



Our Philosophy

Robust information security is driven not by technology but by business needs, evaluated with technical skill, and implemented together with operational processes that render it effective. Information Security measures are not technical decisions, they are *risk management* decisions that employ technical criteria. Understanding this fundamental philosophy allows the undertaking of information security efforts within your organization, enables clear requirements that permit accurate project management, and facilitates a high-quality outcome while managing costs. The bottom line is – it's *Your* business, and we're here to help. We *only* succeed if you do.

Security Architecture

Information Security technology continues to evolve at a fast pace in response to rapid proliferation of internet-enabled applications. As e-Business services move your capital into the electronic domain, the need to protect these assets increases. Balancing e-Security with performance in modern network infrastructures can be a daunting task: designing VPN's with QOS, integrating Intrusion Detection and Network Management, implementing perimeter security while allowing secure remote access, building an *integrated* incident response capability ... require expertise well beyond the administrative and technology knowledge needed to operate and maintain such an infrastructure. Choosing the correct architecture requires more than just technical specification. Good architecture decisions also require solid business, economic, and operations management knowledge, integrating business management with technology, and not unlike insurance decisions, optimizing cost-effectiveness, providing enough without spending too much. Sound security architecture *enhances* business all the way to the bottom line: it provides ***Return on Investment***.

Security Design

Architectural Services define an overall approach and high-level functional design. Translating this to detailed design requires a thorough understanding of high-level architecture as well as detailed capabilities and configurations across a wide array of software and hardware products from multiple vendors. Detailed design services provide you with specific hardware and software configurations that can be readily implemented. Detailed Security Design services integrate the technical architecture requirements with the asset and intellectual property protection needs of your business as expressed in your company's security policy. The result is a secure infrastructure where each element of the architecture is clearly derived from needs of the business, can be audited, verified, and later can be modified as business and market needs demand.

Security Policy

The need for a security policy in business is often misunderstood. Robust policy provides documentation of business needs expressed as technological and operational requirements. It is the reference foundation that articulates each organization's unique requirements in a manner that can be directly designed, implemented, and verified. Perfect security is not absolute security, rather, it is the optimum mixture of risk acceptance and risk mitigation through technical and operational processes and capabilities. No outsider can make these decisions for you. Rather, by quantifying risk and providing knowledge of how these risks can be mitigated as well as sound cost estimation, you are able to make the decisions that are best for your business. Once the decision processes are complete, the rationale is captured in a Security Policy Analysis, while the specific resulting requirements are captured in a Security Policy document. This unique combination of documentation enables you to readily revisit your requirements as business needs change.