



Omnidirectional Cybersecurity and Privacy

Argosy Omnimedia, Inc.

Version 0.9

05/25/2005

Document Number: A001700

Argosy Omnimedia, Inc
6110 Executive Blvd., Suite 1065
Rockville, MD 20852
<http://www.argoc.com>

For more information contact:

Rob Montgomery
301.816.9373 x17

rob.montgomery@argoc.com

Table of Content:

What is Omnidirectional Cybersecurity?3

What is Different about Argosy’s Security Solution?.....3

 “Nobody has ever been fired by buying Symantec”4

Who has to comply with security regulations?.....5

Who enforces compliance?5

What regulations could apply to me?.....5

 FISMA5

 HIPAA.....5

 DITSCAP5

 NIACAP6

What is Certification and Accreditation?.....6

 Services Provided by Argosy6

For More Information 11

What is Omnidirectional Cybersecurity?

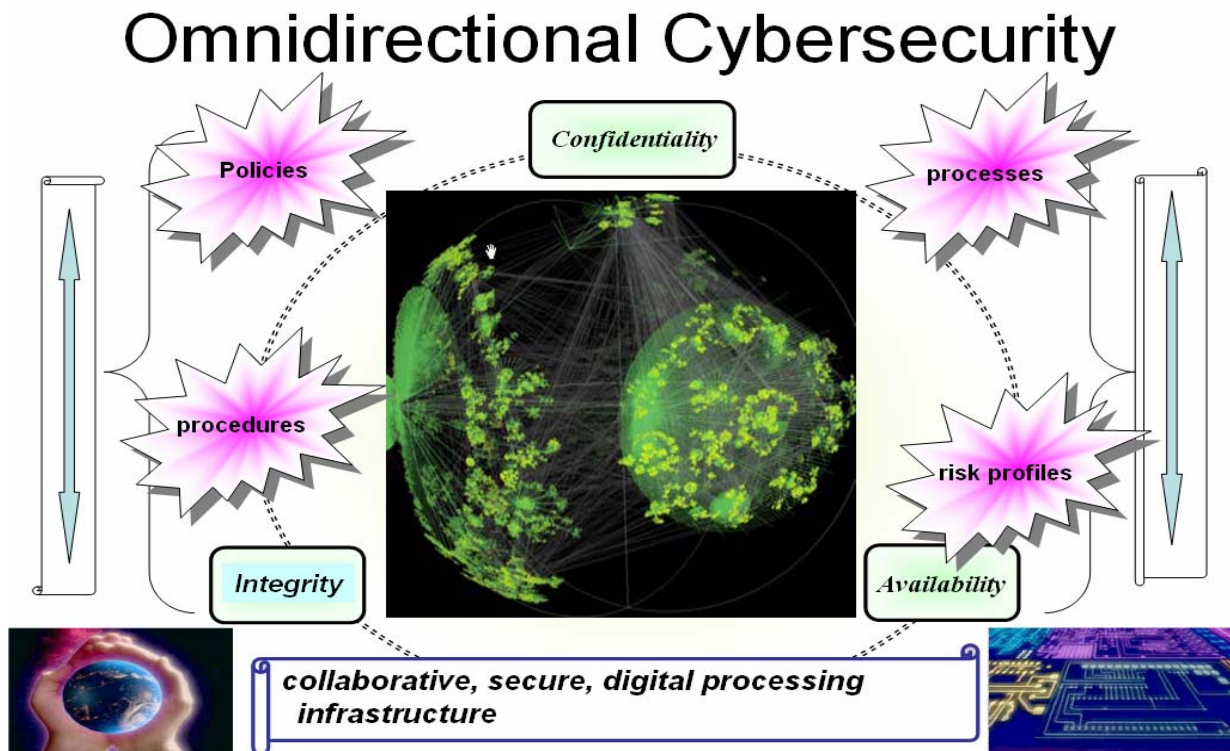
Omnidirectional CyberSecurity – The ability to achieve and maintain the highest level of information **Confidentiality, Integrity, and Availability** throughout the enterprise, as well as throughout the loosely coupled collaboration networks of your organization’s trading partners, regulatory agencies 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, digital processing infrastructure.

