency devices are consistently setup based on the developed and approved standard configurations. Any variations to the base-line configuration should be approved by management and documented. Further, we recommend management perform periodic reviews of all agency devices to determine whether changes from the base-line configuration have occurred.

Authentication to
Devices

In three agencies, access was gained by the auditor to several devices as an anonymous user or through the default username and password established at the initial configuration by the application vendor. Some printers allowed the auditor to log on as the administrator, view stored documents, alter the printer settings, and change the administrator password, which would effectively give the auditor complete control over the printer settings and potentially any document images residing on it. Such a situation could potentially allow a user the ability to connect to other computing devices on the same agency network as the controlled printer. Administrative control was also available on other network devices, which could potentially allow a user with malicious intent to access other computing devices on the network or execute a DoS attack that would slow down or stop traffic from being transmitted between the agency and outside users. Such a situation would interfere with any services the agency provides to the public. As auditors, we did not exploit these weaknesses, but another individual could if the logons and passwords are not strengthened.

Recommendations We recommend all default usernames and passwords established at the initial configuration by the application vendor be altered by the agency upon installation of new computing devices. In addition, a password should be assigned to any computing devices that, by default, allow anonymous user access with no required password. Passwords should be strong and structured in accordance with the COT enterprise "User ID and Password" policy or the agency policy, if stronger than the COT enterprise policy. If an agency policy is in place, we recommend it contain the requirement that all default credentials must be changed upon installation and passwords be assigned to services that, by default, do not require a password.

Further, as future computing devices are installed on the agency's network, they should be reviewed for open communication channels and services to verify that all default credentials have been altered and do not allow access without a required password.

Summary of FY 2013 IT Audit Security Findings and Recommendations

Software Version Control

In eight agencies, no policy was in place for regularly reviewing software installed on computing devices to ensure it is up-to-date. Once software is installed, any new version released by the vendor should be considered for update. Since hackers constantly try to identify software security flaws that would potentially allow them to gain access to computing devices, vendors attempt to fix flaws identified in the newest versions. If an agency fails to proactively update its software and it remains outdated, it is potentially open to attack. This could possibly allow a user with malicious intent to access a computing device, disrupt the processing of the software, or use the machine to perform unauthorized actions through a particular program or its operating system.

Recommendations

We recommend each agency create a software version control policy. This policy should include the procedures for monitoring all critical software installed on agency computing devices to ensure it is up-to-date. The policy should provide the instructions to download, test, and install the necessary update if software is determined to be outdated. The personnel responsible for each step in this process should be included in this policy. Additionally, the policy should have a requirement of a periodic review of computing devices to ensure software versions are current. Finally, if outdated software must be retained due to other system requirements, the policy should establish a process to document these instances, the reasoning behind this determination, and management’s approval.

Agency Vulnerability Assessments

Two agencies did not have a policy in place requiring them to periodically scan their computing devices for security weaknesses. Furthermore, regular security scans were not performed on computing devices within these agencies. The COT enterprise “Critical Systems Vulnerability Assessments” policy requires agencies to perform biennial vulnerability assessments on the agency computer network and servers to ensure they are appropriately secured against known security weaknesses.

Recommendations

We recommend each agency create a policy to address the performance of security scans, distribute the policy to key security personnel, and ensure adherence to the agency policy and to the COT enterprise “Critical Systems Vulnerability Assessments” policy for vulnerability assessments. The security scan policy, at a minimum, should address the frequency of scans, the overall scope of the scans, documentation retention, and requirements for correcting issues identified in the scans.

**Password Policies
and Audits**

Ten agencies did not perform regular reviews to determine the strength of network user account passwords despite COT having an enterprise “Password Auditing and Policy Enforcement for Network Domains” in place that requires quarterly password reviews to ensure they are strong enough to not be easily guessed or cracked. Additionally, COT did not adhere to its own policy during the fiscal year and stated there were technical issues that prevented the correct information from being obtained. Subsequent to audit fieldwork completion, we learned that COT resolved the technical issues and password reviews are expected to begin in the fall of 2013. We also identified multiple agencies whose password composition and use requirements were incomplete, incorrect, or were inconsistent with the established procedures. Weak or easily guessed passwords could potentially allow unauthorized access to agency data and resources.

Recommendations

We recommend each agency create a policy to require regular network user account password strength reviews to ensure all network passwords are adequately secure so they cannot be easily guessed or cracked by a computer program. Once implemented, each agency should institute a periodic review process with scheduled reviews to follow. Results of these password reviews should be maintained for audit purposes.

