Reducing Risk Through Enterprise Data Identification

Cybersecurity

Initiation date: August 2015

Completion date: October 2015

Nomination submitted by:
Nelson P. Moe
Chief Information Officer
Commonwealth of Virginia
Virginia Information Technologies Agency

www.vita.virginia.gov

2016 Commonwealth of Virginia NASCIO Award Submission
Project: Reducing Risk through Enterprise Data Identification
Category: Cybersecurity

Executive Summary

Virginia has taken significant steps to leverage its centralized information technology (IT) infrastructure for maximum protection of cyber assets. A recent data identification project illustrates how this platform enabled executive leadership and agencies to collaborate, significantly improve risk management, and better protect citizen data.

A critical part of an effective risk management strategy is a complete understanding of the data used by an organization and how it impacts business operations. However, that information was not fully available across the enterprise of 89 executive branch agencies served by the Virginia Information Technologies Agency (VITA). Without such an understanding of the data, proper resources could not be identified and put in place to ensure data security and availability for appropriate use by citizens, business and government entities and other stakeholders.

To improve the commonwealth's cybersecurity posture relative to data, Virginia Governor Terry McAuliffe signed Executive Directive six (ED-6), "Expanding Cyber-Related Risk Management Activities" on Aug. 26, 2015. The directive required VITA and the chief information officer (CIO) of the commonwealth to provide an updated inventory of all data and computer systems by Oct. 15, 2015.

To comply, VITA's commonwealth security and risk management (CSRM) directorate developed a standardized method to identify all data sets used by executive branch agencies. A data classification and risk assessment was applied to both the data and the IT systems that contain it. Collaboration between the agencies, the governor's office and VITA provided insight into the data and how it impacts the commonwealth. Combining the information about the sets provided actionable information on how the data is used.

The scope of the initiative was vast. The number of records processed by 2,435 systems is nearly 160 billion records per year. As part of the project, approximately 1,700 data sets containing more than 191 billion records were classified. An additional 1,309 sensitive systems were identified and prioritized.

Consistent risk evaluation criteria was applied to data sets and IT systems along with a top-line view of the commonwealth's most important data and systems – and how they interact. A 37 percent increase in cybersecurity funding for agencies over the next biennium was allocated to evaluate and protect the identified data and systems. This funding is based on metrics and enables future benefits to citizens and agencies.

This project resulted in a substantially better understanding of what data is in use throughout the commonwealth, how that data impacts business and whether security measures are in place for each data set.

Description of the Business Problem

The commonwealth has taken significant steps in recent years to centralize cybersecurity and maximize the results of Virginia's strategy to protect the data to which it is entrusted. A critical part of an effective risk management strategy is a complete understanding of the data used by an organization and how it impacts business operations.

However, that information was not fully available across the enterprise of 89 executive branch agencies served. Without such an understanding of the data, proper resources could not be identified and put in place to ensure the data remains secure and available for appropriate use by citizens, business and government entities and other stakeholders.

While the commonwealth has established metrics to measure the effectiveness of the statewide information security program, the ability to focus on individual risk scenarios and the resources needed to mitigate them has proven to be difficult. In order to provide a more detailed risk analysis, information about the data usage in the commonwealth was needed. The result of this need was a data inventory effort.

The business problem can be broken down into four primary objectives:

- Efficiently apply resources needed to identify risks and implement effective security controls.
- Prioritize implementation of security controls to IT systems and data.
- Apply a common methodology to determine availability requirements for each IT system based on business needs.
- Prioritize detailed risk reviews of IT systems and data.

With a full understanding of the data sets in the commonwealth, it is possible to prioritize the availability of systems. Classifying data importance to each agency's business allows an effective method to rank and prioritize systems based on risk to availability. In the case of an outage or a cyberattack it is possible to restore systems in a way that supports business needs. Additionally it is possible to apply more granular risk evaluation of security controls needed to protect the confidentiality, integrity and availability of the data.

Concept

Gov. Terry McAuliffe signed Executive Directive Six (ED-6) on Aug. 26, 2015 as a commitment "to expanding our cyber-related risk management activities and strengthening our ability to protect the information entrusted to our care."

The directive required VITA to provide an updated inventory of all data and computer systems by Oct. 15, 2015 – or in just less than two months.

