PERFORMANCE AUDIT REPORT

State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2014-2016)

A Report to the Legislative Post Audit Committee
By the Legislative Division of Post Audit
State of Kansas
December 2016

R-16-014

Legislative Division of Post Audit

The **Legislative Division of Post Audit** is the audit arm of the Kansas Legislature. Created in 1971, the division's mission is to conduct audits that provide the Legislature with accurate, unbiased information on the performance of state and local government. The division's audits typically examine whether agencies and programs are effective in carrying out their duties, efficient with their resources, or in compliance with relevant laws, regulations and other requirements.

The division's audits are performed at the direction of the **Legislative Post Audit Committee**, a bipartisan committee comprising five senators and five representatives. By law, individual legislators, legislative committees, or the Governor may request a performance audit, but the Legislative Post Audit Committee determines which audits will be conducted.

Although the Legislative Post Audit Committee determines the areas of government that will be audited, the audits themselves are conducted independently by the division's professional staff. The division's reports are issued without any input from the committee or other legislators. As a result, the findings, conclusions, and recommendations included in the division's audits do not necessarily reflect the views of the Legislative Post Audit Committee or any of its members.

The division conducts its audit work in accordance with applicable government auditing standards set forth by the U.S. Government Accountability Office. These standards pertain to the auditor's professional qualifications, the quality of the audit, and the characteristics of professional and meaningful reports. The standards also have been endorsed by the American Institute of Certified Public Accountants (AICPA) and adopted by the Legislative Post Audit Committee.

LEGISLATIVE DIVISION OF POST AUDIT

800 SW Jackson
Suite 1200
Topeka, Kansas 66612-2212
Telephone: (785) 296-3792
Fax: (785) 296-4482
Website: **http://www.kslpa.org**

Scott Frank, Legislative Post Auditor

HOW DO I REQUEST AN AUDIT?

By law, individual legislators, legislative committees, or the Governor may request an audit, but any audit work conducted by the division must be directed by the Legislative Post Audit Committee. Any legislator who would like to request an audit should contact the division directly at (785) 296-3792.

The Legislative Division of Post Audit supports full access to the services of state government for all citizens. Upon request, the division can provide its audit reports in an appropriate alternative format to accommodate persons with visual impairments. Persons with hearing or speech disabilities may reach the division through the Kansas Relay Center at 1-800-766-3777. The division's office hours are 8:00 a.m. to 5:00 p.m., Monday through Friday.

LEGISLATURE OF KANSAS

LEGISLATIVE DIVISION OF POST AUDIT

800 SOUTHWEST JACKSON STREET, SUITE 1200
TOPEKA, KANSAS 66612-2212
TELEPHONE (785) 296-3792
FAX (785) 296-4482
WWW.KSLPA.ORG

December 7, 2016

To: Members, Legislative Post Audit Committee

Senator Michael O'Donnell, Chair	Representative Virgil Peck, Jr., Vice-Chair
Senator Anthony Hensley	Representative John Barker
Senator Laura Kelly	Representative Tom Burroughs
Senator Jeff Longbine	Representative Peggy Mast
Senator Julia Lynn	Representative Ed Trimmer

This report contains the findings and conclusions from our completed performance audit report, *State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2014-2016)*. We would be happy to discuss the findings or any other items presented in this report with any legislative committees, individual legislators, or other state officials.

Sincerely,

Scott Frank
Legislative Post Auditor

This report was created by Alex Gard, PMP, CISA; Clyde Meador, SSCP, and Michael Nixon, CISSP. Katrin Osterhaus, PMP, CIA, CGAP, was the audit manager. If you need any additional information about the report's findings, please contact Alex Gard at the Division's offices.

Legislative Division of Post Audit
800 SW Jackson Street, Suite 1200
Topeka, Kansas 66612

(785) 296-3792
Website: www.kslpa.org

Table of Contents

List of Figures

List of Appendices

State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2014-2016)

State agencies collect, maintain, and process a wealth of confidential information in their computer systems to perform their work. Examples range from individuals' social security numbers to educational information, and from medical and tax information to financial information used to process paychecks and child care assistance benefits.

Agencies use multiple security layers to protect data and computers from cyber or physical attacks. These layers include locked doors, employee badges, network firewalls, and user passwords. These controls should be evaluated periodically to ensure the agency's sensitive data is sufficiently protected from accidental or intentional data breaches.

State agencies have a significant amount of autonomy in how they develop, apply, and monitor these security controls. The Kansas Information Technology Executive Council (ITEC) has developed standards across various security areas including security awareness training, access controls, and physical and environmental safeguards. These standards were created to ensure state agencies develop adequate security controls. However, agencies have a significant amount of autonomy in how they develop, apply, and monitor these security controls.

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

> **Do selected agencies adequately comply with applicable information technology security standards and employ adequate controls for emerging technologies?**

As part of the audit work at each agency, we did the following to evaluate the agencies' security controls. We interviewed agency officials and security staff, performed a series of vulnerability scans on agency workstations, servers, and websites, reviewed applicable policies and procedures, reviewed employee files for evidence of IT security training and other relevant documentation, and observed agencies' data centers security environments. We also performed limited social engineering tests for agencies that volunteered to participate. Our review of internal controls was designed to evaluate whether agencies set up appropriate

expectations and structures to adhere to applicable requirements and best practices.

We issued reports to each agency throughout the three-year audit cycle as soon as the work was completed. The individual audit reports to those agencies are confidential under K.S.A. 45-221 (a)(12) because the information they contain could jeopardize the agency's IT security.

This report presents a summary of our findings from audits on 20 individual agencies from July 2014 through December 2016. It was not conducted in accordance with generally accepted government auditing standards.

Our findings begin on page 7, following a brief overview of IT security.

Most State Agencies Maintain Confidential or Sensitive Information

We surveyed all state agencies to identify those that maintain sensitive data and created an inventory of the systems that house that data. Of the 100 agencies we surveyed, 75 maintained some form of confidential or sensitive information.

- 71 agencies maintained Personally Identifiable Information (PII), such as names, addresses, and dates of birth
- 40 agencies maintained tax information
- 36 agencies maintained Protected Health Information (PHI)
- 28 agencies maintained student-related records protected under the Family Educational Rights and Privacy Act (FERPA)
- 18 agencies maintained credit card information

As the results demonstrate, most Kansas agencies collect and maintain at least some sensitive information. Some of this data has significant penalties for loss or disclosure. For example, compromised health information can range from $100 per violation (up to $25,000 per year) to $250,000 and 10 years in prison. To protect it, safeguards must be put in place to prevent unauthorized access from both outside and within the agency.