Further, specific to those agencies whose password composition and use requirements were found to be lacking, we recommend the established procedures be reviewed and strengthened as necessary to conform to the COT enterprise “Password Auditing and Policy Enforcement for Network Domains” with strict adherence to follow. If there is a business need for a noncompliant user password, the rationale should be thoroughly documented and approved by management.

**Segregation of
Duties**

In five agencies, instances were found where users were granted the ability to perform more than one job duty that, for proper segregation of duties, a single person should not be allowed to perform at the same time. This situation could potentially result in the processing of transactions without the required approvals being applied; unauthorized modification of files, data, and programs; or intentional or unintentional actions taken within the data processing system that could change or remove data. Examples of users with excessive or inappropriate access include users who share an account that allows the users to administer the system and users who have been provided access rights to perform administrative, operational, and/or programming functions within the system. For example, a programmer should not also have administrative rights to a system because it would provide the opportunity for unauthorized program changes to be made without the knowledge and approval of management.

Summary of FY 2013 IT Audit Security Findings and Recommendations

Recommendations We recommend agencies review access rights provided to staff and make changes to access rights to ensure proper segregation between administrative, operations, development, and programming functions. Further, we suggest management look at the responsibilities assigned to individual staff to determine whether there are ways to reallocate job duties among existing staff to place separation between these functions.

Wireless Networks

One agency did not develop or implement a policy governing the security of its wireless networks. The agency had an existing “Wireless Device Usage Policy;” however, it focused on the types of wireless devices, such as cell phones and other handheld devices, used to connect to wireless networks. The policy failed to identify the agency’s wireless networks, provide configuration requirements for the networks, and address the granting of access to the networks. Without consistently following strong policies and procedures surrounding the setup and security of wireless networks, an agency can potentially present an easy access point to their network resources and data to unauthorized users.

Recommendations We recommend the agency develop a written policy explaining security measures implemented for their wireless networks. The location of WAPs used to obtain access to the agency’s wireless networks, configuration and security settings, and access restrictions should be documented within the policy. This will ensure that all employees and visitors are aware of the security measures in place for the agency’s current wireless networks and any future installations. The policy should be reviewed and updated as configuration settings are altered or new security measures are implemented.

Security Policy

Two agencies did not have comprehensive IT control policies and procedures in place to govern critical agency applications. One of the agencies adopted a policy; however, it was incomplete and did not address all aspects of application security associated with the agency’s data processing system. The remaining agency has a decentralized governance model, which does not allow adequate oversight authority to implement IT control policies and procedures to secure all IT resources of the agency’s business units. The lack of formalized, written IT control policies and procedures could result in users or management misunderstanding their responsibilities, leading to inconsistent or incomplete controls over the agency network and IT resources.

Summary of FY 2013 IT Audit Security Findings and Recommendations

Recommendations We recommend the agency establish an overarching IT governance authority, such as a Chief Information Security Officer, that is responsible for designing and implementing standard IT controls and providing centralized oversight of these controls for all IT resources, if they have not done so already. For all agencies, this authority should ensure security-related policies and procedures are formalized and distributed to the underlying offices and departments to ensure awareness of their responsibilities in relation to IT controls. These policies and procedures should be reviewed on a regular basis to ensure they are complete and accurate.

**External Audit
(Cloud Security)**

One agency contracted with an outside vendor to support and maintain a critical agency program and the associated database in the vendor's data center; however, the agency did not ensure an external audit of the vendor's data center was completed. In the absence of an external security review, the agency can place no reliance on the security of the program and database since they have no physical oversight of these resources. If the physical or logical security at a vendor's data center is inadequate, it could potentially allow agency data to be exposed to unauthorized users or co-mingled with other entities' data housed and maintained by the vendor.

Recommendations We recommend the agency determine whether an external audit of the vendor's data center has been performed. If an external audit was not performed, the agency should contract with a third party vendor to perform a security review of the vendor's data center with emphasis on the state agency's data. Once complete, a copy should be made available to the APA.

**Security Log
Monitoring**

Many internal processes log activity on the system, including changes made to data, when users log on and off, incorrect login attempts, and other data that is setup to be monitored. In order for this information to be useful, it should be monitored for any suspicious activity. One agency performs this monitoring using software they purchased, and it was confirmed the software complies with federal regulations for performing security reviews on servers containing federal information. However, there is not a policy in place to require this review, to establish how often it is required, to define the type of review that should be performed, or the amount of time the logs should be kept. We also found no other individual was assigned as a backup to perform the monitoring in the event the individual responsible is out of the office. Two additional agencies were identified that had no formal procedures in place to periodically review security audit logs. Regular review of the logs by agency staff can assist in timely identification of unauthorized access attempts, changes made to application data or programming, or potential security breaches.

