Information Security Strategic Plan

State of Kansas
Enterprise Security Office
Information Security Strategic Plan
Chief Information Security Officer

Background

- Purpose for the development of the IT Security Strategic plan was to provide a roadmap to reduce risk and exposure to the State.
- The findings revealed in LPA Audit Report R-14-007 2014 concerning the lack of funding, lack of adequate personnel, and lack of data classification management.
- Increasing attacks against the State IT Infrastructure.
- CISO findings compared against SAN 20
- LPA Committee request for a plan on how to fix the issues and what the cost would be to do so.

Audits

- Repeated findings spanning more than five years
  - Audit findings that are repeated year after year indicate a fundamental lack of accountability with regard to State information resources.
  - Lack of qualified security personnel, reporting, and organizational structure has greatly contributed to the overall increase in Risk to state information resources
  - The decentralized approach to both IT and IT Security have made implementing enterprise class solutions to provide consistency and common standards across the enterprise extremely difficult and thereby increasing our exposure to an ever-growing number of cyber threats
  - Standardization and centralized security controls allow organizations to establish and maintain excepted security standards, which reduce overall exposure and decrease risk to the enterprise.

Audit Strategy

- What changed?
  - In December of 2013, the CISOs office sat down with LPA Auditors and asked the question "we have done the same audit year after year, with the same results, do we want to continue doing it? Or should we be asking different questions that might help determine the root cause and truly improve the situation?

  - I'm a member of a national committee that conducts evaluations on all 50 states, our findings are made available to the States and to the US Congress. What we found in 2012 was that States neither had adequate security staff nor adequate security funding, and there was and still is a lack of awareness of what sensitive data is and how to classify it to in order protect it appropriately.

Audit Kansas Trending

- Another question asked was whether or not Kansas is trending with the Nation; after the conclusion of latest round of LPA security audits it was determined that Kansas was trending with at least some States, but unfortunately this trend is not in the right direction. According to some Kansas is on a direct parallel path with South Carolina prior to their 100 million dollar plus breach.
- That trend towards a major breach is real; it might be said it is not a question of if, it is truly a question of when, if not already. The risk continues to increase; the inability in a decentralized security setting to protect our information resources is unreasonable and unmanageable.
- While certain functions of IT can be managed in a decentralized fashion, security (for the most part) cannot because of the nature of what it does. In an environment where establishing and adhering to standards, accountability and reducing risk is subject to an ever growing gap in resources, centralization and consolidation of security and security personnel is paramount.

Strategic Plan

- The plan presented answers two questions; how and how much? Some no longer with the State interpreted Rep Burroughs request during an LPAC hearing in July 2014, as a plan to fix the findings of the last audit. My understanding of Rep Burroughs request was that the LPAC wanted a solution to decade old problem.
- The Kansas population was 2,893,957 in 2013, the cost per Kansas resident to fund the Information Security Office is about $8.50 per person to protect their data for year one. One breach could cost the state in just identity protection alone about $28,939,570.00 per year for several years.
- Over the last three years, I have consulted with industry, government and other security experts, reached out to both KU and KSU CISOs and began to develop an IT Security Strategic plan.
- Normally, this plan would dovetail with a IT Strategic Plan, however, there hasn't been one in several years. While the IT Strategic Plan is in the development stage, the Security Strategic Plan represents the best that it can be at this time.

Strategic Plan continued

- KSU & KU CISO's and I began to look at audit findings, and what we have done in the past to fix similar problems. Combined, myself, the KSU and KU CISOs have over 50 years of experience with IT and IT Security. This plan addresses the action needed to correct not only the audit findings, but to provide a roadmap and strategy for success of the State of Kansas IT Security program over the next 5 years.
- Citizens, residents and businesses of Kansas look to the State to protect the information they have provided to the State, it is our responsibility to ensure that we maintain the Public Trust. One of guiding principals in the development of the plan was to make sure we provided for Public trust. Information Security for government is the enabler of technology and business.

Strategic Plan Fix

- The plan calls for the consolidation of security technology and security personnel. It calls for the complete funding of security, so that agencies no longer need to make the hard choice to sacrifice security as the result of reduced agency funding. Likewise the consolidation of security technology and personnel removes the burden of determining what adequate security resources they may need.
- The plan calls for the development of the KISO, (Kansas Information Security Office) which is stand-alone from OITS. The new KISO would report to State Security Council (regularly) and to Legislative, Judicial and ITEC CITO's, as required or requested. This would be both through formal and informal methods.

