SOLUTIONS & IDEAS

TRANSFORMING THE ENTERPRISE OF GOVERNMENT

Making the business case for cybersecurity

Cybersecurity has been one of the fastest growing sectors in the federal government over recent years. It's a 24/7/365 job as threats are constant in an online world. In fact, the Government Accountability Office reported in June that "the number of cyber incidents reported by federal agencies increased in fiscal year 2013 significantly over the prior three years."

At more than 46,000 cyber incidents in fiscal 2013 and growing, greater assets will be required to fund cybersecurity programs. Have you asked your team: "What are we doing to ensure budget allocation for cybersecurity not only today, but in the coming years?"

One of the best ways to justify cybersecurity investment is to develop a business case through the Capital Planning and Investment Control (CPIC) process. And the best time to finesse business cases through CPIC is right now.

Even with the growing cyber threat, agencies are being asked to defend their IT portfolios and adapt new technologies in order to reduce IT spending.

Cybersecurity teams must advocate for their programs and be able to defend the need for funding. CPIC is critical for cybersecurity leaders if they are to effectively manage their portfolios.

The Office of Management and Budget mandates that agencies develop an annual business case (formerly the Exhibit 300). OMB expects agencies to submit business cases for its review and inclusion on its public-facing Federal IT Dashboard.

In September, agencies submitted their IT portfolios, including budget requests and initial budget year 2016 business cases. Final business cases will be sent in late February 2015. This interim between initial and final submission is when agencies should thoroughly review the current and future state of their IT portfolios.

Now is the time to ask, "Do we have adequate funding to protect the agency from online attacks now and in the future? Are resources in place to ensure that these programs can operate in a high-threat environment?"

This is more than examining last year's budget to see how much was spent on cybersecurity and then allocating a nominal funding increase for future years. That is not effective planning and potentially increases risks to the programs. If the program needs are not in place, program professionals need to communicate shortfalls to leadership.

Agency leaders need a full understanding of their business environment to include the organizational missions, portfolios, architecture, capabilities, resources and constraints so that they can make hard decisions if resources need to be reallocated. They must understand the cybersecurity universe, not only within the federal sector, but to the extent possible how the private sector is planning and budgeting to meet online threats.

That may require agency leaders to completely rethink and reassess their programs.

CPIC supports planning

In a complex business and IT environment, the repeatable CPIC process enables the federal government to control its IT funding and manage IT programs. In layman's terms, the CPIC process can be thought of as a three-legged stool: budget planning and implementation, program management and control, and management and oversight. Each leg is critical to support the stool.

CPIC was envisioned to be a process that links budget planning, and strategic planning to a specific program and its performance. By leveraging the OMB business case, agencies have at their fingertips a multiyear budget plan, justified investment portfolio and business case, and efficient plan for resource allocation.

KEVIN SMITH
INTEGRITY MANAGEMENT CONSULTING

Use the next three months to analyze the data that was submitted to OMB in early September. Doing so will make a stronger case for the cybersecurity programs that will be a major requirement for the future. Now is the time to ask and answer the question, "Does our agency's IT program make the budget case to counter expected and unexpected cybersecurity threats?" □

Kevin Smith is a senior program manager for Integrity Management Consulting.