Summary of FY 2013 IT Audit Security Findings and Recommendations

Recommendations We recommend agencies create a written policy governing the security log monitoring process for the servers in which critical agency data resides. Further, a backup for the current reviewer should be appointed and provided training to allow this individual to perform the required tasks. This process also applies to federal data housed or processed by state agencies.

Physical Security

One agency did not have adequate physical security measures in place to protect agency data and resources. Adequate physical security controls should be in place to ensure that access to an agency's facility and IT resources is restricted to authorized employees only. An external vendor performed a security assessment and identified several physical security concerns. These concerns were confirmed to still exist during APA auditors' walk-through of the agency's facilities.

Recommendations We recommend agencies implement formalized physical security policies to ensure IT resources are adequately secured. Where applicable, a surveillance system should be in place that will allow security personnel to monitor the parking lot as well as doors to the building. System wiring closets that provide system and network connectivity should be free of clutter and only used for electrical purposes. We further recommend agencies implement background checks on all external staff with access to their IT resources and facilities.

Chapter 4

Finance and Administration Cabinet's Commonwealth Office of Technology Chief Information Security Office Cyber Security Initiatives

Enterprise Policies

The Commonwealth Office of Technology (COT) is charged with ensuring the confidentiality, integrity, and availability of the Commonwealth's computing environment. KRS 42.724 gives the Office of the Chief Information Security Officer (CISO) the responsibility to ensure the efficiency and effectiveness of IT security functions and responsibilities.

Enterprise policies articulate the rules and regulations of state government regarding IT. These policies determine the type of activities that are approved for both agencies and employees. The Enterprise IT policies that include the Security policies are located at <http://technology.ky.gov/governance/Pages/policies.aspx> and are also listed in Appendix 3.

The Security Office is implementing an Enterprise Information Security Program Policy this year that provides clearly defined, measurable, and enforceable security controls that can be consistently applied at an enterprise level. The Enterprise Information Security Program Policy is enacted to align with the security framework of the National Institute of Security Standards (NIST) Special Publication 800-53. The purpose of this policy is to provide a security framework to create security safeguards, best practices and standards. This policy also offers a dynamic security plan to protect the Commonwealth's infrastructure and critical assets. In addition, the adoption of this common framework and its controls for the Commonwealth offers several advantages that include agencies sharing a common vocabulary and common set of concepts related to information security controls, which will improve communication and understanding with and among the agencies. Other advantages include common standards for auditing, common methods for compliance monitoring, and greater insight into the overall security posture of the Commonwealth.

Commonwealth Cyber Security Collaboration

The Commonwealth of Kentucky is an active member of the *Multi-State Information Sharing and Analysis Center (MS-ISAC)*. The CISO is the administrator for the Commonwealth. The mission of the MS-ISAC is to improve the overall security posture for state, local, territorial and tribal governments. MS-ISAC provides collaboration and information sharing among members, private sector partners and the U.S. Department of Homeland Security. Being in MS-ISAC, COT has two-way sharing of information and early warnings on cyber security threats. MS-ISAC provides a process for gathering and disseminating information on cyber security incidents.

The Commonwealth hosts meetings every two months on *Cyber Security Information Sharing*. The goal of these meetings is to tighten partnerships and to discuss the current landscape of cyber security issues and ways to strengthen the Commonwealth's defense.

The Commonwealth is an active participant with the *National Association of State Chief Information Officers (NASCIO)*. The Commonwealth also actively participates in the NASCIO Security and Privacy Committee that meets monthly. NASCIO is a professional organization for all state CIOs, which fosters a continual exchange of state information that includes cyber security.

Chapter 4

Finance and Administration Cabinet's Commonwealth Office of Technology Chief Information Security Office Cyber Security Initiatives

The Commonwealth works closely with the *U.S. Department of Homeland Security* and *Kentucky Department of Homeland Security*. The Commonwealth attends bi-monthly secure video teleconferences. This program shares classified cyber security information with appropriately cleared members. The program establishes the means to share classified level cyber security information. This capability provides federal and state governments with information on critical cyber security risks as well as federal-state collaboration and communication on cyber security issues, both current and future.

Active Cyber Security Initiatives

Every year, Governor Beshear proclaims October as Cyber Security Awareness Month for Kentucky. Associated with this effort, COT distributes security awareness posters, bookmarks and calendars from MS-ISAC across state government. During the month, COT hosts several sessions on security for all interested state staff to increase awareness.