State Agencies Are Consistently Targeted Because They Maintain Valuable Information

Several recent security reports have observed that hackers target government entities because they maintain valuable confidential information. For example, a 2016 data security report from Verizon shows government agencies at the top of the list for cyber-espionage, ahead of manufacturing, professional, and information services industries. Similarly, a May 2016 report by the Department of Homeland Security confirmed cyber criminals exploit university networks because of their multiple levels of connectivity and accessibility among students and faculty. Additionally, an August 2016 alert by the Federal Bureau of Investigation asked states to check their voter database online security based on breaches in Illinois and Arizona voter registration databases. Finally, according to an October 2016 article in by the Pew Charitable Trusts, local and state governments were struck by as many as 450 ransom attack infections a month between October 2015 and May 2016.

Hackers may target a specific state agency because of the confidential information it maintains. Some agencies make enticing targets because hackers know they maintain large amounts of confidential information such as credit card information, social security numbers, and tax data. Hackers specifically target these agencies to steal and resell their information on the black market.

Hackers also use broad attacks against numerous networks and sort out the information they collect afterwards. Instead of targeting any one specific entity, hackers use automated software to search the Internet for active servers they can gain access to. Once access is gained, the hacker typically collects all the information they can, then sort it out later to see if there is anything of value. (This is the cyberattack version of a car thief who tests every car door looking for an unlocked car they can steal.) In addition, once a hacker gains access to a system, they can continue to exploit ways to gain increasingly valuable data as long as they remain undetected.

Confidential data can also be compromised from within an agency. Although many IT security controls are intended to prevent network access from outside an agency, some are also designed to help limit employees' unauthorized access to confidential information. Specifically, they help protect confidential data from theft and help ensure that only authorized staff can view it. When those controls are not in place, staff may be able to view sensitive data they should not have access to, or they could intentionally extract confidential data for personal gain.

In addition, agencies often provide third-party contractors rights to certain data. If the agency does not take proper steps to protect itself through such things as proper non-disclosure agreements, background checks, and access monitoring, the risk increases that sensitive or confidential data may fall into unauthorized hands.

OV-1
Insufficient Security Controls Lead To Lost or Stolen Data Across State Governments

The following examples illustrate that state agencies are not immune to security failures, which can lead to data loss and costly remediation:

- **In 2012, the South Carolina's Department of Revenue was hacked because an employee clicked on an embedded and malicious link in an email**. The malware allowed hackers to steal nearly 3.6 million social security numbers and nearly 400,000 credit and debit card numbers. Strong security policies and procedures, including awareness training, may have prevented this incident.

- **In 2014, confidential information from the Oregon WorkSource Management Information System was compromised.** The Oregon Employment Department received an anonymous tip about a vulnerability and identified intrusion of its WorkSource Information System (the state's public workforce system to help individuals find jobs, increase skills, and explore training options). Social security numbers, addresses, and other information usually found on job applications from roughly 850,000 individuals were compromised. Risk and security assessments, and proper software application controls may have prevented this incident.

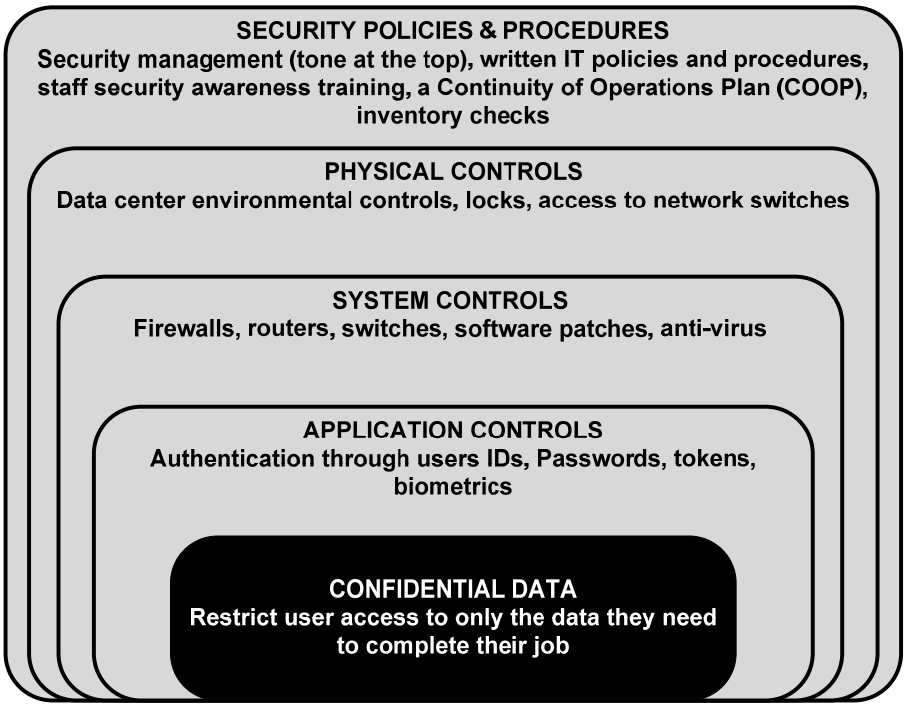
- **In November 2014, the Texas Health and Human Services Commission had an "unauthorized disclosure" incident.** This occurred when a former contractor did not turn over computer equipment and paper records containing Medicaid and health information for 2 million individuals. Stringent third party contracting processes, including specific termination procedures, may have prevented this incident.

Insufficient security controls have led to lost or stolen information from several state governments. Security controls help ensure that sensitive information is not lost, stolen, or compromised. When controls are not implemented properly, security incidents can occur. ***Figure OV-1*** on page 4 provides several examples of security incidents at state agencies in recent years. These events can cost millions in fines and penalties, credit monitoring, security upgrades, and lost confidence in state government.