What is Different about Argosy’s Security Solution?

What is it that makes Argosy’s Omnidirectional Cybersecurity unique?

- Transcends traditional enterprise-wide network boundaries to secure and protect distributed, collaborative network infrastructures
- Secures non-traditional network devices such as medical diagnostics, imaging and data acquisition terminals (e.g. RFID)



- Integrated Privacy domain into design, assessment, and remediation.

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 federal regulations and standards (e.g. FIPS 130 and DoD 8500)
- Enterprise-wide and collaborative in scope built upon Argosy's institutional knowledge of e-Business design expertise coupled with business continuity best practices...we build it right because, often times, we have to operate and maintain it as a Business Process Outsourced (BPO) service.
- Vertical market focused on dispersed, 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, but 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:

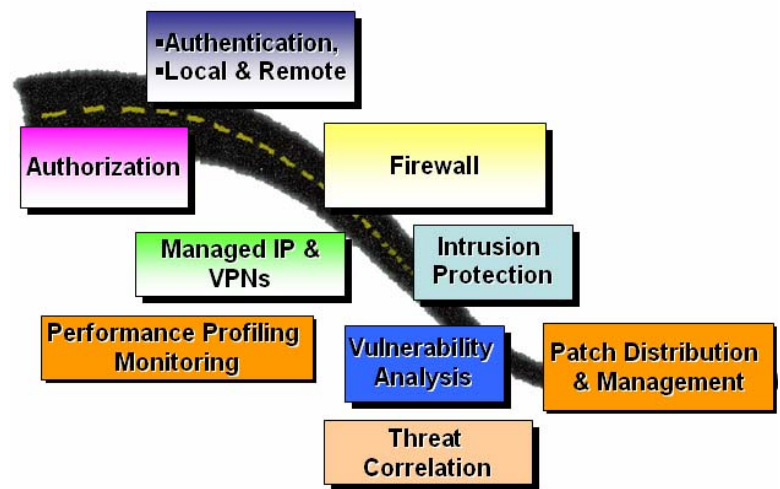
- Authentication, Local & Remote
- Authorization
- Managed IP & VPNs (Walled Garden)
- Firewall
- Intrusion Protection
- Patch Distribution and Management

- Performance Profiling and Monitoring
- Threat Correlation
- Vulnerability Analysis

Argosy security services include:

- Security architecture development
- Risk analysis and assessment
- 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)
- Graduate degrees specializing in information assurance
- Security services bonded

“Nobody has ever been fired by buying Symantec”

Sound familiar? It's a new security spin on an old adage. If your organization's culture and policy is;

“there’s nothing special about our business processes and what we do.....we are just like everyone else”, then let’s face it, you would be better served by one of the other leaders in the security industry. Companies like Symantec and ISS have world-class people and technology and your organization may be better served if their packaged solutions fit your requirements.

A single, productized solution will not work for everyone. Like most companies, the critical components of your business processes are very different from those of other organizations. **Your organizational culture and personality is what makes your organization different from all others. This is why your clients and constituents come to you first.** 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, speciality devices like healthcare diagnostics and laboratory devices, VPNs with collaboration partners further complicated by different or conflicting standard operating procedures (SOPs) across multiple collaboration networks are involved. *The reality is, a security architecture requires customization to your unique requirements and information technology investments.*

Who has to comply with security regulations?

- Federal Cabinet Level Departments and Agencies
- State Agencies
- Local Municipalities
- Commercial, private industry

Who enforces compliance?

- Federal and State security and privacy enforcement officers – Home agency compliance
- OMB – Federal agency FISMA compliance
- Inspector General (IG) offices – Home agency compliance
- Commercial entity security officer – To applicable regulations (e.g. HIPAA, SoX)

What regulations could apply to me?