Over the past two years, a third-party security assessment of the Commonwealth's security posture has been conducted. In addition, COT has participated with the U.S. Department of Homeland Security in a Cyber Resilience Review. From the results of the assessment and review, COT's Security Office has implemented a Security Roadmap which outlines risk areas based on priority and cost evaluation.

COT has implemented several improvements over the past year from the Security Roadmap that include:

1. An Incident Response Policy and Plan for the Enterprise. This policy establishes the necessity and procedures for agencies and COT to identify security incidents when they occur and to notify appropriate personnel.
2. Security Awareness and Training
 - a. Security staff are trained and certified on security.
 - b. A security video will be available by the end this year to all state employees on security awareness.
 - c. Security training will be implemented this year for all COT staff to cover the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), and overall IT security awareness.
3. Infrastructure baseline security measures. The baseline measures help secure the network from potential intrusion.
4. Several security policies and standards that cover the enterprise information security program, incident response, data classification, encryption standards and media protection.

The Security Office also has active partners that COT works with closely on proactive activities to identify and correct potential areas of weakness across the Commonwealth's infrastructure.

Chapter 4

Finance and Administration Cabinet's Commonwealth Office of Technology Chief Information Security Office Cyber Security Initiatives

Governor Beshear signed Executive Order 2012-880 "Regarding the Centralization of Information Technology Infrastructure Resources across the Commonwealth," which directs the executive branch to adopt a centralized IT infrastructure services model. The adoption of a centralized model intends to improve security, promote information sharing, and assist agencies in focusing on their mission rather than operations issues. Some of the primary benefits of this action are: cost savings, reduced risk, better positioning for the future, and improved services. The security and infrastructure consolidations are expected to reduce the Commonwealth's risks associated with system failure and privacy or security breaches. The full executive order is available at <http://finance.ky.gov/initiatives/ITinfrastructureinitiative/Pages/default.aspx>

COT undergoes several audits every year conducted by the Internal Revenue Service (IRS), Center for Medicaid Services (CMS), Social Security Administration (SSA), and APA. These audits cover areas within security such as access control, physical security, and data protection. COT has created a Risk and Compliance group that will specialize in IT compliance needs and ensure that exceptions from the audits are addressed appropriately for the enterprise.

COT, the U.S. Department of Homeland Security, and the Kentucky Department of Homeland Security are planning a Cyber Tabletop Exercise. The goal of the exercise is to complete an assessment of the Commonwealth of Kentucky's current cyber security plans, policies, and procedures prior to and during a cyber-attack, focusing on the abilities to prevent, minimize, confine, or contain damages, and to enhance rapid recovery.

In conclusion, it is vital that work continues on strengthening the security posture of the Commonwealth. This includes the partnerships along with the Security Roadmap and the Centralization of the IT Infrastructure. These efforts will continue to reduce risks and improve the overall security posture of the Commonwealth.

Cyber Legislation

According to the Congressional Research Service report, “Cybersecurity: Authoritative Reports and Resources,” as of June 2013, at least fifty federal laws had provisions related to cyber security. In the last three Congresses alone, 111th through 113th, over 100 cyber security bills and resolutions were introduced. However, none of these became law. In fact, over a decade has passed since any comprehensive federal cyber legislation has passed.

While the federal government was unable to pass comprehensive cyber legislation, 46 states passed what are known as breach notification laws. Currently, the four states without a breach notification law are Alabama, South Dakota, New Mexico, and Kentucky. These laws require businesses and/or government entities to notify individuals if their personal information was jeopardized or at risk of being jeopardized due to a security breach. California was the first state to pass a breach notification law, Senate Bill (SB) 1376, in 2002. While these laws vary from state to state, the vast majority of these laws follow the basic template set forth by California. The primary purpose of these laws is to:

- Define what constitutes a breach.
- Define what constitutes “personal information.”
- List the types of entities that must abide by the breach notification laws.
- Set forth a process for entities to notify individuals affected by a breach.
- Set forth the type of information that should be encrypted.
- Exclude entities already subject to federal laws that include breach notification provisions.
- Set forth penalties for entities that do not comply with these laws.

California’s breach notification law has become the template from which most other states have modeled their own legislation. These laws are viewed by many policy experts as a baseline for state cyber security efforts. See the National Conference of State Legislatures Heat Map that identifies the strength of states’ breach notification laws at Appendix 4. However, this is by no means the only cyber legislation enacted. Other state-enacted legislation that broadly falls under the category of cyber legislation addresses:

- Computer crimes.
- Child pornography.
- Cyber-bullying and cyber-stalking.
- Identity theft.
- Social media.
- Crimes dealing with physical damage to computers.
- Crimes against computer users.

