SPECTRIM

Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management

Category: Cybersecurity

State of Texas

Edward Block, Chief Information Security Officer

Texas Department of Information Resources

300 W. 15th Street, Suite 1300

Austin, TX 78701

Initiation Date: July 1, 2014

Completion Date: December 31, 2015

Executive Summary

On February 13, 2015 President Obama signed an executive order establishing that organizations “must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible”. Fortunately, Texas Department of Information Resources (DIR) Office of the Chief Information Security Officer (OCISO) had already started building a governance, risk and compliance solution aimed at exactly that.

With 140 plus state agencies and institutions of higher education (IHE) and over 325,000 employees across the state of Texas, determining overall state security risks and keeping everyone informed are difficult tasks. The goal was to provide a service so agencies and IHEs could better manage their security programs, while enabling the OCISO to address key risks at a statewide level.

Although state organizations are all united by being part of the Texas government, they are run independently. Agencies and IHEs have their own information technology management, data centers and information security offices. Collaboration on a statewide basis has been typically done via email lists, with little resulting feedback. Through SPECTRIM, the Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management, OCSIO customers have a single hub where they have visibility into threats, attacks, risks and responses. Not only does this benefit a particular organization, but it helps the OCISO determine commonalities of statewide threats and incidents, and risks can be easily identified across the state.

SPECTRIM provides other key tools to better manage cybersecurity risk and incidents. Risk assessments are based on NIST 800-53 controls. In a matter of seconds, an information security office is able to see where their agency has or has not implemented specific NIST controls. The agencies and IHEs are also required to report their maturity according to the Texas Cybersecurity Framework using SPECTRIM. It enables them to create a plan for improving their maturity. The OCISO uses this information to report to the Texas legislature on information security risks, and where state law makers should focus their attention.

Overall, the key benefits of the SPECTRIM portal include a central source of data for analytics when it comes to safeguarding citizen information. Additionally, DIR licensed SPECTRIM for all state agencies and IHEs so they all have access to the same tools, regardless of their size or budget.

Concept

SPECTRIM enabled the replacement of three tools and combine everything into a single platform which creates synergies for the OCISO. DIR replaced an outdated security incident reporting system, a retired system for performing risk assessments, and a very large and complex spreadsheet for submitting the maturity of key security controls according to the Texas Information Cybersecurity Framework.

Optimizing incident response: State agencies and IHEs are required to submit monthly incident reports to OCISO. The system they were using was outdated and cumbersome, and the information collected was not keeping up with the changes in technology. If an organization wanted more insight on past incidents, it was nearly impossible unless they had an internal process. Urgent incidents that were required to be reported to the OCISO were not always submitted in a timely manner and when reported, there was no acknowledgement that the OCISO staff received them. The organizations had no real incentive to focus on reporting meaningful data because the process and tool was a burden. The OSCIO staff had a difficult time compiling meaningful data and metrics due to the lack of standard information being collected. Not only were they not gaining the expected benefits, it was also costing them valuable time.

Improving risk assessments: The software that state agencies and IHEs were using for risk assessments was being discontinued. OCISO wanted a Governance, Risk, and Compliance (GRC) solution that could help organizations perform their information security risk assessments, while enabling the OCISO to see risks at a statewide basis. The goal was to build in workflow for approval processes and reduce duplication of effort, creating efficiencies.

Enhancing the Texas Cybersecurity Framework for security planning and maturity level reporting: In 2013 the Texas legislature passed a bill requiring state agencies and IHEs to submit a security plan to DIR every two years. Another bill passed requiring DIR to develop a cybersecurity framework. To meet these requirements, the OCISO started developing the Texas Cybersecurity Framework at the same time that NIST was developing the national Cybersecurity Framework. Unfortunately the legislated time line would not allow the OCISO to simply adopt the NIST framework. The OCISO adopted NIST’s high-level functional areas of identify, protect, detect, respond, and recover and defined 40 key control areas under the functional areas. Initially, state agencies and IHEs were required to document their maturity level for each of the 40 key control areas and plans for improvements in MS Excel spreadsheets. The department identified the need for a tool that provided organizations with the ability to continuously monitor and assess their maturity levels for each of the 40 key control areas and manage plans for improving their controls. The tool also needed to give the OCISO the ability to analyze the data from all organizations and provide a report to the legislature.