Agencies Should Use a Multi-Layered Approach to Protect Their Confidential Information

To protect against data loss or theft, agencies should implement integrated layers of IT security controls. ***Figure OV-2*** below summarizes the various security layers that agencies often rely on to secure confidential information. As the figure shows, security layers are composed of different controls including IT policies or software applications. Using multiple layers of security requires unauthorized individuals to overcome numerous barriers to reach sensitive or confidential information. Even if one layer is compromised, the others still protect the system.

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



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

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

The State of Kansas has developed standards for each security layer to help agencies develop a robust system to protect confidential and sensitive data. The Legislature statutorily created the Information Technology Executive Council (ITEC) in 1998 to set IT standards for state agencies. ITEC comprises 17 members from all three branches of state government, as well as local governments and private businesses. To help protect confidential data, ITEC has developed security standards that represent the minimum requirements for state agencies. In 2014, ITEC revised those standards which, among other things, now require the Board of Regents' institutions to abide by those requirements. When designed and implemented properly, following the standards helps create multiple security layers to help prevent security failures.

Agencies Must Use Limited Resources To Balance Their Business Needs Against Security Risks

Implementing security controls takes staff time and may require additional IT assets. While some security controls can be implemented without large capital investments, almost all controls require sufficient staff time to develop, monitor, and evaluate. For example, agencies need staff to write or revise policies and procedures, provide security awareness training to agency employees, monitor incidents, and perform vulnerability scanning of agency machines. Some security controls also require continuous financial resources for such things as upgrading firewalls, replacing outdated operating systems on computers or servers, and purchasing anti-virus or mobile device management software.

Additional IT controls often can reduce speed or limit functionality, creating a tradeoff between business needs and security risks. Even well-designed IT controls can be inconvenient. For example, having to change a user password every 90 days or being locked out from repeatedly entering a password incorrectly help protect the system, but both controls can be disruptive to an employee's work.

Agencies must evaluate and understand their security risks to be able to make informed decisions. Threats from the outside (new viruses or malware, phishing attempts, or denial of service attacks) as well as threats from the inside (a new application system, changes in retention policies, staff turnover), must be evaluated and reevaluated repeatedly. Agencies should perform periodic risk assessments to identify existing or new vulnerabilities. In turn, they should use the results to evaluate which vulnerabilities need to be addressed, balancing the need to address the risk against the cost of new controls. Limited agency budgets make this balancing act even more difficult.

Do Selected State Agencies Have Adequate IT Security Processes to Ensure That Confidential Information is Protected?

Two-thirds of the 20 agencies we reviewed between 2014 and 2016 did not substantively comply with applicable IT security standards (page 7). Agencies failed to implement certain IT security controls resulting in high-risk or critical vulnerabilities (page 10). For example, few agencies properly scanned their workstations and servers or patched known vulnerabilities, thus increasing the number of weaknesses hackers might exploit (page 10). Many agencies used unsupported software or had vulnerable websites, creating risks which can be difficult to mitigate (page 11). Half the agencies had poor access and environmental controls for their data centers, therefore increasing the risk of data loss (page 13). Several agencies did not adopt strong password settings increasing the risk for brute force attacks (page 14). Additionally, several agencies did not adequately protect their network boundaries or did not sufficiently protect their systems from malicious code (page 15), and they did not conduct background checks or follow security protocols for departing staff, which could lead to security incidents (page 16). Lastly, many agencies did not conduct security awareness training, and our social engineering tests demonstrated a lack of understanding for security protocols (page 18).

13 of 20 Agencies We Reviewed During 2014-2016 Did Not Substantively Comply with Applicable IT Security Standards

We audited 20 agencies during the past three-year IT audit cycle. Through our survey of all state agencies at the start of 2014, we assessed the inherent security risk for each agency. Agencies that processed payments, or had a large amount of confidential data such as protected health information, tax information, or educational records generally were considered the riskiest.

We selected 20 agencies for review between 2014 and 2016 using our risk assessment and the results from our previous IT audits. ***Figure 1-1*** on page 8 lists the audited agencies, as well as their staffing and total expenditures for fiscal year 2016. As the figure shows, most of the agencies were relatively large and provide a variety of critical services.

This cycle of IT audits measured compliance with a larger number of security controls than our past audits. Our office has conducted IT security audits since early 2000. Through 2013, those audits generally focused on a handful of security processes at each agency. We decided to evaluate a much broader number of security controls to gain a more comprehensive understanding of each agency's security posture. In all, we evaluated about 50-100

security processes at each agency. Those processes were based on the state standards promulgated by the Kansas Information Technology Executive Council (ITEC), but also included a few best practices in emerging areas such as relying on unsupported software and operating systems, website vulnerabilities, and policies for using mobile devices. ***Appendix A*** on page 22 provides an overview of the types of processes we evaluated as part of each agency audit.

Figure 1-1
2014-2016 IT Security Audit Cycle
List of Audited Agencies (a)

Agency Name	Number of FTE Staff (FY 2015)	Expenditures (FY 2015) (b)
Department of Transportation	2,738	$2,016,000,000
Department on Aging and Disabilities Services	257	$1,515,200,000
University of Kansas	5,342	$868,700,000
Kansas State University	3,862	$718,500,000
University of Kansas Medical Center (c)	2,716	$336,100,000
Department of Labor	420	$335,800,000
Wichita State University	2,017	$321,700,000
Kansas Board of Regents	63	$215,900,000
Department of Corrections (d)	480	$202,400,000
Department of Revenue	1,072	$119,400,000
Emporia State University	798	$90,400,000
Department of Wildlife, Parks and Tourism	341	$65,800,000
Department of Agriculture	320	$49,300,000
Kansas Neurological Institute	462	$26,400,000
Parsons State Hospital	467	$26,400,000
Kansas Insurance Department	126	$26,300,000
Kansas Corporation Commission	195	$19,200,000
Office of the Bank Commissioner	106	$10,600,000
Kansas Commission on Peace Officers' Standards and Training (e)	7	$800,000
Kansas Dental Board	3	$400,000

(a) The individual audit reports are confidential under K.S.A. 45-221(a)(12).
(b) Rounded to the nearest $100,000
(c) This included the main campus and the Wichita campus, conducted as a separate Part II audit which was more limited in scope.
(d) The audit excluded the individual correctional facilities.
(e) This agency volunteered for the audit to better understand its security posture.