The good news is that Kentucky has a number of laws related to the areas discussed above. The bad news is that breach notification laws have twice been proposed in the Kentucky legislature, in 2006 and 2008, and twice failed to pass. Although such laws do not cover all government cyber security concerns, they represent a significant step toward protecting citizen privacy rights and should motivate governments to increase their cyber security efforts.

When governments collect sensitive personal information that, if compromised, could result in identity theft or other serious consequences, the governments also have the responsibility to make efforts to protect that data. Despite the most well-intentioned efforts, security breaches, unfortunately, will still likely occur. When they do, governments have a responsibility to notify all individuals impacted by the breach. After all, it is the individuals' data, and they will be forced to deal with the ramifications of having it compromised.

Recent national headlines related to the National Security Agency revelations and Chinese and Russian hackers attacking businesses and government entities have facilitated the discussion of cyber security threats. During the 2014 Kentucky legislative session, the General Assembly has the opportunity to assist in ensuring the security of its constituents' personal, health, business, and other information. To that end, the APA will be working with the General Assembly to draft new breach notification legislation.

Without specific legislation to require accountability for reporting cyber security breaches, there are no means of determining the financial impact or other consequences to the Commonwealth and its citizens. When considering cyber security, the question must be asked “[a]re we willing to pay now or pay more later?”

Each of the items identified below represent activity that is either a blatantly malicious attack or a condition that creates an unnecessary risk.

External or Internal threats:

- DoS (Denial of Service) – sending either specially crafted material or large amounts of general material to a host with the intention of overwhelming its ability to operate on a network or to provide services.
- Social engineering – applying psychological techniques to people with the intention of eliciting information that will assist in furthering an attack.
- SQL (Structured Query Language) injection – submitting crafted material that is intended to be passed to a database where the material is misinterpreted as database commands that either alter the data or return it to the submitter.
- XSS (Cross Site Scripting) – planting malicious code in a public area, such as web page comments, discussion forums, etc., with the intention that unsuspecting visitors will compromise their systems by executing that code.
- Buffer overflows – sending highly specific material to a networked application with the intention of over-filling the application's input buffer in such a way that it begins to execute code contained within that material.
- Intentional data destruction – deleting, flagging as unused space, or wiping files. Wiping files destructively over-writes content with new material.
- Ransomware – maliciously encrypting files so that the owner can no longer access those files until a ransom is paid and the attacker decrypts the files making them again accessible to the owner.
- Default or trivial access credentials – failing to change account names and passwords from their factory defaults, allowing unauthorized access to anyone who can find those defaults online or in product manuals.

External only threats:

- Phishing – posting emails and/or web pages that purport to be a known and trusted entity, such as a bank, and then soliciting confidential information such as account names and passwords.
- War-dialing – automated phone calling to a group or range of phone numbers with the intention of identifying fax machines, modems, and similar devices that may be connected to an internal network that can be used to by-pass the normal perimeter defenses, such as firewalls and switches.
- War-driving – scanning a geographic area for WAP that might allow access to otherwise protected networks.

Internal only threats:

- Malicious insider – staff, temps, janitors, disgruntled employees, vendors, etc.
- Shoulder surfing – the practice of watching a person type their password in order to misuse it later.
- User errors – opening unsolicited email (phishing) or browsing malicious web sites.
- User negligence – becoming a victim of social engineering or establishing trivial passwords.
- Improperly configured or managed hardware and software.
- Outdated or unpatched software.
- Unsecure programming practices.
- Unsecured openings in network perimeter (ports).
- Rogue wireless access points – WAPs installed without authorization and without the knowledge of the network's owner/operator.
- Rogue or unknown modems – modems installed without authorization or the knowledge of the network's owner/operator.
- Unintended information leakage – the unintended posting of information (sensitive, confidential, or informational) that can either aide in furthering an attack or mistakenly exposes information.
- Ineffective or absent internal controls, including lack of separation of duties, excessive access rights, or nonexistent or weak policies.