The inventory requirements included (but were not limited to):

- Determination of sensitivity and criticality of systems and data

- Risk prioritization and scope of systems and data, and
- Development of a risk-based approach to enhance protection of systems and data.

The ED also required the secretary of technology and VITA to recommend strategies to strengthen and modernize agencies' cybersecurity profiles by Oct. 15, 2015, including:

- Completion of security audits,
- Development of risk mitigation and resilience plans, and
- Plans for remediation with completion dates.

To satisfy this request, VITA's chosen strategy was to apply a data classification and risk assessment to both the data and the IT systems that contain it, concentrated on three primary areas:

- Identification of commonwealth data sets
- Assessment of security controls impacting the data sets
- Evaluating the importance of each data set to its stakeholder

VITA CSRM staff used RSA Archer governance, risk and compliance tool to perform an assessment of each agency. The assessment contained a series of "yes or no" questions based on the commonwealth's implementation of the NIST cybersecurity framework. Each agency answered questions that first classified the data into the basic category of sensitive or not sensitive and then further labeled the data as a specific type of sensitive data (e.g. personally identifiable information, personal health information, payment card industry data, etc.).

The RSA Archer solution was chosen due to its capability for ease of changes and its ability to quickly collect information. Additionally the tool already contained some risk information about the commonwealth enterprise IT environment. Associating the data set information with the IT system inventory and the business process information allowed a direct connection between the IT operating environment and the business needs of each agency. Understanding the business needs provided a way to accurately evaluate the importance of each IT system and data set to each agency business owner.

Depending on the type of data in the data set, the assessment automatically adapted to determine the security protections in place. Additionally, each agency was required to associate each data set with a corresponding business process and IT system to provide an understanding of how the data set is used. This association allowed a consistent evaluation of how the data impacts business and what would happen if the data was compromised, unavailable, or altered.

The project scope included:

- Inventory of data managed throughout the commonwealth's agencies, including personally identifiable, credit card, health information and other sensitive data.
- The association of data sets with commonwealth business processes, to better explain how the data is used.

- Identification of external and internal parties relying on the data, to understand who is using the data.
- Matching data sets with IT systems, providing insight into which applications are conduits to each data set.

A combination of CSRM staff, contractors, and agency personnel worked diligently together to gather the inventory in 50 days. The effort required brining on some staff augmentation in order to assist agencies with gathering accurate data and analyzing the results. Most of the approximately $130,000 expended on the effort was included with the staff augmentation resources. The rest of the effort utilized five of the staff in CSRM and representatives from agencies. The initiative was successful in identifying data across all agencies.

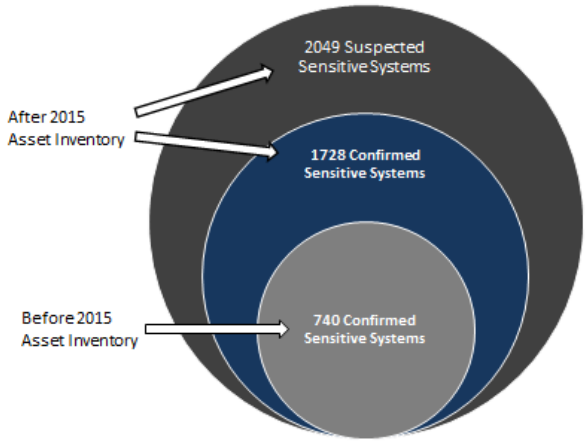
With the short time frame this effort occurred within it was imperative that communications to participating personnel were effective and efficient. Agencies were given instructions on how to capture information about data sets as well as provided an analyst to assist them in their data collection. Agencies had the option to put the information directly into the RSA Archer tool or they could collect it using templates provided by CSRM. The templates were then imported directly into the tool for analysis. The RSA Archer application was an enormous help with this effort as the user interface was very simplistic.

The results were analyzed for impact to data confidentiality, integrity or availability. Existing risk assessments, business impact analysis and audit reports were also reviewed to identify the need for a detailed risk review and existing security controls. All systems then were risk-ranked so that the highest risk systems could be targeted first for review and remediation. Once the ranking was completed the resources necessary to remediate the highest risk systems were categorized and a corresponding cost of necessary resources was prepared.