The Fix and Cost

- People are a number one concern. It does no good to have technology deployed if you don't have the bodies to respond and fix the situations. No amount of software or hardware can reduce the risk to an acceptable level for the State. Only trained, qualified security professional have the necessary skill sets to do so.
- Consolidation of personnel that report directly to the CISO, and the CISOs office reports risk directly to the Secretaries, or the appropriate senior executive. Security personnel must report independently of the CIO and IT Infrastructure as noted in LPA audit findings.

Kansas Information Security Office (KISO) Formation

- KISO to provide all security personnel, enterprise technology solutions to State government.
- KISO will support, develop and manage identity access management for all systems.
- KISO will maintain and manage through a Managed Security Service, all firewalls, intrusion detection systems and other security controls as meet agency requirements.
- KISO will provide to agencies, boards, and commissions a “trained” security professional to perform the functions of Information Security Officer.

KISO Secure Kansas

- KISO will provide as needed, or required, limited support for municipalities and counties of the State.
- KISO will provide assistance and support to educational institutions in the State to protect the information of Kansas students grades K-12.
- KISO will continue to develop a comprehensive relationship between the Regents and the State.
  - In 2013 as the Chair of the Security Council, I directed the development of a sub-committee to rewrite the State Security Policy to not only better serve the State, but to also serve the regents. With the assistance of the CISO from KSU, KU and others, the security council delivered to the State a revised Security Plan that both the Regents and the State have agreed to use. This marks the first time that both regents and State will operate off the same Security Policy.
  - It will be the goal of the KISO to continue to develop various security programs and embrace the goal of mutual support and mutual growth of both the Regents and State security programs.

Dec 11, 2014 Financial Services Sector

- On December 9, Hackers breached payment solutions provider CHARGE Anywhere: Undetected since 2009. Electronic payment solutions provider CHARGE Anywhere stated December 9 that attackers had gained access to its network as early as November 2009 using a previously unknown and undetected piece of malware and were able to capture payment card data from some communications that did not have encryption. The company discovered the compromise September 22 and an investigation found that network traffic capture occurred between August 17 and September 24.
- What is important to note is that the attackers where in the network undetected for over 5 years. "The investigation revealed that an unauthorized person initially gained access to the network and installed sophisticated malware that was then used to create the ability to capture segments of outbound network traffic," the company said. "Much of the outbound traffic was encrypted. However, the format and method of connection for certain outbound messages enabled the unauthorized person to capture and ultimately then gain access to plain text payment card transaction authorization requests." This type of attack would seem to indicate lack of adequate trained person, lack of monitoring, lack of personnel to respond to the situation. Very similar to our situation here in the State today.

Dec 11, 2014 DHS Open Source Report

- On any given day we look at these threats as well as hundreds of others that are similar in nature. And since there is no centralized security, no way to enforce security standards at the end of the day we realize how lucky we were not to have been hit. And we go on to do it again the following day, 7 days a week. But for how long before we are just one of the victims or a causality of the Cyber-Wars

  - December 10, Red October cyber spy op goes mobile via spear-phishing. Researchers with Blue Coat and Kaspersky Lab identified and analyzed a cyber-espionage campaign that appears similar to the RedOctober campaign dubbed Cloud Atlas or Inception Framework that has been targeting the Android, iOS, and BlackBerry devices of specific users in the government, finance, energy, military, and engineering sectors in several countries via spearphishing. The malware appears to primarily be designed to record phone conversations and can also track locations, monitor text messages, and read contact lists.
  - December 10, Trihedral fixes vulnerability in SCADA monitoring and control software. Trihedral Engineering Ltd., released software updates for its VTScada (VTS) supervisory control and data acquisition (SCADA) software to close a vulnerability that could be used by an unauthenticated attacker to crash VTS servers. The software is used in industries including the energy, chemical, manufacturing, agriculture, transportation, and communications sectors.
  - December 10, Flash Player 16.0.0.235 fixes remote code execution bug exploited in the wild. Adobe released patches for six vulnerabilities in its Flash Player software, including a vulnerability reported by a researcher that could allow arbitrary code to be executed on affected systems. The arbitrary code execution vulnerability has been observed being exploited in the wild and all users were advised to update their versions of Flash Player as soon as possible.
  - December 10, SQL injection, other vulnerabilities found in InfiniteWP admin panel. A researcher with Slik identified and reported several vulnerabilities in the InfiniteWP administration application for WordPress Web sites, including SQL injection vulnerabilities that could be used by an unauthenticated attacker to gain control of WordPress sites.
  - December 10, Flaw in AirWatch by VMware leaks info in multi-tenant environments. VMware released an update for its AirWatch enterprise mobile management and security platform December 10 that closes vulnerabilities that could allow a user that manages a deployment in a multi-tenant environment to view the statistics and organizational information of another tenant.

