Information Assurance

A White Paper

Security, Government & Infrastructure, a division of Intergraph

INTERGRAPH

Table of Contents

1. Introduction

The need for information assurance (IA) has increased dramatically in recent years due to computing trends and the proliferation of the Internet, e-commerce, and advanced computer crimes and cyberthreats. As a result, more organizations are realizing the need for effective countermeasures against attacks on their information. However, recognizing the need for information assurance and security is only half the battle. With innumerable security technologies, vendors, and plans to choose from, and a lack of security knowledge and dedicated resources, many organizations simply do not know where to begin.

Assessment is a key starting point to creating an effective security program and should serve as a regular means of testing existing security programs and capabilities. Although no security program can be 100 percent effective, there are several fundamental security objectives and methods that should be a part of any organization's information assurance infrastructure. Using effective security planning and technology, organizations can mitigate the many threats they face and allocate scarce resources to protecting their most valued information.

Intergraph offers comprehensive, tailored IA solutions to commercial and government customers to help organizations protect their information and knowledge. Intergraph delivers IA through a product life-cycle approach to security, which comprises risk review, policy, implementation, administration, and audit. Operating in today's information-based world is not without risk, but through effective IA solutions, organizations can reduce that risk and increase success.

2. Information Assurance

1. Information assurance and security have become major concerns in today's business world. (See Figure 1.) With business becoming increasingly information-based and the Internet and e-commerce growing tremendously, organizations face significant challenges in trying to protect their information. Threats such as hacking, employee information theft, and viruses can cause severe damage to a company's operations and reputation. This document should serve as a learning tool for managers to use to educate themselves on information assurance and help them understand why it is so important, how to assess their own security needs, and how to implement an effective information assurance/security program.

2005 CSI/FBI Computer Crime and Security Survey

- Virus attacks continue to be the greatest source of financial losses. Unauthorized access, however, showed a dramatic cost increase and replaced denial-of-service as the second most significant contributor to computer crime losses during the past year.
- Unauthorized use of computer systems has increased slightly according to survey respondents.
- Two specific areas (unauthorized access to information and theft of proprietary information) did show significant increases in average loss per respondent.
- Web site incidents have increased dramatically.
- The percentage of organizations reporting computer intrusions to law enforcement has continued its multi-year decline. The key reason cited for not reporting intrusions to law enforcement is the concern of negative publicity.
- More than 87 percent of the organizations conduct security audits, up from 82 percent in last year's survey.
- The Sarbanes-Oxley Act has begun to have an impacat on information security in more industry sectors than last year.
- The vast majority of respondents view security awareness training as important. However, (on average) respondents from all sectors do not believe their organization invests enough in this training.

Figure 1: *2005 CSI/FBI Computer Crime and Security Survey*

3. Information Assurance Defined

Information assurance (IA), the act of securing and protecting an organization's electronic assets, is a continuous life-cycle process that must be managed effectively as part of an organization's overall security strategy. Historically, management used a hands-off approach to dealing with their organization's IT issues, essentially leaving them to information systems (IS) staff. Today, successful companies treat mission-critical computer networks and the information they contain as any other valuable organizational asset – they understand and actively manage their systems as part of their overall business strategy.

IA is a business enabler, allowing organizations to conduct electronic business operations in a secure fashion. With the explosion of the Internet and e-commerce and subsequent usage of these vehicles in everyday business operations, IS security is now viewed as a measure of business competence. Shareholders and taxpayers expect organizations to protect their information assets as vigorously as they protect their investment and public assets. By creating a security program, an organization's management team makes a clear statement to its stakeholders that the protection of electronic data is an enterprisewide priority. Protecting information assets also reduces an organization's exposure to liability in the event of a security incident, a crucial benefit in today's world of increasing security threats.