Source: Governor's Budget Report, Fiscal Year 2017, Vol. 2

About two-thirds of the agencies (13 of 20) did not sufficiently comply with applicable IT security standards and had not employed adequate controls for emerging issues. The seven

agencies that passed our audit had few critical or high-level findings. Conversely, the 13 agencies that did not pass our audit had numerous critical or high-level findings.

It is important to recognize that not all IT controls are created equal. For example, not requiring employees to sign an acceptable-use policy prior to using an agency system is not as critical as wiping confidential information from computers that are being decommissioned. ***Figure 1-2*** below describes how we categorized control weaknesses (vulnerabilities) from low to critical risk. As the figure shows, we considered vulnerabilities to be critical when they created an imminent threat for data loss. Other vulnerabilities were considered low risk. These were either unlikely to occur or the impact to the agency would have been insignificant.

Figure 1-2
Categorization of Findings by Level of Severity

We classified each control weakness we identified through our audit work into one of the following five categories of vulnerability based on two dimensions, defined below:

- Likelihood refers to a vulnerability being exploited or acted upon now or in the future.
- Impact refers to the effect an exploited vulnerability would have on the agency in terms of its operations, remediation cost, or reputational damage.

CRITICAL: Vulnerabilities that create an imminent threat for data loss (destruction, inaccessibility) or theft, because the detected vulnerability has a high likelihood of occurring, and the impact would have critical consequences for the agency or the state. The agency has no or ineffective mitigating controls to reduce the vulnerability status.

HIGH: Vulnerabilities that create a threat for data loss (destruction, inaccessibility) or theft, because the detected vulnerability has a probable or possible likelihood of occurring, and the impact would have severe consequences for the agency or the state. Additionally, the agency has minimal or ineffective mitigating controls.

MODERATE: Vulnerabilities that create a moderate threat for data loss (destruction, inaccessibility) or theft, because the detected vulnerability can have varying levels of likely occurrence, but the level of impact on operations to the agency or state moderate that likelihood. The agency may have mitigating controls that reduce the risk level.

LOW: Vulnerabilities that create a low threat for data loss (destruction, inaccessibility) or theft, because the detected vulnerability is either probable to cause a security incident, but the impact of such event is trivial, or the likelihood of the vulnerability creating a security incident is low, but the impact could have severe consequences for the agency or the state. The agency may have mitigating controls that reduce the risk level.

TECHNICAL ISSUES: Weaknesses in an agency's documentation or security processes that do not strictly adhere to ITEC standards.

Agencies Failed to Implement Certain IT Security Controls Resulting in High-Risk or Critical Vulnerabilities

Problems in a handful of areas led to the most severe vulnerabilities. ***Figure 1-3*** below includes a "heat map" which summarizes the findings from the 20 audited agencies. The figure ranks security areas based on the highest number of critical findings, with the color scheme indicating the frequency of critical findings from highest (dark red) to none (dark green). The same color scheme is used for each of the remaining vulnerability levels to highlight which security areas had the highest and lowest numbers of findings. As the heat map shows, areas of greatest concern were systems operations, emerging issues, and physical security.

Figure 1-3
Heatmap of IT Security Findings Across 20 State Agencies (CY 2014-2016)

Security Areas	Critical (a)	High	Moderate	Low	Total
Systems Operations	8	11	34	2	55
Emerging Issues (b)	7	10	20	19	56
Physical Security	3	11	18	11	43
Access Control	3	10	22	40	75
Systems Configuration	3	9	21	17	50
Personnel Security	3	8	23	29	63
Security Awareness Training	0	11	10	16	37
Data Protection	1	4	11	14	30
Continuity of Operations Planning	0	3	14	0	17
Risk Assessment/Security Planning (c)	0	0	10	11	21
Incident Response	0	0	13	8	21
System Audit (c)	0	0	4	11	15
Total Number of Vulnerabilities	**28**	**77**	**200**	**178**	**483**

(a) This heatmap is sorted based on the highest to low est number of critical vulnerabilities across the 12 areas.
(b) Emerging Issues includes unsupported softw are and unsecured w ebsites, as w ell as mobile device, social media, and cloud provider controls.
(c) Security Planning and System Audit w ere not evaluated in 2016.
Source: LPA summary of IT security audit reports of 20 agencies conducted from July 2014 to December 2016

SYSTEMS OPERATIONS

Few Agencies Properly Scanned Their Workstations and Servers or Patched Known Vulnerabilities, Increasing the Number of Weaknesses Hackers Might Exploit

Over time, vulnerabilities in computer software are discovered that could allow someone to break into or otherwise harm an agency's network. Software manufacturers are constantly developing "patches" for these vulnerabilities as they are discovered. A basic function of an organization's IT staff is to scan their computers to identify vulnerabilities, then test and apply patches to keep the systems secure. ITEC requirements mandate this process should occur a minimum of once every six months.

At each agency, we used vulnerability scanning software to identify unpatched vulnerabilities on a sample of workstations and servers. We excluded recently discovered vulnerabilities from our

analysis, as well as unpatched vulnerabilities for which the agency had valid business reasons for not applying the patches. We focused on high and critical vulnerabilities. Our standard for workstations was an average of 10 or fewer critical and high vulnerabilities per machine, with a stricter standard of two or fewer vulnerabilities per server for the systems we reviewed.

Most agencies had too many unpatched vulnerabilities. During this three-year audit period, we found most agencies had a high number of patchable vulnerabilities. It was not uncommon to see an average of 20 critical and high-risk vulnerabilities per machine, which is twice the number of vulnerabilities we considered acceptable. We saw several agencies exceeding our threshold much further. For example, one agency had an average of 46 vulnerabilities on machines that were directly controlled by the IT department. The results were even worse for computers that not directly controlled by the IT department–241 vulnerabilities per machine. In several agencies, Microsoft vulnerabilities accounted for most of the critical and high vulnerabilities, even though those are generally the easiest to fix.

Agencies often lacked the knowledge, resources or management support to scan and patch computers adequately. In some cases, staff did not know about the scan and patch requirements, or lacked the knowledge, tools or time to perform the work. In numerous instances, we learned staff did not have automated patching processes for Microsoft or third-party software, or did not set up patching processes properly. In other cases, pushback from other agency staff contributed to problems with installing patches.