To meet the use cases for Incident Response, Risk Assessments and the Texas Cybersecurity Framework, the OCISO decided to procure a GRC tool for statewide use. Questionnaires were sent to a number of leading GRC providers and demonstrations were provided by the top contenders. Through this competitive process, RSA Archer was selected.

RSA Archer is a collection of governance, risk, and compliance functions connected through standard interface, a series of menus, which all have the same look and feel. OCISO is using the enterprise, policy, risk, compliance and incident modules of Archer as the foundation for SPECTRIM. It met the three key use cases as well as allowing organizations could see how they compared to other organizations of similar size or the state as a whole. The standard interface results in an easy to use portal, where accessing a security incident or printing a report uses the same search and reporting screens as if you are accessing a risk assessment or other data in the application. SPECTRIM cost approximately $2.2 million in software as a service and development costs during this timeframe.

Governance of the portal is provided by the Statewide Information Security Advisory Committee, which is made up of representatives of state agencies, universities, and other partners. Design of the various functions has been provided by subcommittees made up of representatives of state organizations. For example, 15 different state agencies and IHEs were involved with the creation of the risk assessment module.

The OCISO also reports to DIR's Board of Directors on a quarterly basis, providing statistics about current adoption rates. This is extremely valuable in determining what the OCISO can do to improve the tool, and ensuring that customer needs are being met.

Significance

The Texas OCISO manages large amounts of security and risk information for 140+ state agencies and higher education institutions. Incident data in particular was stored in many places, making it impossible to analyze and respond with new programs to assist organizations. In addition, OCISO systems and processes were out-of-date and cumbersome, creating inefficiencies.

Using the legacy security incident reporting system, agencies put numbers in every month and never received any information back out of it. Using SPECTRIM, organizations can report their monthly incidents but also see how they stack up against other organizations of similar size or the state as a whole. Texas Administrative Code 202 requires organizations to report any incident that meets one of three criteria: the loss of protected information, if law enforcement has to be contacted or if it can propagate to other state systems. SPECTRIM gives agencies a way to enter their incidents with automated and just-in-time notifications made to the OCISO. That way if the Texas has a major attack underway, the OCISO is notified more quickly and resources can be deployed to assist and communicate at a much more rapid rate. Additionally, SPECTRIM gives organizations the ability to track all their incidents. This benefits the organization because if they track individual incidents, then their monthly report is automatically generated for them. This enables them to spend valuable security time protecting citizen data rather than complying with DIR reporting requirements. And it allows them to view all their incidents over time, by threat actor/action and compare the same to organizations of similar size.

The incident reporting module aligns to the VERIS framework, which is used by Verizon to create their annual Data Breach Report (DBR). This enables the OCISO to compare overall state of Texas data with the data presented in the DBR, giving additional insight into the state's overall security posture.

The risk assessment process also changed. The retired system had one questionnaire which agencies would export to a spreadsheet and then parse the questions to send to the various personnel with risk information. SPECTRIM provides questionnaires based on functional areas, so that a questionnaire, for example about the security program, can be answered once online, and then automatically applied to risks on other agency systems. The retired system did not have a way to track risk acceptance, risk mitigation and the resulting residual risk score. SPECTRIM provides this, along with the ability to create risk remediation plans and timed exceptions to policies when an organization chooses to accept risk rather than remediate.

In 2014, state agencies and higher education institutions were required to submit security plans consisting of a maturity assessment of key security controls and a roadmap for improving the assessed maturity. SPECTRIM allows users to update maturity of controls on an ongoing basis and can extract real time data to make smarter business decisions as well as provide leadership valuable insight. Because the data is stored in SPECTRIM, organizations will be able to trend year over year to see how the maturity of controls has changed.

The 2016-2020 Texas State Strategic Plan for Information Resources Management lists cybersecurity as its first goal. One of the goals is *to "implement policies and standards aligned with the Texas Cybersecurity Framework, which provides cybersecurity policies, training, and standards to assist agencies in mitigating risks and improving the resiliency of state information systems against cyberattacks".* SPECTRIM enables the OCISO to see where the key risks are on a state-wide basis. The OCISO can also analyze data about risks, weaknesses and events so it can appropriately set policy and guidance, provide assistance and training, and provide useful information to state leadership on the stance of Texas information security.