Security Category	FY 2013 (11 agencies audited)	FY 2012 (10 agencies audited)	FY 2011 (10 agencies audited)
Vulnerability Scan			
<i>Server Configuration</i> 2	8 agencies (6 repeats)	6 agencies (5 repeats)	7 agencies (6 repeats)
<i>Authentication to Devices</i>	3 agencies (2 repeats)	5 agencies (3 repeats)	4 agencies (4 repeats)
<i>Software Version Control</i> 1	8 agencies (3 repeats)		
<i>Outdated Software w/Vulnerabilities</i> 1		3 agencies (3 repeats)	4 agencies (2 repeats)
<i>Information Leakage</i> 2		3 agencies (3 repeats)	6 agencies (3 repeats)
<i>Vulnerabilities</i>		1 agency (no repeats)	
<i>Security Banner</i>		1 agency (1 repeat)	2 agencies (2 repeats)
<i>Enticement</i>			2 agencies (2 repeats)
Anti-Virus		1 agency (1 repeat)	1 agency (1 repeat)
Microsoft Outlook Public Folders			1 agency (1 repeat)
Network Neighborhood	1 agency (1 repeat)	1 agency (1 repeat)	1 agency (1 repeat)
Security Policy	2 agencies (2 repeats)	1 agency (1 repeat)	2 agencies (1 repeat)
External Audit	1 agency (no repeats)		
Logical Security			
<i>Logical Security Policies</i>	6 agencies (10 separate comments - 5 repeats)	5 agencies (11 separate comments - 11 repeats)	5 agencies (10 separate comments - 10 repeats)
<i>Lack of Supporting Documentation</i>	8 agencies (13 separate comments - 6 repeats)	6 agencies (9 separate comments - 8 repeats)	8 agencies (14 separate comments - 12 repeats)
<i>Inappropriate Access</i>	7 agencies (9 separate comments - 5 repeats)	6 agencies (10 separate comments - 8 repeats)	7 agencies (12 separate comments - 11 repeats)
<i>Revocation of Access</i>	3 agencies (no repeats)	2 agencies (2 repeats)	2 agencies (2 repeats)
<i>Security Options Configuration</i>	1 agency (2 separate comments - 2 repeats)	4 agencies (5 separate comments - 4 repeats)	3 agencies (5 separate comments - 5 repeats)
Security Log Monitoring	3 agencies (3 repeats)	4 agencies (5 separate comments - 5 repeats)	5 agencies (6 separate comments - 5 repeats)
Physical Security	1 agency (no repeats)		
Website Content Review		1 agency (no repeats)	
Segregation of Duties	5 agencies (3 repeats)	5 agencies (6 separate comments - 4 repeats)	3 agencies (5 separate comments - 5 repeats)
Agency Vulnerability Assessments 3	2 agencies (no repeats)		
Password Policies and Audits 3	10 agencies (no repeats)		
Wireless Networks 3	1 agency (no repeats)		
Data Protection 3	3 agencies (no repeats)		
Incident Handling 3	1 agency (no repeats)		

- 1 - Prior to FY 2013, issues related to outdated software with publicly known vulnerabilities were reported in the "Outdated Software with Vulnerabilities" comment. In FY 2013, we refocused this comment toward the agency's policies and procedures for managing software updates. Therefore, the comment title changed to "Software Version Control."
- 2 - Prior to FY 2013, issues related to information leakage were reported in the "Information Leakage" comment. In FY 2013, we refocused this comment toward the configuration involved in securing information that should not be provided to anonymous users. Therefore, this type of issue is now included in the "Configuration" comment along with other configuration issues.
- 3 - During FY 2013, we performed additional audit procedures of reviews of agency policies, procedures, and controls related to vulnerability assessments, password policies and audits, wireless networks, data protection, and incident handling. Therefore, there were no comments related to these issues previous to FY 2013.

Enterprise IT policies are created and issued by COT. These information technology policies establish the rules and regulations to be followed by Executive Branch state government agencies and employees.

The following descriptions were taken from the COT Enterprise IT Policies website, <http://technology.ky.gov/governance/Pages/policies.aspx>.

- **CIO-060 -- Internet and Electronic Mail Acceptable Use Policy**
Revised 03/19/2013. Effective 05/15/1996.
This policy is to define and outline acceptable use of Internet and Electronic mail (E-mail) resources in state government.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-5282/>
- **CIO-061 -- Social Media Policy**
Revised 03/19/2013. Effective 07/01/2011.
This policy is to define and outline acceptable use of Social Media resources in state government.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-350018/>
- **CIO-071 -- Wireless Voice and Data Services Policy**
Revised 03/19/2013. Effective 09/12/2001.
This policy defines deployment and acceptable use of wireless devices within the Executive Branch of state government.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-3922>
- **CIO-072 -- User ID and Password Policy**
Revised 08/26/2013. Effective 06/01/2002.
This policy supports the Enterprise Architecture for end-user security and represents a set of standards to be followed by all employees for User ID and Password usage.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-13212>
- **CIO-073 -- Anti-Virus Policy**
Revised 08/22/2008. Effective 06/01/2002.
The purpose of this policy is to help protect all computing devices from malicious software (viruses, Trojans, worms, hoaxes).
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-13213>
- **CIO-074 -- Enterprise Network Security Architecture Policy**
Revised 11/01/2005. Effective 12/01/2002.
The purpose of this policy is to describe enhancements to the Enterprise Network Security Architecture to realign resources in the most appropriate security environment.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-13211>
- **CIO-075 -- Enterprise IT Project Approval Process**
Revised 01/07/2010. Effective 09/01/2002
This policy is intended to enhance the probability of IT project success across the enterprise.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-13727/>

