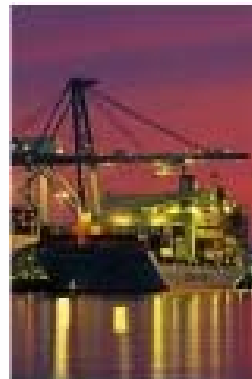


Omnidirectional CyberSecurity – The ability to achieve and maintain the highest level of information Confidentiality, Integrity and Availability throughout the enterprise, as well as throughout the loosely coupled collaboration networks with trading partners, regulatory agencies and subcontractor/vendors is one of the keys to survival and success into today’s information centric world. Comprehensive Information Assurance is sufficiently difficult to achieve in a stable, controlled environment. The reality, however, is that enterprises are constantly challenged by the introduction of new technologies, level of staff expertise and the need to securely collaborate with organizations **beyond their direct control**. These challenges are constant and coming from every direction. Today’s information technology professionals need the ability to integrate policies, processes, procedures, risk profiles and technology into an omnidirectional view of a collaborative, secure, information processing infrastructure.

Today’s research and development teams consist of multiple organizational staff members with very deep and focused expertise who need to freely collaborate with one another on a project-by-project basis. Healthcare, for example, is one of the most highly “networked” industries requiring the value added input from multiple, geographically dispersed professionals from different organizations working on a single patient or case.



A single, productized solution will not work for everyone. A majority of your business processes are very different from those of other organizations. Yes, you can standardize on an accounting, human resources and customer relationship applications, but how you integrate other unique processes of your business is what sets your organization apart from all others. Many Managed Security Services Providers (MSSP) have fine technology and solutions for homogeneous environments, however, their packaged solutions start to break-down when legacy infrastructure and VPNs with collaboration partners further complicated by different or conflicting standard operating procedures (SOPs) across multiple collaboration networks are involved. ***Omnidirectional CyberSecurity is a suite of consulting services combined with “best-in-class” technology products customized to meet the demanding requirements of your organization’s mission critical IT infrastructure.***



Argosy Omnimedia has been working with clients since 1997 on the implementation of secure, Internet-enabled, enterprise-wide and multi-organizational collaboration networks and e-Business solutions.

Argosy's security professionals can conceptualize, implement and operate a comprehensive, **Omnidirectional CyberSecurity Solution** for your organization that is:

- Engineered to the specific and unique SOPs, staffing, functional and technology requirements of your networks
- Compliant with applicable regulations and standards such as state consumer breach notification, FISMA, NIST and vertical market organizations (e.g. HIMSS CPRI Toolkit).
- Enterprise-wide and collaborative in scope built upon Argosy's institutional knowledge of e-Business design expertise coupled with business continuity best practices.
- Federated, distributed information technology assets across loosely coupled multi-organizational collaboration networks like those found in research and development, life science, healthcare communities of interest, and shared high-performance computing environments
- Staffed by a combination of Argosy onsite personnel supported by offsite, 24/7 technology/product expertise. This hybrid staffing approach ensures that sensitive information never leaves your network boundary and you gain the benefits of having a highly leveraged, trained and skilled outsourced organization with "ownership" of your infrastructure, problems and solutions.

Argosy solutions combine our best-in-class consulting, development and operations staff expertise with best-in-class technologies and products in the following functional areas:

- Authentication, Local & Remote
- Authorization
- Public Key Infrastructure (PKI)
- Managed IP & VPNs (Walled Garden)
- Firewall
- Intrusion Protection
- Patch Distribution and Management
- Performance Profiling and Monitoring
- Threat Correlation
- Vulnerability Analysis

Argosy security services include:

- Security architecture development
- Risk analysis and assessment
- Security assessment and testing
- Managed security services (on-site and off-site)
- Investigation of security events
- Forensic analysis
- Procurement management – requirements, RFP development, technology and vendor analysis and recommendation

Argosy's staff consist of experts with extensive expertise in the information assurance field characterized by:

- Certifications (e.g. CISSP, CISA, DRI)
- Security services bonding
- Graduate degrees specializing in information assurance

For a complimentary readiness analysis contact:
Rob.Montgomery@argoc.com 301.816.9373 x17
www.argoc.com