Virginia Information Technologies Agency

VITA

NASCIO

Representing Chief Information Officers of the States

Strategic Planning with Security as a Priority

CATEGORY: Enterprise IT Management Initiatives

Initiation Date: August 2014
Completion Date: December 2014

Nomination submitted by:
Eric R. Link
Interim Chief Information Officer
Commonwealth of Virginia
Virginia Information Technologies Agency

June 1, 2015

www.vita.virginia.gov

Executive Summary

The Virginia Information Technologies Agency (VITA) IT strategic plan is designed to guide agencies with a set of strategic directions for consideration when planning technology investments. In August 2014, the agency incorporated information security into the plan.

Prior to this initiative, various agencies within the Commonwealth of Virginia (COV) did not invest in information security programs because of insufficient resources. Although security requirements were in place, agencies were not allocating adequate resources to security programs. Agencies were not properly planning to replace end-of-life IT products, which posed an increased risk to data entrusted to the commonwealth.

Today, the commonwealth has a comprehensive view of the state's IT environment to support sufficient security programs and maintain supported systems for agencies. This resulted from the incorporation of the VITA Commonwealth Security and Risk Management (CSRM) program in VITA's IT strategic planning process. The addition of cybersecurity in the agency's strategic plan, as a result the agency's budget, helps VITA fulfill its responsibility of project oversight and ensure the appropriate resources are allocated to the areas with the most significant risk.

Since its inception, the VITA CSRM program has identified 60 agencies with operational risks and issues (ORIs). At those agencies, 193 ORIs have been identified; 81 percent now have business requirements in the strategic plan to address the findings.

Best practices include:

- Ensuring legacy systems are decommissioned or modernized
- Identifying areas of risk that need investment to mitigate
- Ensuring that IT resources are invested in the appropriate areas
- The identification of operation and maintenance costs for enterprise investments

This will serve as a model for other state agencies because it provides a methodology for addressing IT risk as part of the IT enterprise investment strategies and ties investment to decision making regarding new projects. It also ensures there are total realized costs for operations and maintenance of the cross-functional security services. As more IT services are implemented within an agency, more overhead is expected for the management of systems.

The cybersecurity costs of the maintenance and operations often are overlooked. This process guarantees that the costs for cybersecurity are realized and a proper investment is made. This will help prevent security incidents and issues that are more expensive than the investment to reduce or mitigate the risks of the environment up front.

Description of the Business Problem

The Virginia Information Technologies Agency (VITA) is responsible for oversight of information technology (IT) projects for executive branch agencies. It also is responsible for security of the state's IT assets and the data therein entrusted to the commonwealth by its citizens. VITA reviews projects and prepares a statewide IT strategic plan, but security deficiencies, needed improvements and necessary funding often were not included.

As a result and prior to this initiative, numerous state agencies were not investing in their information security programs to be compliant with commonwealth IT security policies and standards. Although security requirements have been in place for several years, agencies were not allocating sufficient resources to security programs. In addition, agencies were not planning properly to replace end-of-life IT products such as Windows 2000, Windows XP and other unsupported software. These end-of-life products increased risk to data entrusted to the commonwealth.

Solution

As part of VITA's Commonwealth Security Risk Management (CSRM) program, VITA identified the gaps in the information security programs and project planning of other agencies. The program official launched in August 2014 with VITA's updated IT strategic planning process and continues to operate successfully. Since its implementation, the CSRM program has identified 60 agencies with operational risks and issues (ORIs). At those agencies, 193 ORIs have been identified; 81 percent now will have business requirements in the strategic plan to address the findings.

For the first time, the commonwealth has a comprehensive view of the resources needed and the investments required to ensure agencies have an adequate security program and maintain supported systems.

The IT strategic planning process helps VITA fulfill the agency's responsibility for project oversight and guarantee that appropriate resources are allocated to the areas with the most significant risk. To accomplish this task, clear communication to stakeholders and participants is crucial.

Mandatory training was initiated to help agencies understand how to implement the strategic plan. Each agency had staff attended trainings on ORI and a subsequent meeting with their VITA customer account manager who explained the details for each finding leading to an ORI. This allowed the agency to express concerns. This simple step was critical to understanding the risk management portion of the IT strategic planning process.