- **CIO-076 -- Firewall and Virtual Private Network Administration and Content Filtering Policy**
Revised 03/19/2013. Effective 01/01/2003.
The administration of firewalls, virtual private networks (VPNs), and content filtering is a primary component in securing the infrastructure and must conform to this policy.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-13776>
- **CIO-078 -- Intranet Wireless Local Area Network (WLAN) Policy**
Revised 03/01/2013. Effective 06/10/2003
The purpose of this policy is to outline security and data integrity measures required for secure wireless LAN installations within the state's intranet zone.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-21536>
- **CIO-079 -- Logon Security Notice**
Revised 11/01/2005. Effective 04/01/2004.
This policy is intended to protect the confidentiality, availability, and integrity of the Commonwealth's information technology resources, by requiring all logon screens include a security notice indicating that the system must be used for authorized purposes only.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-35941/>
- **CIO-080 -- Password Auditing and Policy Enforcement for Network Domains**
Revised 11/01/2005. Effective 04/01/2004.
This policy has been enacted to outline the audit processes required to identify security vulnerabilities and threats as they relate to domain password usage and to measure compliance with the enterprise policy, User ID and Password Policy (CIO-072).
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-35938>
- **CIO-081 -- Securing Unattended Workstations**
Revised 03/19/2013. Effective 04/01/2004.
This policy requires all workstations utilizing the Kentucky Information Highway (KIH) to be adequately secured when unattended, in order to protect the confidentiality, availability, and integrity of the Commonwealth's information technology resources.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-35939>
- **CIO-082 -- Critical Systems Vulnerability Assessments**
Revised 11/21/2008. Effective 05/15/2004.
The purpose of this policy is to establish procedures for network vulnerability assessments of the servers and operational environments of critical systems by state agencies utilizing the KIH.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-37850>
- **CIO-083 -- Storage of Confidential Information on Portable Devices and Media**
Revised 03/19/2013. Effective 01/18/2010.
This policy requires all portable computing and storage devices containing confidential data to be encrypted in order to protect the confidentiality, availability, and integrity of the Commonwealth's information technology resources.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-326883>

- **CIO-084 -- Email Review Request**
Revised 07/28/2009. Effective 03/28/2005.
The purpose of this policy is to provide procedures for cabinets/agencies to follow when requesting a review of an employee e-mail account.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-50065>
- **CIO-085 -- Agency Security Contact**
Effective 08/01/2005.
The intent of this policy is to ensure the establishment of a formal communications link between COT and the organizational entities that use COT services.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-67586/>
- **CIO-086 -- State Agency Local Print Policy**
Revised 07/11/2013. Effective 09/01/2008.
Where it does not impede the ability of state workers to conduct agency business, this policy directs agency staff to make conscious decisions to print only where there are tangible benefits for printed output, and, when printing is necessary, to print in black and white and in duplex.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-278424>
- **CIO-087 -- Internet Usage Review Request Policy**
Revised 07/28/2009. Effective 01/07/2009.
The purpose of this policy is to provide procedures for agencies to follow when requesting a review of an employee's Internet usage.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-301611>
- **CIO-090 - Information Security Incident Response Policy**
Effective 03/05/2013.
This policy identifies the necessity and procedures for agencies and COT to identify and notify appropriate personnel when a security incident occurs.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-378586>
- **CIO-091 – Enterprise Information Security Program**
Effective 10/07/2013.
This policy has been created to align the Commonwealth's Enterprise Information Security Program with the security framework of the current NIST Special Publication 800-53 Security and Privacy Controls.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-383208>
- **CIO-092 – Media Protection Policy**
Effective 10/07/2013.
This policy ensures proper provisions are in place to protect information stored on media, both digital and non-digital, throughout the media's useful life until its sanitization or destruction.
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-383209>

During the FY 2013 review, the following Enterprise Policy was also in place. This policy has since been superseded by **CIO-092 – Media Protection Policy** listed above and has been removed from the policy website.