Significance of the Project

The project encompassed collaboration of multiple stakeholders including agencies, the governor's office and VITA. Each stakeholder provided details about their data sets including how they impact the commonwealth. Engaging the significant number of stakeholders and gathering insight into the operation of their business processes enabled an innovative approach to evaluating risk to the business and ways to improve the commonwealth security posture.

Citizens are also representative stakeholders, as the focus of the commonwealth cybersecurity program is to ensure that citizen and commonwealth data remain secure and available. This project supports that focus by identifying risk and applying efficient use of resources to improve the cyber security program. The outcome has the benefit of not only reducing risk but also being an effective and efficient use of resources.



The scope of the data to be inventoried grew significantly during the discovery phase of the project. Prior to the inventory, CSRM was aware of 740 confirmed sensitive systems among executive branch agencies. After the inventory, 2,049 sensitive systems were identified. 1,728 systems have already been confirmed as sensitive, the remaining 321 are under additional review to confirm their level of sensitivity. The resulting inventory proved to be a much more accurate understanding of systems and how they interact with commonwealth data.

Once the full inventory of data sets was identified, the next step included determining if any additional resources were needed to perform a detailed risk review of the data and the IT systems accessing the data. The project helped to substantially clarify funding needs for enhanced cybersecurity across the enterprise of executive branch agencies. Based on the results of the data set assessment and the number of confirmed sensitive systems and potential sensitive systems, VITA CSRM staff members first identified gaps in the risk evaluation of the data and IT systems, and then recommended the most effective approach for investing cybersecurity resources. Thanks to this project, it became possible to create a list of systems to be remediated and prioritized by importance of the data in the system.

An example of the project outcome includes additional information about systems that support either business processes or applications that have an impact to life or safety functions. These systems now have been more clearly prioritized above systems that may have only administrative impact. Controls could range from legacy upgrades to optimized security monitoring to innovative ways to encrypt data – all possible with clear understanding.

Overall this project was a model use of providing actionable qualitative and quantitative data to government executive leadership in order to make risk based and financial decisions. The extensive participation of executive branch agencies and the data provided allowed the governor and his cabinet to decide how best to allocate resources to address the risks that were discovered during the data inventory process. Resources were allocated according to priorities set by the governor and are reflected by other states and government related entities such as NASCIO.

NASCIO State CIO priorities addressed include:

- Security risk management - This effort focused on the opportunity to assess resource requirements and reinforce data protection.

- Legacy modernization - Cybersecurity enhancements included an inventory of systems throughout agencies to promote accountability and in some cases, even result in replacement of antiquated services.

The project addresses an important priority of the governor:

- Cybersecurity and upgraded technology - Enhance current technology platforms and infrastructure while protecting all data

Benefits and Impact of the Project

The project has numerous benefits for Virginia's citizens and executive branch agencies. The initiative resulted in a 177 percent increase of sensitive systems identified. This information helps the commonwealth understand where to focus efforts, either reducing the number of sensitive systems via centralization or providing resources to effectively evaluate those systems for risk. The resources necessary to identify the additional data sets was minimal compared to the cost of a compromise of the IT systems containing the newly identified systems.

Quantitative benefits include:

- Approximately 1,700 data sets containing more than 191 billion records were reviewed and evaluated.
- An additional 1,309 sensitive systems were identified and prioritized.
- The number of records processed by 2,435 systems was found to be around 160 billion records per year.
- A 37 percent increase in cybersecurity funding was allocated to evaluate and protect the identified data and systems.

Qualitative benefits include:

- A complete understanding of the commonwealth's most important data and systems along with any significant issues impacting the data and systems.
- Comprehensive inventory of data and systems with a standardized method of evaluation.
- Consistent risk evaluation criteria applied to data sets and IT systems.
- Enhanced understanding about oversight of the commonwealth's data.

Finally, consistent risk evaluation criteria was applied to data sets and IT systems, along with a top-line view of the commonwealth's most important data and systems – and how they interact. A 37 percent increase in cybersecurity funding for agencies over the next biennium was allocated to evaluate and protect the identified data and systems. This funding is based on metrics and enables future benefits to citizens and agencies.

This project resulted in a substantially better understanding of what data is in use throughout the commonwealth, how that data impacts business and whether security measures are in place for each data set. Going forward the data inventory will be maintained as part of the overall information security program with required updates and annual evaluation.