Without a systematic approach to identify and patch vulnerabilities, agencies leave their systems open to attack from hackers. New vulnerabilities are discovered daily and can only be addressed through an effective scan and patch process. Hackers can send infected email attachments to unsuspecting users to exploit unpatched vulnerabilities and gain access to an agency's network. This risk is often elevated when the agency also lacks other controls, such as proper security awareness training or systemic anti-virus protection.

EMERGING ISSUES

Many Agencies Used Unsupported Software or Had Vulnerable Websites, Creating Risks Which Can Be Difficult to Mitigate

Vendors must constantly update operating systems and software to prevent newly discovered vulnerabilities from being exploited. Eventually, keeping those systems current becomes ineffective, so the vendors announce a date when they will stop releasing updates for the software. Once that date occurs, the software is considered

"unsupported" by the vendor, which is also known as having reached "end of life."

More than half of the agencies continued to use at least some computers with unsupported operating systems. For example, several agencies continued to use one or more systems with Windows Server 2003 (which reached end of life in July 2015) or Windows XP (which reached end of life in April 2014). We learned several agencies did not know those computers were still in use, did not know the extent to which they were in existence, or did not sufficiently prioritize the upgrades. In other cases, we learned the machines ran programs or lab equipment that were incompatible with newer operating systems, but IT staff did not always know about or take steps to reduce the risks.

Agencies also continued to use applications that were no longer supported by the vendor. Our scans frequently found unsupported software on the computers we scanned. For example, one agency had outdated versions of Adobe Acrobat and Internet Explorer software, while another agency had many machines with an XML Parser driver that had reached end of life. In this instance, staff did not know how to remedy the issue because there was no automated solution.

At least four agencies maintained websites with high or critical security issues. Websites need to be reviewed periodically to ensure they are hardened against the latest forms of attack. Our reviews detected several websites with known vulnerabilities such as Heartbleed, POODLE, DROWN, BEAST, and FREAK. ***Appendix B*** on page 24 provides a brief description of these problems. In several instances, IT staff did not know how to monitor websites for vulnerabilities and were surprised to learn of the free tools available for this.

Unsupported operating systems and software as well as unsecured websites represent known and unknown risks to the agency. When operating systems and software become unsupported, the vendor does not provide necessary patches for vulnerabilities that hackers develop on a continuous basis. Agencies can mitigate these risks by segregating those machines from the agency's network. However, this action generally reduces intended business functions or leads to inefficiencies. As a result, upgrading or replacing hardware and software is the best way to mitigate unknown risks associated with unsupported operating systems or software, but also tends to be costly. Similarly, websites with outdated security features can allow attacks ranging from a defaced website to severe business disruptions.

Half the Agencies Had Poor Access and Environmental Controls for Their Data Centers, Increasing the Risk of Data Loss

Agencies typically use data centers to house critical information system hardware. Those discrete physical locations frequently contain highly sensitive information. ITEC standards require agencies to restrict physical access to authorized persons only, and to employ environmental controls to prevent or mitigate damage from water, fire, temperature, and humidity.

Ten agencies did not properly restrict access to their data centers, resulting in critical or high-risk vulnerabilities. In several instances, agency IT staff did not know who had access to the data center, or had not reviewed or updated their lists to ensure only authorized staff had access. For example:

- **Too many people had access to some data centers.** The data center at one agency allowed access for about 260 staff (including individuals from several other agencies) that the agency was not aware of.

- **Agencies allowed generic badges for accessing their data centers.** Generic badges such as "Temp Card 1" or "Front Office" are not tied to a specific person accessing the restricted area. For example, one agency's access lists included 15 generic accounts for the main data center, and six generic accounts for the alternate data center. Without mitigating controls, this increases the risk that an agency cannot trace a problem or incident to a specific individual.

- **Staff did not remove computer rights or data access.** In a couple of instances, keys or electronic badges for staff who had received temporary data center access had not been properly removed. At another agency, 14 departed staff still had data center access, and agency staff could not prove their badges had been reclaimed or destroyed.

- **The agency did not secure the data center.** One agency's data closet was consistently unlocked and left open (due to ventilation issues) to all agency employees as well as maintenance staff servicing the building.

Several agencies' data centers lacked proper environmental controls. For example, one data center lacked appropriate fire suppression or water controls, despite water pipes running through the data center and pipes having burst previously. Another agency's data closet was missing water, fire, temperature and humidity controls, and those issues had been identified at least six years prior to our audit.

Agencies' lack of understanding contributed to inadequate data center controls. Agency staff often lacked policies or procedures for reviewing access rights periodically. Additionally, IT officials often did not implement sufficient controls because

they did not consider the risks posed by internal staff to compromise data or hardware in the data center either intentionally or unintentionally. Lastly, several agencies mentioned funding issues as a limiting factor for missing environmental controls.

Poor or non-existent physical controls increase the risk that agencies' data center assets or information could get lost, stolen, or damaged. When staff do not understand physical controls requirements for their data centers, or do not place sufficient priority on ensuring compliance, the agency is at a heightened risk of data loss from intentional or accidental breaches, as well as environmental risks such as a fire. Depending on the agency's mission, this could severely disrupt services.

ACCESS CONTROL

Several Agencies Did Not Adopt Strong Password Settings, Increasing the Risk for Brute Force Attacks

Using passwords to control access to networks and computers is inherently risky because it is a weak way to authenticate users. Despite this risk, passwords remain the most common form of authentication because they are less expensive than stronger alternatives, such as biometric and two-factor authentication. ITEC standards prescribe several access controls including password strength, length, lifespan, and lockout. ***Figure 1-4*** below provides a summary of the key access control rules we reviewed.

Figure 1-4
Key Access Control and Account Management Requirements Related to Identification and Authentication

Feature	Description
Unique System Identifier	All users of information systems processing sensitive data should have a unique system identifier (user name or user ID).
Password Length and Complexity	Passwords with a minimum of eight (8) characters cannot contain the user ID, and must have complexity. Complexity means the password must contain three of four of the following categories: - Uppercase characters - Lowercase characters - Numbers - Special characters (neither letters nor numbers)
	Passwords without complexity must be a minimum of sixteen (16) characters in length.
Password Lifespan	Passwords must be changed at least once every 90 days.
Password Attempts	Information system accounts must be restricted to a maximum of five (5) consecutive failed attempts before being locked out. Additionally, accounts must remain locked out for a minimum of thirty (30) minutes.