FISMA

The Federal Information Security Act (FISMA) requires each agency to inventory its major computer systems, to identify and provide appropriate security protections, and to develop, document, and implement an agency-wide information security program.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996. As part of the Act, Congress called for regulations promoting administrative simplification of healthcare transactions as well as regulations ensuring the privacy and security of patient information. The security regulations are only one of many components of HIPAA. The security regulations dictate the kind of administrative procedures and physical safeguards covered entities must have in place to ensure the confidentiality and integrity of protected health information.

DITSCAP

The Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) is the standardized approach designed to guide DoD agencies through the certification and accreditation process for a single information technology (IT) entity. The aim is to:

- Provide guidance to organizations
- Standardize the [C&A](#) approach for all services

- Define the scope of effort
- Tailor documentation for all system architectures

The Defense Information Assurance Certification and Accreditation Process (DIACAP) DRAFT will supersede the DITSCAP (DoDI 5200.40). The DIACAP will establish the standard DoD process for identifying, implementing, and validating IA Controls, for authorizing the operation of DoD information systems, and for managing IA posture across DoD information systems consistent with Title III of the E-Government Act, the Federal Information Security Management Act (FISMA) and DoD. Directive 8500.1 directs all DoD systems to transition to DIACAP.

NIACAP

National Information Assurance Certification and Accreditation Process (NIACAP), establishes the minimum national standards for certifying and accrediting national security systems. This process provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of a system or site. This process focuses on an enterprise-wide view of the information system (IS) in relation to the organization's mission and the IS business case.

The NIACAP is designed to certify that the IS meets documented accreditation requirements and will continue to maintain the accredited security posture throughout the system life cycle.

Federal and other legislations:

- Privacy Act
- PATRIOT Act
- Identity Theft
- SSN Protection
- Anti-Spam Measures
- Security Standards

- Cyberspace Security Proposals

What is Certification and Accreditation?

Certification and Accreditation (C&A) is the enterprise-wide analysis of the technical and non-technical security governance, controls and security readiness of the IT infrastructure (assets). The deliverable from this analysis is a report detailing how well the assets comply with the applicable requirements, regulations and acceptable level of risk.

Services Provided by Argosy

Argosy's security professionals have a proven track record of providing outsourced staff utilizing the latest network analysis tools for federal agencies throughout all phases of their C&A planning, implementation, analysis execution, and remediation to the following methodologies:

- DITSCAP
- DIACAP
- HIPAA Security
- NIST/FISMA

Across the following functional areas:

- Policy Development
- Risk Assessment
- Compliance Analysis
- Continuity Planning
- Disaster Recovery Planning
- Security Architecture
- Asset Inventory
- Security Testing
 - Vulnerability
 - Penetration
- Security Management (business process outsourcing or managed security service)

Argosy will develop a security compliance program that is designed to meet your organization's specific needs and requirements.

A portfolio of one-time and recurring services will be designed for your organizational engagement portfolio and can be adjusted, as needed, to address

the changing needs, environment and market positioning of your organization. At the highest level of service, continuous, remote monitoring of your network assets can be performed through a highly secure, VPN channel to provide a constant, comprehensive managed security solution. The outsourcing of this information technology business process to Argosy provides the most cost effective solution to achieving the highest levels of security and information assurance throughout your enterprise.

Policy Development

Policies are critical to information security, but many organizations lack policies or have outdated policies. Argosy provides complete information security policy coverage. If you have existing policies, our comprehensive assessment identifies strengths, weaknesses, and gaps in your information security policy program, and provides you with a benchmark against industry best practices.

Most statutory regulations mandate that Information Security Policies be in place to achieve compliance. Even if you are not mandated to follow such practices, our service will be of great benefit. Argosy has experience providing the following "umbrella" policies:

- System Security Authorization Agreements (SSAA) based on the DoD DITSCAP, NIACAP or NIST
- Security Plans based on NIST
- Security Policy based on ISO 17799

Risk Assessment

Risk assessment is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed. Security in any system should be commensurate with its risks. However, the process to determine which security controls are appropriate and cost effective is quite often a complex and sometimes a subjective matter. One of the prime functions of security risk assessment is to put this process onto a more objective basis.