- **CIO-077 -- Sanitization of Information Technology Equipment and Electronic Media Policy**
Revised 03/19/2013. Effective 02/05/2003.
The purpose of this policy is to ensure secure and appropriate disposal of information technology equipment, devices, network components, operating systems, application software and storage media belonging to the Commonwealth to prevent unauthorized use or misuse of state information.

Why Storing and Protecting Data Is Important: Evaluating State Data Breach Notification Laws

Holding Out

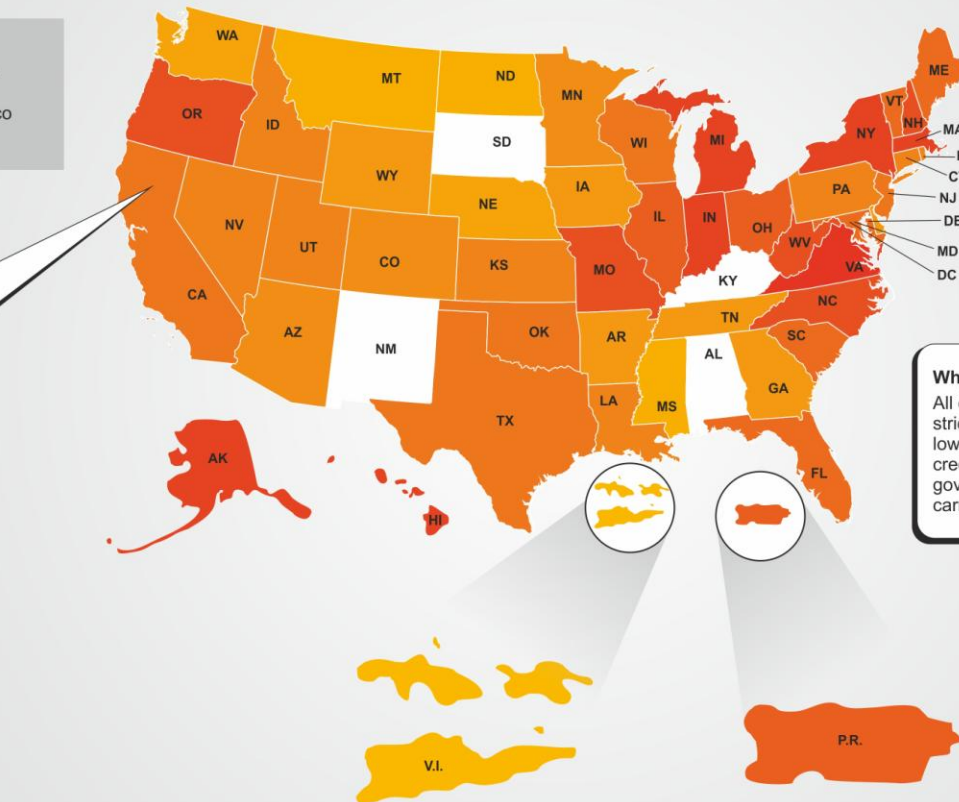
Four states have yet to enact a data breach notification law: Alabama, Kentucky, New Mexico and South Dakota.

The Original Standard

California was the first state to enact data breach notification legislation. The law went into effect on July 1, 2003. Outside the scope used in this analysis, California's laws include provisions specifically for credit reporting agencies and for businesses owning or maintaining medical data. Other states carry these provisions as well.

Why Certain States Stand Out

All of the laws are strict, but the stricter laws include a relatively low bar triggering notification to credit reporting agencies and government entities. They also carry higher maximum fines.



*Note: A score of zero means a data breach notification law does not exist in that state.

State	Score
AL	0
KY	0
NM	0
SD	0
V.I.	5
ND	6
MS	7
MT	7
NE	7
WA	7
AR	8
DE	8
GA	8
IA	8
TN	8
WY	8
AZ	9
CO	9
MN	9
CT	10
ID	10
KS	10
LA	10
NV	10
PA	10
RI	10
UT	10
CA	11
NJ	11
OK	11
TX	11
WI	11
DC	12
FL	12
MD	12
ME	12
SC	12
VT	12
IL	13
OH	13
P.R.	13
MO	14
NC	14
NH	14
OR	14
WV	14
AK	15
HI	15
IN	15
MA	15
MI	15
NY	15
VA	16

Less strict More strict

Key: The darker the state, the more strict the law



SOURCE: Imation Corp. based on evaluation of individual state laws obtained via National Conference of State Legislatures website and evaluations available publicly online from various law firms.
 NOTE: This information should not be considered legal advice and is not based on a legal analysis of the laws. Check with your attorney regarding laws applicable to your business.
 As of July 2, 2012.
 Imation is a global scalable storage and data security company. For more information, visit: www.imation.com/compliancemap