Integration into the strategic plan involved a combination of business processes and technology. CSRM was integrated into the IT strategic planning and project initiation process to evaluate new projects and programs that are submitted for VITA's project oversight approval. When it's received, CSRM staff review the project or program and identify whether the agency should commit funds and address outstanding security issues before proceeding with an additional project. This process also integrates into the commonwealth-wide risk management program to help reduce risks to commonwealth IT systems and data.

In the past, VITA proactively identified ORIs in the IT strategic plans for agencies with insufficient security, audit and risk management programs. When agencies submitted their IT strategic plans with requests for new IT investments, VITA reviewed any open findings for the agency. If an ORI is identified as a significant risk, the CSRM team may recommend that the chief information officer (CIO) of the commonwealth hold the investment request until an appropriate plan of action or remediation was in place to address findings.

According to the Code of Virginia, the CIO may limit additional IT investments pending acceptable corrective actions and recommend to the governor and secretary of technology any other appropriate actions. This legislative capacity is one of the cornerstones of the implementation of the program. The section of code allows the CIO to require remediation or a remediation plan to be put in place before an agency can invest in additional technology services.

Significance of the Project

Agencies no longer have the option to delay maintenance or replacement of critical information systems. This provides an opportunity to clearly identify the operation and maintenance costs of running agency IT systems. Additionally, agencies can no longer defer funding their information security programs or legacy system upgrades. The change will protect Virginia by avoiding further development of "30-year-old" systems, reduce risk to the commonwealth IT environment, and ensure the necessary project plans are in place to maintain a supported IT environment.

Several of NASCIO's State CIO Priorities for 2015 apply to this initiative, including:

- Security (1)
- Consolidation/optimization (3)
- Budget and cost control (5)
- Strategic IT planning (7)
- Customer relationship management (10)

Governor Terry McAuliffe has listed cybersecurity in the 2014 Governor's Enterprise Strategic Priorities. The efficient use of IT resources and legislature's focus on cyber and IT resource supplement the governor's goal to "enhance current technology platforms and infrastructure while protecting all data." Stakeholders include:

- The Governor – Ensures systems remain secure and support cybersecurity initiatives
- Legislature – Understanding of where resources should be allocated to address significant security and enterprise project concerns
- The CIO – Implements best practices and ties cybersecurity to the funding of projects and programs, understands the prioritization of projects, legacy and non-supported system remediation
- Citizens – Ensures efficient use of resources citizen data remains safe and secure

Incorporating security into the strategic plan gives VITA a better understanding of the funding requirements of other agencies. It also prevents systems from becoming legacy; and, if there are existing legacy systems, everything necessary to keep them up-to-date is done.

Benefits of the Project

The incorporation of security into the IT strategic planning process includes many long-term goals that will benefit the commonwealth. Fewer legacy systems, better funding planning, and identification of cost for operations and maintenance allows for:

- A better understanding of support contracts and whether to in-source or outsource or approach with a different strategy
- Ensures operational maintenance and costs are included as part of the project/program lifecycle

It also impacts key stakeholders, including:

- Governor – Reduces IT risk to the operation of the environment, both financial and security
- Legislature – More decision information when approving/developing budgets for agency programs
- CIO – Allows for a better understanding of IT investments needed to maintain the environment and for a better understanding of the necessary investment to address cyber security issues
- Citizens – Results in better management of commonwealth funds

The updated IT strategic plan also provides an opportunity for better planning, understanding and a more secure IT environment. This gives VITA an opportunity to plan in advance for the annual budget. The commonwealth will carry fewer security risks.

The program improves the identification of estimated costs for maintenance, understanding of how many systems and environments are impacted, and identification of agencies that need to expand or reprioritize budgets.

As stated by Governor McAuliffe, Virginia “[strives to] not only [become] recognized as a national leader, but *the* leader [for cybersecurity,]” by meeting cybersecurity priorities, following best practices and protecting the systems and data entrusted to the commonwealth.