There are a number of distinct approaches to risk assessment. Risks may be identified during normal operations or as the result of a C&A effort, risk analysis, or an incident. In the past substantial resources have been expended preparing complex analyses of systems with limited tangible benefit in terms of improved security for the IS. Rather than try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them.

What is a Risk Assessment?

The Argosy risk approach will consider:

- Major factors in risk management
- Value of the information, system or application
- Threats and Vulnerabilities
- Effectiveness of current or proposed safeguards

After the threats and vulnerabilities are identified, reducing the vulnerability or the threat must minimize the risk. Argosy will evaluate the degree of risk to the system.

For each residual risk, Argosy will design and implement a counter measure consisting of one of the following:

Deterrent controls to reduce the likelihood of a deliberate attack

Preventative controls to protect vulnerabilities and make an attack unsuccessful or reduce its impact

Corrective controls to reduce the effect of an attack

Detective controls to discover attacks and trigger preventative or corrective controls

A cost benefit analysis of alternatives will be used to identify appropriate cost-effective countermeasures to mitigate the risk.

Compliance Analysis

Compliance assessment, or testing, evaluates the operational implementation of the security design to assess how well the security procedures, software, hardware, and firmware support the highest levels of information confidentiality, integrity, availability, and accountability. Documented compliance is performed to all appropriate laws, directives and policies. At the end of your assessment, you will receive a detailed report containing:

- Management Overview
- Technical overview
- A prioritized findings manifest of configuration problems and device vulnerabilities
- Recommended remediation of configuration problems and device vulnerabilities

Continuity Planning

Effective Business Continuity for pervasive enterprise information systems involves a comprehensive collection of skills, expertise and training to ensure that a given plan, resources and technology meet the expectations of an organization's management, customers and business partners for high-availability business operations. Argosy's staff of experienced IT network engineers and enterprise application development professionals know how to translate these expectations and business objectives into a comprehensive business Continuity plan and implementation that is designed to meet the unique requirements of your organization.

What is the ROI of your business continuity plan?

Placing a value on direct damages associated with the disruption of your organization's information management infrastructure can be a difficult and challenging task. Argosy will work with your business owners to find the best balance between tolerable service outages and intolerable operational disruptions. Through the proper selection of services and technologies and a valuation of the cost of forecasted outages, Argosy can help your organization optimize expenditures on Business Continuity (BC).

From Assessment through Planning into Implementation, Argosy's consulting services cover the full range of management and information technology expertise necessary to ensure highly available business operations under various types of disruption scenarios. Below is a brief overview of some of these services:

Business Impact Assessment (BIA) is designed to elicit, identify and evaluate the value of each IT service to an organization and understand the interdependencies of these services under multiple disaster or outage scenarios.

Security Audit and Assessment (SAA) examines the current practices and technologies that are in place and then make recommendations for improvements. Assessment services include managed probing of current electronic security protections to assess effectiveness.

Business Continuity Plan (BCP), also referred to as a disaster recovery plan, presents a set of recommendations, based on the results from the BIA and SAA, for how to improve overall operational availability through improved security and disaster recovery services such as off-site backup and restoral.

Disaster Recovery Planning

Disaster recovery planning is effectively the preparation of those steps that will be necessary for recovery from a disaster or other crisis situation.

Every business and organization can experience a serious incident which can prevent it from continuing normal operations. This can happen any day at any time. The potential causes are many and varied: flood, explosion, computer malfunction, accident, grievous act... the list is endless.

The Disaster Recovery Plan is the most important item in your armory. It is what you will turn to if there is indeed a disaster or other serious incident. Hopefully, you will never have to use it, but if you do, it can be the difference between the loss of your organization and its survival. It is therefore absolutely critical that it is workable - that it is of sufficient quality to guide you through the crisis.

The plan itself is the core of the whole planning exercise, and is of critical importance. It is vital, therefore, that if you are to manage an incident successfully, the plan itself must be of the highest quality and be up to date.

