Security Architecture

PREPARED BY JOE MARSHALL AND JON MUNSHAW

Updated October 29, 2019

TALOS

CONTENTS

INTRODUCTION

Security architecture and design is a vital function of a healthy enterprise. It's essential to be able to articulate risk to the larger business and maintain risk thresholds as defined by the policies set by leadership. Security architecture is, fundamentally, about understanding IT architecture relationships, and ensuring security is a vital element of its implementation. In conjunction with governance, risk and compliance mandates, a strong security architecture program will be able to articulate risks to various stakeholders within the enterprise and ensure security standards are met at the outset of a project.

THE PROBLEM

It's not easy to be a security architect. You have to be knowledgeable about many technical topics and must rely heavily on your relationships with the larger business to find acceptable ways to enable the business to operate securely. Security does not operate in a vacuum — an architect performs a careful balancing act with the demands of the business while minimizing the risk to the enterprise. To accomplish that, architects must maintain key relationships with IT and project management groups. This also means a security architect must have a strong fundamental core in IT architecture and technology, security architecture, security technical controls, cyber threats, and strong soft skills to communicate all of these things to various aspects of the business. Security architecture and design are the tip of your spear to steer your business into acceptable risk waters. Having security built into projects and your enterprise from the beginning is both more efficient and vastly cheaper than bolting on controls after the fact. As a CISO, it is absolutely vital that security architects have a seat at the table for projects big and small to ensure a secure enterprise, and enshrine their inclusion as a standard (and documented) business practice.

A couple of special points here are worth mentioning: A security architect will have to manage external architectures not contained in the actual enterprise, but can directly affect the risk posture of the enterprise. These should be high on the radar on any architect in our increasingly cloud-connected world. Additionally, an architect should understand IoT security — these devices, like HVACs, IP Cameras, and other third-party services are problematic for security and may introduce risk into an enterprise outside of the understood risks by commodity hardware, software and outside personnel.

THE SOLUTION

NIST Special Publication 800-53, specifically PL-8, does a great job of explaining the importance of this, and the supplemental controls are great, as well. Security architecture is, at its core, a vital part of a defense in depth strategy. With a strong security architecture and design program in place, you'll be able to manage your enterprise's risk on both project-to-project tactical level and larger risk-informed strategic level.

CHECKLIST

ID	Item	Y	Description
Security Architecture			
	Cultivate a security architecture program that helps the business address the risks associated with confidentiality, integrity and availability.		Develop risk-based policies that ensure your architect has an effective back-stop to ensure security standards are being met consistently.
	Make the inclusion of security architecture a vital and business mandated element in all stages of IT project design and implementation. No project is too big or small.		Hire wisely — A security architect must be incredibly knowledgeable about IT and security, but must have equally strong communication and people skills.
	Ensure that your architects have a strong grasp of third-party and internet-of-things-based threats and risk.		Make sure your architecture programs also have a strong grasp of legal and regulatory requirements, and that those requirements are reflected in the security architecture.
	Empower your architects to interface with any echelon of the business and cultivate important relationships to ensure risk-based policies are understood and accepted.		Ensure the business knows that security architecture is there to enable the business, not hinder it. Everyone wins when the business operates securely.