Chapter XV
Enterprise Architecture as Context and Method for Designing and Implementing Information Security and Data Privacy Controls in Government Agencies

Scott Bernard
Carnegie Mellon University, USA

Shuyuan Mary Ho
Syracuse University, USA

ABSTRACT

Government agencies are committing an increasing amount of resources to information security and data privacy solutions in order to meet legal and mission requirements for protecting agency information in the face of increasingly sophisticated global threats. Enterprise Architecture (EA) provides an agency-wide context and method that includes a security sub-architecture which can be used to design and implement effective controls. EA is scalable, which promotes consistency and alignment in controls at the enterprise, program, and system levels. EA also can help government agencies improve existing security and data privacy programs by enabling them to move beyond a system-level perspective and begin to promote an enterprise-wide view of security and privacy, as well as improve the agility and effectiveness of lifecycle activities for the development, implementation, and operation of related security and privacy controls that will assure the confidentiality, integrity, and availability of the agency's data and information. This chapter presents the EA^3 "Cube" EA methodology and framework, including an integrated security architecture, that is suitable for use by government agencies for the development of risk-adjusted security and privacy controls that are designed into the agency's work processes, information flows, systems, applications, and network infrastructure.

INTRODUCTION

Designing and implementing effective controls for information security and data privacy in government agencies is optimized through integration with other areas of governance including: strategic planning, capital investment planning, enterprise architecture, program management, and workforce planning. This chapter focuses on the role that enterprise architecture (EA) plays in designing, implementing, and operating security and data privacy controls in complex organizations, including government agencies. Information security and data privacy are intertwined concepts that work like a thread that weaves through the strategic, business, and technology levels of an EA framework to produce risk-adjusted solutions that assure the confidentiality, integrity, and availability of the agency's data and information in the face of growing global threats to government functions and mission accomplishment.

The threats to the security of a government agency's business and technology operating environment come in many forms. This includes hackers, disgruntled employees, runaway technologies, poor system maintenance, natural disasters, terrorism, and unintentional mistakes. As the global use of information technology (IT) continues to accelerate, government agencies are increasingly exposed to daily threats to the confidentiality, integrity, and availability of their information. How seriously the agency addresses these threats is often related on how aware the agency is of its dependency on IT to support key government services, and the probability of a threat affecting the agency. Without an awareness of the full scope of global threats and/or industry best practices to counter those threats, government agencies may not invest in a sufficiently robust and scalable information security and data privacy program, nor will they incorporate best practices such as EA to promote program success.

One fundamental aspect of security and privacy is the realization that there isn't a 100% foolproof solution or set of solutions for any government agency. The reason for this is that program activities and controls are created by members of the agency, and even the people in the most trusted security or system administration positions can decide to disable, evade, or sabotage the security solutions. This type of insider threat is the "Achilles Heel" of all security and privacy programs, and creates what are referred to as "risk-adjusted" solutions. This means that a security or privacy solution is selected based on several considerations, including the cost, the level of protection needed, the effect on end-users and system administrators, and the effectiveness of available technologies.

An integrated set of security and privacy controls for the agency is best created by including these requirements in the planning of all EA segments, components, and systems; doing so in a top-down manner (beginning at the "strategic" level of the EA framework) so that security is an embedded part of all of the agency's strategic initiatives and business services. For information-centric enterprises, including security and privacy as a required design element of strategic initiatives can provide a strong and meaningful statement about the importance of protecting the business and technology operating environment.

Information security and data privacy requirements and solutions should be a consideration in business process reengineering and improvement activities throughout the agency, and should be part of the design of information flows, IT systems, applications, databases, knowledge warehouses, Websites, and network infrastructures. Information security and data privacy are also key checklist items when making acquisition decisions for IT hardware, software, and support services.