The Argosy Disaster recovery planning approach will consider:

- Pre-Planning Activities (Project Initiation)
- Vulnerability Assessment and General Definition
- Requirements
- Business Impact Analysis
- Detailed Definition of Requirements
- Plan Development
- Testing Program
- Maintenance Program
- Initial Plan Testing and Plan Implementation

Security Architecture

Security architecture decisions are critical. A poor security architecture can make it difficult or impossible to secure your network and require continuing costly investment in security products and services. Argosy's network security architecture service focuses on defining technical security controls for the client's IT network that build upon existing the existing infrastructure, systems, and policies, and enables a consistent and best practices level of security throughout the network.

Our Key Benefits to Security architecture include:

- Secure your network, systems, and information to the appropriate level
- Identify a clear plan to securing future IT needs
- Save money in security product and life cycle costs

Argosy methodology has three primary goals in any security architecture design:

- **Prevention:** keeping the adversary out in the first place. Prevention applies to both internal and external threats, as well as networks, hosts, and applications.
- **Detection:** recognizing specific instances of improper or unauthorized activities before extensive damage is done. Prompt detection allows the client to isolate an adversary, analyze the probable intent of the attack, and limit the damage when deployed in conjunction with a response.
- **Response:** initiating specific actions to isolate or prevent further unauthorized activity and to recover from whatever damage has occurred. Response includes the containment of the compromise, repair of the vulnerability, recovery, and evidence collection for pursuing the hacker.

Our network security architectural approach and engagement will address the key aspects of the IT network. These are likely to include:

- Major network interfaces to other client networks, business partners, and the Internet
- Underlying network components that form the transport infrastructure
- Common network services and supporting infrastructures
- Network and security management
- User authentication and management
- Key applications

Argosy will provide a security architecture document, technical and executive presentations, and a solutions matrix that will identify how the architecture provides the required protection for current and planned systems, applications, and information.

Asset Inventory

Gain control over your IT environment - and IT costs.

Do you know how many PCs you have installed? Do you know what software you are running and whether the licenses are valid? Keeping track of what you own and who's using it is an integral part of managing the total cost of ownership of your technology investments.

Argosy will help you understand what IT assets you have and where they are located. Our team utilizes our project management methodology combined with the latest technology in data collection tools. This proven process allows us to accurately record and report our findings, providing you with detailed hardware and software data and an overall understanding of your IT assets.

Our Asset Inventory services include:

- External Inventory Services
an external inventory provides a detailed report of all assets in the environment regardless of their utilization. We collect asset specific information available on the exterior of the asset as well as user demographic information including the precise location of the asset.
- Internal Inventory Services
Provides a detailed list of installed software on each workstation, including manufacturer name and software titles with revision levels identified. The software database and associated reports provide a basis for an audit of current software licensing compliance. Information such as BIOS revision dates, installed memory, available hard disk space and software revision levels are also collected. Internal inventories can often be accomplished across your network eliminating the need to visit each desktop.
- Internal /External Inventory Services
Providing detailed hardware and software information, this comprehensive inventory provides an overall understanding of your IT assets. Coupled with department and accurate

location information this combination of both the External and Internal processes provides a means to accurately determine the upgrades necessary to solve many specific business requirements.

Vulnerability and Penetration

“Ethical hacking” is a term gaining popularity in the cybersecurity industry. All this means is that “friendly” forces will try to compromise your network from the outside (and sometimes from the inside) using a range of vulnerability and penetration tools that a typical hacker would use. This recommended (by security best practices) preemptive testing of your network, as a hacker would, is designed to ensure that your organization will not become the victim of a successful attack.

Remediation Services

At the end of the day, an assessment is not worth a whole lot unless the organization is willing and able to remediate those designs and devices that are creating the vulnerabilities in the first place.

Argosy staff can work with your staff to effect improvements across the entire spectrum of options available such as:

- Legacy Network Reengineering
- Device and Technology Recommendations
- Network Architecture
- Procurement Management
- Integration
- Implementation
- Re-testing and Corrective Action Validation

For More Information

For more information contact:

Rob Montgomery

301.816.9373 x17

rob.montgomery@argoc.com