4. Market Characterization and Analysis

"Security is off the back burner. In the old world of private networks, you get security through the privacy of the network In the new networked world, you want to keep the bad guys out, but you also want to let the good guys in."
– Information Week[2]

The above quote captures the dilemma most organizations face today. The Internet represents a fundamental paradigm shift away from processing-based computing to information access-based computing. Complicating this transition is the need to protect the most important assets of an organization – information and knowledge. Financial data, intellectual property, key business processes, product specifications, customer lists, marketing plans, knowledge repositories, and sensitive/confidential data are only a few examples of these many intangible assets.

4.1 Current Situation

The value of information as a corporate asset depends on an organization's ability to maintain its information confidentiality, integrity, and availability. However, challenging these requirements is an ever-increasing need to provide employees, business partners, customers, and government agencies proper access to corporate information. Subsequently, many companies are employing intranets, extranets, and other Web applications that often subject their information and knowledge to threats.

4.2 Market Drivers and Trends

Traditionally, organizations built security systems based on a strong perimeter defense, which was appropriate for mainframe-based computing with little external interaction. However, several trends have changed the perimeter-based security model:

- Computing has largely shifted from centrally located, shared mainframe computers to single user workstations on individuals' desktops.
- Desks have become virtualized. People work from home, while traveling, or in meetings, but still need access to computing resources and corporate data. Users, not a central computer resources group, often administer these virtual workstations.
- Companies are not necessarily single entities. A company may have offices throughout the world; it may enter into joint ventures with competitors; and it may need to exchange information with numerous suppliers, customers, government groups, and other entities.
- Most professionals use e-mail and have Internet access from their desktop, an increasing number of companies have Web sites, and distributed computing is the dominant computing model. All this personal connectivity comes at a price. Increasingly, people deal electronically with others whom they do not know and have no reason to trust. People are also far more inclined to electronically distribute proprietary information that they have not protected through encryption or other means.

In addition to computing trends, a growing number of threats to organizations' bottom lines drive the need for information security. Crippling distributed denial-of-service attacks, powerful viruses, information theft intrusions, and Internet abuses by employees are just some of the things that can debilitate business operations. Whether from a virus-writer in a far off country or a disgruntled internal employee, attacks on information infrastructures can cost millions in liability claims and lost sales, customers, trade secrets, and productivity. According to a survey conducted in 2005 of U.S. corporations, government agencies, universities, and financial and medical institutions:

- 69% of respondents either detected computer security breaches within the last 12 months or did not know whether their computer security had been breached
- Respondents reported more than $130.1 billion in financial losses from computer security breaches.
- The most serious financial losses occurred through virus attacks (more than $42.7 billion), unauthorized access (more than $31.2 billion), and theft of proprietary information (more than $30.9 billion).
- 65% of respondents detected system penetration from the outside
- 35% of respondents detected denial-of-service attacks
- 48% of respondents detected employee abuse of Internet access
- 75% of respondents detected computer viruses[5]

These statistics illustrate the legitimate dangers inherent in attaching to and transmitting data over an insecure network like the Internet. However, the tremendous proliferation of the Internet makes it a necessity in today's business environment. That is why security and information assurance solutions are critical to an organization's ability to build and maintain its information infrastructure.

4.3 Current Technology

Now that security has become a key focus across most industries and organizations, customers have a breadth of security technology and services at their disposal. Over recent years, the network security market has exploded with products that are increasingly more powerful and easier to use. Similarly, the number of firms specializing in information assurance services has dramatically risen.

Today, many security applications are based on public key infrastructure (PKI). This form of transaction security helps ensure that business transactions consider data integrity, confidentiality, authentication, and nonrepudiation. In business terms, PKI allows two businesses to use a public network like the Internet to verify users are who they claim to be (authentication), allows private communication with one another (confidentiality), ensures messages parties exchange have not been tampered with (integrity), and prevents a denial that a business transaction occurred (nonrepudiation). PKI can also confirm the validity or time of issue of an electronic message and validate the authenticity of a message's issuer.