Source: ITEC Policy 7230A, section 9

Seven agencies had inadequate password settings, resulting in critical or high-risk vulnerabilities. We saw agencies that had weak settings on password length or complexity, did not require users to change their passwords, or did not appropriately lock users out after typing in a wrong password too many times. For example, one agency did not have a lockout function and the password complexity rule was not enabled. Another agency did not control password settings for Apple machines on the network. Those machines' default password settings did not have password expiration or lockout features enabled. Lastly, at least two agencies had shared accounts, allowing multiple people to log into the same account, making it impossible for improper transactions to be traced to a particular individual.

IT staff frequently cited pushback from users as the reason those controls were not implemented. It can be difficult to convince users new security controls such as complex passwords are necessary. Other (non-security) IT or management staff may overrule the necessity of these controls for the sake of efficiency. Lastly, several staff told us they did not implement password requirements because those requirements were incompatible with other applications. In those cases, staff generally had not attempted to fix the compatibility problem, implement compensating controls, or document their acceptance of the unmitigated risks.

When fewer access control mechanisms are in place, the risk increases that an agency's network could be hacked through a brute force attack. In a brute force attack, attackers use automated software to repeatedly guess a user's password until they are successful. The best protection against a brute force attack is to require strong passwords which are difficult to figure out and enable the lockout setting which will quickly interrupt the attack after a few unsuccessful tries.

SYSTEMS CONFIGURATION

Several Agencies Did Not Adequately Protect Their Network Boundaries or Did Not Sufficiently Protect Their Systems from Malicious Code

ITEC standards require agencies implement network boundaries (firewalls) with the ability to monitor and control network communications. As part of proper boundary protection, agencies also should create different security zones. This allows trusted communications within the agency while keeping outside communications from reaching servers or computers within the trusted zones.

At least four agencies did not set up their firewalls properly. One agency did not have a proper zone for its outward facing server, which was placed on the agency's trusted network. This could allow hackers to access the agency's network from the

outside. Several other agencies had a firewall, but they were not configured properly. Additionally, agencies did not always have the capacity to properly monitor and log network communications.

At least six agencies had poor anti-virus protection. Malicious code protection and periodic scanning with anti-virus software protects machines from being infected with such things as viruses, worms, and Trojan horses. ***Appendix B*** on page 24 provides a brief description of these problems. Such malicious code can delete files, replicate to other computers across the network, access and steal sensitive data or hold agency data for ransom. We saw several problems in this area:

- **Not all machines were protected.** In one agency, 14 of the 139 scanned machines we sampled did not have anti-virus software installed. Additional machines at that agency had anti-virus products that were not managed through the IT department, and in some cases were outdated. Several other agencies had anti-virus procedures and monitoring on Windows-based machines, but lacked software or authority to install or centrally manage anti-virus software for servers or Apple computers.

- **Not enough files were scanned.** Several agencies scanned computers weekly as required, but the anti-virus scan was not deep enough to ensure computers were free of issues.

- **Users could circumvent or disable the anti-virus software on their machines.** In one agency, users could purchase computers without going through the central IT department, resulting in IT staff being unaware and unable to outfit those computers with the appropriate anti-virus software. In other agencies, users could disable the software and often did to increase the computers' performance.

Each of these problems creates a hole in the agency's security posture. Without systematic protection and monitoring, malware can infiltrate computers and damage or compromise information without the owners' consent or knowledge. Additionally, one infected machine can quickly infect others on the agency's network, which increases the risk of unauthorized access or data compromise.

PERSONNEL SECURITY

Several Agencies Did Not Conduct Background Checks or Follow Security Protocols for Departing Staff, Which Could Lead to Security Incidents

One best practice we evaluated concerned background checks for individuals with access to data centers or other sensitive areas. State law requires background checks for the Office of the Information Technology Services (OITS) data center in Topeka, and a Criminal Justice Information Services (CJIS) security policy requires a background check for anyone accessing a data center

that holds or processes unencrypted criminal justice information. Other standards also support this security control.

At least four agencies did not background check everyone who had access to their data centers. For example, one agency had several data centers with criminal justice information. However, our analysis showed 22 employees with access to one of its data centers had not received the federally required fingerprint check. At another agency, we found 24 of the 30 custodial and maintenance staff from the Department of Administration with data center access had not been background checked.

Several agencies did not have processes to retrieve badges, keys, or computers from departing staff. Not ensuring those items are retrieved may appear harmless, but could result in a security incident. Here are several examples of what we saw:

- **One agency did not ensure it retrieved electronic badges.** For three former employees whose badges we specifically looked for, their supervisors told us none of the three badges had been reclaimed. These badges could be used to gain physical access to several secured areas within agency facilities.

- **Another agency did not have a working process to ensure keys to buildings were returned.** For two of ten employees in our sample, the agency could not demonstrate the keys were requested back. For a third employee, the request for keys was not sent until nearly two months after their departure. These keys provided access to buildings that housed protected health information.

- **A third agency did not have a systematic process to ensure staff returned computers.** For one of five former employees in our sample, IT staff were unaware her computer had not been returned until we inquired about it. Aside from the value of the computer itself, it could have contained local files of confidential information.

Several agencies did not disable or deactivate building or computer access in a timely fashion. Agencies should eliminate unnecessary permissions or revoke system access to employee or contractor accounts when individuals are transferred or terminated. At one agency, we found the badges for 7 of 12 former employees in our sample were not deactivated timely, including several badges that were still active and unaccounted for. At another agency, we found 3 of 16 accounts for former employees had not been disabled. Additionally, two deactivated accounts had not been disabled timely, with one account having remained active for 245 days after that employee left the agency.

Too much trust in staff, poor processes, and insufficient communication contributed to problems in this area. Staff did not always have policies and procedures to mitigate potential

security risks from onboarding or offboarding staff. In general, agency staff did not think to put controls in place because they doubted that new or former employees could cause security problems. In several agencies, IT and human resources divisions did not adequately communicate what needed to be done and who was responsible. One agency had additional mitigating processes (identifying inactive accounts) which reduced but did not eliminate the risk.