Impact

SPECTRIM enables all risk assessments, security plans and security incident reports to be generated and housed in one tool. It not only provides a cohesive system with uniform reporting for all state organizations, it provides powerful analytics that can not only provide individual organizations with meaningful metrics, but also help DIR provide the legislature and governor's office more timely and reliable data on incidents and risks across the state of Texas.

SPECTRIM has provided savings in terms of personnel hours spent when performing risk assessments. For example, one agency that implemented the legacy risk assessment system reported that central IT spent 40 hours responding to and completing the same questions over and over for different risk assessments. Now that central IT group spends an hour to complete the questions once and SPECTRIM is able to apply the results to the many other applicable risk assessments. This saves central IT 39 hours to do other tasks. They had similar issues with the old DIR incident tool in the time and effort it took to get and enter information versus now with

SPECTRIM. With resources often maxed out in agency information security departments, saving time and effort in risk assessments and incidents allow for more time on other security tasks.

The law regarding implementation of the Texas Cybersecurity Framework requires a report to the legislature after all of the agencies and IHEs submit the information to the OCISO. In 2014, efforts to analyze the data for reporting to the legislature took more than 1,000 hours to normalize and link so it could be analyzed in order to create recommendations. SPECTRIM enables the same reports to be generated with one click. It enables state organizations to see risk assessment findings that are associated with each of the controls, giving them more definitive data from which to assess their maturity rather than it being a totally subjective process. Additionally, they can see their data and update their maturity levels and roadmaps continually, making this an on-going process instead of a biennial exercise.

DIR also operates a Network Security Operations Center (NSOC), where 20 terabytes of daily traffic between the internet and the state agencies is analyzed and filtered. Although not a part of the original concept, when they became aware of the SPECTRIM portal, they saw the value and in a matter of a few weeks, OCISO was able to modify the incident module for their use. The NSOC began using SPECTRIM to provide incident alerts that the agencies respond to, letting the NSOC know whether an alert is true or a false positive. This enables the NSOC to tune their filters to provide better incident alerting to all of the state agencies they serve. SPECTRIM enabled the NSOC to produce a 2015 Threat Report that shows what incidents are making it through the perimeter defenses that the NSOC provides. Of the half a billion weekly IPS blocks in 2015, 381 alerts were still detected from inside the shared network. The 381 alerts were distributed to the various state agencies and tracked through SPECTRIM. Through the data collected in SPECTRIM, the NSOC is able to determine more rapidly what tools should be added or removed from the network for providing the most effective network security. Through customer feedback using SPECTRIM, the NSOC has maintained a 92% true positive rate of incidents reported.

The impact to the OCISO's customers is significant. Agencies with 7 employees now have the same tools as agencies with 50,000. This helps to minimize the disparity between organizations, and allows smaller agencies the ability to use a tool they generally would not have the resources to procure. One large university was in the process of purchasing RSA Archer for use in their security office. Instead they opted to use SPECTRIM, resulting in over $1.5 million in cost savings. Out of 140+ agencies and IHEs, 84% are currently collaborating by including their security incident information every month. The OCISO anticipates 96% utilization by the fall of 2016.

Not only does SPECTRIM enable the core functionality that the OCISO intended, it allows DIR to use it for other functions that require communication and collaboration with other agencies. As other DIR employees learn about Archer and its ease of use and flexibility, they are asking the OCISO to provide other applications; for example, an application for agencies to report their compliance with various state laws. This was previously done using an online survey tool.

In closing, SPECTRIM has made a fundamental change in the way the OCISO manages risks for the state as a whole. The Texas Cybersecurity Framework and Agency Security Plan process put security programs across the state on a roadmap of continual and steady improvement. SPECTRIM enables the OCISO to manage the Framework's elements while relating maturity to risk, and a cyclical management plan that keeps all of the components on track for evolution. This makes DIR and the OCISO well suited to manage risk within the state at a highly competent level.