PKI technology can be applied anytime an organization passes information over an open medium, such as the Internet, or when the sensitivity of information warrants its protection, such as when storing sensitive material on an easily accessible computer. Currently, PKI supports electronic commerce, messaging systems for the Department of Defense, cellular telephony, Internet communications, and many other applications. Financial institutions such as banks and brokerage firms, health care entities like hospitals and insurance firms, and government agencies all use PKI to provide secure identification, authorization, and access.

PKI is one of several security technologies organizations may employ to protect their information. With e-commerce increasing as a common business practice, more organizations are relying on security technologies to protect their electronic data. The table in Figure 2 lists some of these other popular security tools and their usage among e-commerce companies:

EC Security Controls[1]

Percentage of respondents using the following security tools and products in their e-commerce initiatives

TOOL	B2C	B2B
User IDs/Passwords	86%	85%
Firewalls/Packet Filtering	N/A	79%
Transactional Encryption (SSL/SET/SHTTP)	67%	60%
Server Segregation (DMZ)	50%	51%
Application-Specific Controls	44%	N/A
Authentication Servers (Kerberos, Radius, RAS)	40%	46%
Digital Certificate-based Authentication	39%	45%
Point-to-Point Encryption (VPNs)	38%	56%
Dedicated Circuits	20%	36%
Authentication Tokens (hard or soft, including smart cards)	20%	29%
Other	3%	3%
None	3%	1%

Figure 2: *EC Security Controls*

5. Information Assurance and Security Fundamentals

Simply defined, information security is the methods used to protect information and information assets like computer systems. These methods can be organized into three categories, including management controls (created by managers), operational controls (implemented by people), and technical controls (implemented by computer systems and software). Typically, people think of security in terms of technical controls. However, as Figure 3 explains, all three types of controls are critical to effective security:

Management controls	Operational controls	Technical controls
Computer security policy	Personnel security	Identification and authentication – permits only authorized users into a computer system
Management of the corporate security program	Security training and awareness	Access control – permits access only to data or systems for which the user has been authorized
Computer security risk management	Business continuity planning	Audit trails – records kept by a computer system to associate a potential security event with an individual end user
	Security incident handling	Cryptography – an important tool for protecting information
	Physical security	

Figure 3: *Types of Controls*

Information security is also a form of risk management. Despite the best security technologies and architecture, there is no known way to provide complete information protection. Thus, risk mitigation is the only practical approach for an organization to take. In risk mitigation, management prevents the most probable and costly threats while accepting some residual risk. Even government intelligence agencies, which have very stringent security requirements, have moved from the costly risk avoidance approach to mitigation. Although no security plan can be guaranteed to be 100 percent effective, any plan that targets key security objectives with competent technology and administration can greatly reduce the likelihood that a security incident will occur. Figure 4 highlights several major objectives and exemplary applications of security:

Security objective	Definition	Traditional methods	Electronic methods
Authentication	User authentication verifies the identity of the other party. Data origin authentication verifies the origin of the data.	Driver's license, passport, or other authentication by a trusted authority	Digital Certificates – digitally signed by a trusted external authority
Confidentiality	Protects data from unauthorized access.	Physical security, such as conducting business behind closed doors or locking papers in a safe	Encryption/Decryption – a cryptographic method of scrambling data into an unreadable form that can later be unscrambled back to its original, readable form
Integrity	Ensures information is accurate and has not been tampered with. This is one of the highest priority goals of most organizations.	Careful inspection of the document to ensure it accurately represents the intended data	Hashing – a technique that can detect a change to even a single bit of data
Nonrepudiation	Provides proof of participation in an electronic transaction, a key need in e-commerce	A handwritten signature	Digital Signature – the electronic equivalent of a written signature that proves a transaction occurred
Authorization	Permission to perform a task or operation	A handwritten signature	Digital Signature