Improper personnel protocols increase the risk that employees might steal or otherwise compromise sensitive data. As discussed above, in certain situations background checks are required through law or federal policies. In the event of a security incident, failure to conduct those checks could increase associated penalties and fines. Not recovering a computer from a former employee can have more implications than the cost of the physical machine. Any data on the computer could be sensitive or confidential, and has the potential of being used against the agency or its employees. Lastly, not disabling access promptly exposes the agency to unnecessary risk which increases significantly if the person did not leave the agency voluntarily.

SECURITY AWARENESS TRAINING

Many Agencies Did Not Conduct Security Awareness Training, And Our Social Engineering Tests Demonstrated a Lack of Understanding for Security Protocols

Governmental agencies are a valuable target. The first line of defense against many attacks is to educate employees about why security controls are necessary and where the risks come from. ITEC standards require new users to receive security awareness training within their first 90 days, and for all users to receive annual refresher training. The training should cover a variety of topics, including password creation and confidentiality, physical security, internet usage, portable devices, and social engineering.

About half of the agencies did not provide systematic security awareness training, resulting in significant risks. Generally, agencies did not understand the need or importance for initial or annual training for all users. Some agencies did not have a process to ensure training reached all the staff. Often we noted IT staff lacked policies in this area or did not communicate with the agency's human resources department to ensure this security control was being met. Several IT staff stated they did not have a program or automatic tracking mechanisms to monitor compliance and had not thought of other, more low-tech options. For example, staff could take attendance at training sessions and follow up on staff who missed the training session.

Our social engineering efforts demonstrated staff at some agencies lacked an understanding of security awareness

protocols. ***Figure 1-5*** below provides more information about what social engineering is and what we did in this area.

Figure 1-5
Social Engineering Uses Peoples' Trusting Nature to Circumvent Internal Controls

Social engineering attacks attempt to gain sensitive information through personal interactions and psychological manipulation. We started offering social engineering tests in 2015 as an optional service. Seven agencies volunteered to undergo these tests, which included the following.

- **Clean Desk Checks:** We inspected employee work areas and looked for login information (written username or passwords) that was kept in plain sight (e.g. sticky note on monitor) or obvious locations (e.g. under the keyboard).
- **Computer Media Checks:** We inspected employee work areas and looked for computers that were not properly secured or were left on outside regular office hours and determined whether screen locks prevented further access.
- **Door Checks:** We attempted to access restricted areas by following authorized staff without showing our credentials, and tested whether doors to restricted areas were physically locked.
- **Pretext Phone Calls:** We phoned agency employees and attempted to solicit information which could be used to help gain access to the agency's network or threaten the agency's security posture (e.g. user's login and password information).
- **Simulated "Phishing" Emails:** We used publicly available information to craft and send e-mails to agency employees, and used various scenarios to entice users to click on links we embedded in the emails.
- **Trash Checks:** We checked employee work areas and other areas designated for agency trash disposal to determine whether staff had discarded sensitive information in unsecure trash bins or containers, which would then be accessible to others (e.g. other employees, maintenance workers, contractors) not authorized to view that information.

We did not conduct every test at every agency that volunteered. The testing depended on the size of the agency, the physical configuration, and the time we had available to conduct the tests and analyze the results.

As the figure shows, we tried to simulate tactics hackers use to gain access to an agency's network.

- **At one agency, we successfully obtained confidential or sensitive data through door checks, trash checks, and phone calls.** We entered several work areas without being questioned, some of which contained confidential paper records that were not properly secured and were accessible to all agency and maintenance staff. We also found improperly discarded paper documents with sensitive and confidential information including client names and investigative information. At the same agency, two of five employees we judgmentally selected provided password information over the phone.
- **At a second agency, we successfully convinced employees to click on simulated phishing emails; we also found weaknesses in its media destruction process.** In all, 6 of 46 employees clicked on the hyperlink embedded in our simulated phishing emails. Four employees clicked several times, suggesting their actions were not

accidental. The agency also used a paper shredding service. However, rather than using locked bins, the agency allowed staff to collect sensitive documents in unlocked boxes and sacks until the monthly shredding. This could allow unauthorized staff to see sensitive information.

- **At a third agency, we successfully convinced employees to click on simulated phishing emails and saw a username and password displayed in plain sight.** In all, 2 of 50 employees clicked on the hyperlinks embedded in our simulated phishing emails. Additionally, during one of the 13 desk checks we conducted, we saw sticky notes in plain sight with an account's user name and password. Lastly, we retrieved paper documents containing sensitive information (including a social security number) from one locked, but overflowing trash bin.

Each of these agencies did not provide adequate initial or periodic security awareness training, which contributed to the agency's poor security protocols.

Security awareness training is important because people are the weakest link in an agency's security posture. Technology can be used to implement many IT controls. However, untrained employees can diminish the effectiveness of those controls. In turn, this can result in data being mishandled, inappropriately used, or shared with unauthorized people. Things that may seem clear to one employee may not be obvious to the next. For example, all employees should be aware of the dangers of plugging in a flash drive, downloading or sharing copyrighted information, or protecting their computers when working in public areas. Lastly, hackers know people are a great target to bypass technical controls and often use social engineering schemes to prey on their natural inclination to be helpful.

Conclusion

Our IT security audit work over the past three years revealed significant weaknesses in several important security controls across the 20 agencies we audited. Several agencies had previously been audited, and often we noted repeat findings, indicating little progress had been made on those agencies' security postures.

Because Kansas has taken a decentralized, agency-by-agency approach to IT security, the responsibility for adopting ITEC-required and other IT security controls falls to each individual agency. Agencies that failed our audits tended to lack the proper top management attention and support to develop robust security programs. Several agencies did not have a mature IT security function, and a few did not have this function developed at all. In agencies with an IT security presence, the function tended to be inadequately resourced or plagued by turnover. At times, IT security may not be viewed favorably because security measures or requirements slow application and staff productivity or use resources that are needed by IT to support the business units.

In addition, the typical IT security function in most agencies is a sub-function of the IT department. This can create a significant problem if top management does not hear about important security risks because addressing those risks may be in conflict with the IT department's mission to support the business units.

Finally, addressing security risks requires agencies to make financial investments in the IT security function. Convincing top management to make these investments can be a challenging because the benefits are not immediately visible. Such investments are even more difficult to sell to leadership when agency budgets are tight.

Recommendations for Executive Action

We made recommendations to each agency to address the specific security risks found during their audits.