Dec 11, 2014 DHS Open Source Report

- December 10, Flash Player 16.0.0.235 fixes remote code execution bug exploited in the wild. Adobe released patches for six vulnerabilities in its Flash Player software, including a vulnerability reported by a researcher that could allow arbitrary code to be executed on affected systems. The arbitrary code execution vulnerability has been observed being exploited in the wild and all users were advised to update their versions of Flash Player as soon as possible.
- December 10, SQL injection, other vulnerabilities found in InfiniteWP admin panel. A researcher with Slik identified and reported several vulnerabilities in the InfiniteWP administration application for WordPress Web sites, including SQL injection vulnerabilities that could be used by an unauthenticated attacker to gain control of WordPress sites.
- December 10, Flaw in AirWatch by VMware leaks info in multi-tenant environments. VMware released an update for its AirWatch enterprise mobile management and security platform December 10 that closes vulnerabilities that could allow a user that manages a deployment in a multi-tenant environment to view the statistics and organizational information of another tenant.
- December 10, Recursive DNS resolvers affected by serious vulnerability. The Computer Emergency Response Team Coordination Center (CERT/CC) reported December 9 that recursive Domain Name System (DNS) resolvers are vulnerable to an issue where a malicious authoritative server can cause them to follow an infinite chain of referrals, leading to a denial of service (DoS) state.

Dec 11, 2014 DHS Open Source Report

- December 10, Third-party bundling made IBM products most vulnerable: Study. Secunia released a report on security vulnerabilities disclosed between August and October and found that vulnerabilities increased by 40 percent compared to the previous year to a total of 1,841 vulnerabilities in the 20 most vulnerable products, among other findings. The report also found that Google Chrome had the largest number of disclosed security issues, and that IBM was the most vulnerable vendor due to products being bundled with third-party software.
- December 9, Microsoft releases critical IE security update on Patch Tuesday. Microsoft released its monthly Patch Tuesday round of updates for its products December 9, which included 7 security bulletins addressing 24 vulnerabilities. Three vulnerabilities were considered critical and affected Internet Explorer, Microsoft Word and Office Web Apps, and the VBScript scripting engine.
- December 9, New version of Destover malware signed by stolen Sony certificate. Researchers at Kaspersky Lab identified a new variant of the Destover malware used in an attack on Sony Pictures Entertainment that uses a stolen, legitimate certificate from Sony. The malware is basically identical to previous versions except for the use of a certificate.
- December 9, SEO poisoning campaign ensnares several thousand websites, security expert finds. A webmaster identified and researchers from Websense and High-Tech Bridge confirmed that several thousand legitimate Web sites hosted on GoDaddy and other services had been compromised to improve the search engine optimization (SEO) ranking of other sites by inserting links into the legitimate sites. GoDaddy stated that the company was investigating the issue.

Finalizing

- No amount of funding, personnel or technology can assure that no incident can occur.
- What can be guaranteed is that disclosures, incidents and breaches will occur, so the real question is how well we are able to respond to these events? Based on the State's lack of attention to this issue, the current lack of security resources and the decentralized approach to IT and IT security, these events will most certainly result in Major breaches and headline news.

Ending

- We would like to provide to all members of the legislative branch information on a couple of services that we provide that all state, county and municipalities can take advantage of.
- I would personally like to thank you for your time and allowing me to present an overview of our Security Strategic Plan.
- Questions?