APPENDIX A

Examples of ITEC Requirements or Best Practices Across 12 Security Areas

This appendix provides an overview of the types of processes we evaluated as part of each agency audit. The processes are organized within 12 security areas, which in turn are part of four layers of IT security controls

APPENDIX A Examples of ITEC Requirements or Best Practices Across 12 Security Areas	
Security Area	**Security Control Examples**
SECURITY POLICIES AND PROCEDURES LAYER	
Risk Assessment and Security Planning	• Establish a data classification system and assign appropriate controls to each class • Appoint trustees for sensitive datasets • Perform risk assessments on data sets with restricted-use information
Security Awareness Training	• Create an awareness training program that includes comprehensive topics outlined by ITEC • Conduct security awareness training for all information system account holders • Train new employees within 90 days and all employees annually
Continuity of Operations Planning	• Create a Business Contingency Plan for IT and communication resources • Review, update, and test the plan
Incident Response	• Adopt an incident response plan that addresses preparation, detection, analysis, containment, communication, recovery, and post-incident activity • Test the plan annually (e.g. table top) and every five years (full-scale execution)
PHYSICAL CONTROLS LAYER	
Physical Security	• Restrict physical access to data centers to authorized personnel • Maintain a list of authorized personnel and review and update it annually or more frequently as necessary • Use authentication methods for entry to data centers • Implement physical environmental controls that prevent or mitigate damage from water, fire, temperature, and humidity in data centers
Data Protection	• Encrypt sensitive or confidential data when transmitting outside of a security boundary • Use proper media disposal processes for sensitive or confidential electronic or paper media
SYSTEM CONTROLS LAYER	
Systems Configuration	• Maintain an asset inventory • Implement boundary protection (firewall) with capability to monitor and control network communications • Create security zones within the boundary to segregate different classes of data • Employ malicious code protection mechanisms (e.g. anti-virus software) and scan computers for malware weekly
Systems Operations	• Perform vulnerability scans against information systems that process, store or transmit restricted-use information at least biannually • Implement a documented patch management process that includes monitoring for security alerts, testing, and installing of applicable patches • Ensure that critical data is restorable to a known secure state of operations
Emerging Issues	• Do not use unsupported operating systems and software or create compensating controls to mitigate risks • Scan public access website applications to ensure they are free of vulnerabilities • Evaluation of several best practices related to mobile device, social media, and cloud providers which cuts across other security layers.
APPLICATION CONTROLS LAYER	
Access Control	• Create unique system identifiers for each user • Passwords must be sufficiently long or be sufficiently complex • Password lifespans should not exceed 90 days • Users should bet locked out for 30 minutes after 5 consecutive failed log-in attempts
System Audit	• Log user access interactions and system administrator actions to include date, time, source, and description • Ensure log space is sufficient or set logging to overwrite oldest data first.
Personnel Security	• Screen or background check staff or third party users with high level risk access • Revoke system access and eliminate permissions for employees and contractors that are terminated • Recover all property that has been assigned to terminated personnel
Source: ITEC Policy 7230A, Policy 5310, and LPA	

APPENDIX B

Glossary of Information Technology Terminology

Understanding IT terminology can feel like translating a whole other language. We have compiled a glossary of technical terms that are used throughout the report along with their definitions to assist the reader when trying to understand information security terminology.

- Malware – This is a shortened form of "malicious software." It is code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or networks. Viruses, worms, and Trojans are all part of a class of software called malware.

- Virus – This is a type of malware that spreads by inserting a copy of itself into and becoming part of another program. It spreads from one computer to another, leaving infections as it travels.

- Worm – This is a type of malware that makes copies of itself and causes damage similar to a virus. Unlike viruses, worms are standalone software and do not require a host program or human help to spread. Instead, worms either exploit a vulnerability on the target system or use social engineering to trick users into making them run. The worm then takes advantage of file-transport or information-transport features on the system, which allow it to move between systems unaided.

- Trojan – This is a type of malware named after the wooden horse the Greeks used to infiltrate Troy, and operates in a similar fashion. It is a piece of software that looks legitimate but is actually harmful. Typically, users are tricked into loading and running it on their systems. Once activated, it can do anything from irritating the user with pop-up windows to stealing or deleting user files. Unlike viruses and worms, Trojans can only spread through user interaction, such as opening an e-mail attachment or running a file downloaded from the internet.

- Secure Sockets Layer (SSL) – This is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and the browser remains private and intact.

- OpenSSL – This is an open-source (free) version of the SSL and TLS protocols.

- Transport Layer Security (TLS) – This is a protocol that ensures privacy between communicating applications and their users on the internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to SSL.

- Heartbleed – The OpenSSL vulnerability, dubbed "Heartbleed," allows attackers to read the memory of systems using vulnerable versions of the OpenSSL open source library. This allows the attacker to access sensitive information such as login credentials and other personal data.

- POODLE - This is a security vulnerability where a particular version of SSL (SSL v3.0) can be attacked, and the encrypted data between the computers and servers can be potentially intercepted and decrypted.

- DROWN – This is a security vulnerability in SSL and TLS cryptographic protocols, that could allow attackers to decrypt supposedly secure HTTPS connections between internet servers and end users. The attack forces web servers to use an older, insecure version of SSL/TLS known as SSLv2. Although no longer used, SSLv2 is still supported by many web servers. Every time a connection is made using SSLv2, a small amount of data about the server's encryption key is leaked. If enough connections are made to the server, an attacker can piece together the encryption key and decrypt all HTTPS traffic.

- Browser Exploit Against SSL/TLS (BEAST) – This is a tool that exploits a flaw in SSL and TLS 1.0. The attack injects plain text into an encrypted stream, which results in the attacker to eventually decrypt the entire HTTPS request and cookies, and possibly take over a user's session.

- FREAK – This is a security vulnerability in SSL where the attackers intercept communications between a computer and a server and trick the servers into providing a weaker encryption key than they otherwise would. With the servers set to use a weaker key, the attacker can intercept and decrypt the next message from the client, and then basically has the full text of the all the communications between the client and the server.

- Cross-site scripting (XSS) – This is a security vulnerability found in web applications where an attacker uses known vulnerabilities in web-based applications or their servers or plug-ins to "inject" code into web pages viewed by other users. An attacker will fold malicious content or script in with legitimate content from the compromised website. The user's web browser will think all of the content delivered by the website is trusted and will run the malicious script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.