Figure 4: *Major Security Objectives*

6. Assessing an Organization's Security Status

If one were to ask a manager in an organization that has not yet established a complete security program, *"How secure are your organization's computer and network systems,"* most often, the response will be *"We think our system is fairly secure. We have a firewall, a good password, etc.,"* or something similar. This uncertainty about security is typical of most organizations' level of confidence in their system security. Unfortunately, hostile parties need only to find a single network vulnerability, while an organization must protect against a myriad of threats. In evaluating their organization's security program (particularly when doing so for the first time), senior management should ask certain tough questions to fully understand the strengths and weaknesses of their program. See Appendix A for a complete self-assessment questionnaire: In addition to a self-assessment, Intergraph offers the following caveats:

- Management must take a constructive, hands-on approach to help the IS staff deal with security.
- Although the intent is to evaluate in an unbiased and objective way, equal emphasis should be given to the successful security initiatives in place as well as recommended improvements.
- Rarely will you find an IS staff that does not believe or care that security is an important issue. However, if the IS staff is already overwhelmed by current workload, they will be unlikely to welcome the prospect of another major initiative.

Selecting a security solution should be based on the following criteria:

- Ease of maintenance and use (automated solutions that are transparent to the user and easy to maintain are invariably more successful).
- Industry standards (to improve interoperability and integration skill sets of the system administrators who will manage the tools).
- Cost of implementation, development, and maintenance

7. Investing in Information Assurance

Measuring return on investment (ROI) for any IT investment is difficult. This is particularly true for security because it is an ongoing process rather than a discrete project. When justifying an investment in information assurance, an organization should base its decision on the risk assessment process described earlier. By valuating information assets and determining if threats to those assets are too high to simply ignore, an organization can make a reasoned security investment decision.

Funding a complete security program from the ground up is not feasible for most organizations. Hence, implementing a security program requires a phased approach, where the organization's most urgent needs are addressed first. Since the number of vulnerabilities usually exceeds an organization's capacity to implement corrective action, it is essential the organization allocate scarce security resources properly to protect its most valuable assets.

As managers establish and/or assess their organization's security program, they should follow certain fundamental security principles,[6] such as those developed at the National Institute of Standards and Technology (NIST), whose principles include that computer security:

- Should support the mission of the organization
- Is an integral element of sound management
- Should be cost-effective
- Requires explicit responsibilities and accountability
- Requires system owners to have (computer security) responsibilities outside their own organizations
- Requires a comprehensive and integrated approach
- Should be periodically reassessed
- Is constrained by societal factors

8. Intergraph Information Assurance Solutions

Intergraph delivers turnkey services, software, and hardware solutions that address a wide variety of network, system, and security issues. With continual technology changes and marketplace pressure to use the Internet and/or intranets, the design, configuration, and implementation of integrated network systems have become increasingly more difficult. Similarly, systems and data security have become a top priority for customers and IT professionals as they develop and maintain their networking infrastructures. Intergraph provides both commercial and government customers comprehensive IA solutions (firewall, anti-virus, intrusion monitoring, etc.) as an integral part of most projects.

Customers often have difficulty choosing the right technology and services and integrating them within their infrastructure. Too often companies select predefined security packages that do not address their unique situation, needs, and infrastructure. However, Intergraph approaches information assurance from the customer's perspective, creating a solution tailored to their organization. Intergraph views security as a continuous life cycle of process improvements. Rather than taking isolated steps, Intergraph supports an organization's security team in building an integrated, comprehensive process that will increase security both immediately and in the future.

8.1 Risk Review

The objective of a risk assessment is to measure the threats, vulnerabilities, and impacts in a well-defined computing environment. The results are then used to select countermeasures that are both appropriate for protecting the information assets in the system and the employees who must use those assets to meet the business objectives of the firm. In short, security is defined in terms of an organization's specific business environment. Risk assessments are qualitative (considering corporate culture and business needs) and quantitative (ensuring the countermeasure does not cost more than the asset being protected) and comprise five main processes:

Figure 5: *Intergraph Information Assurance Process*

- **Identify key information assets:** Mission-critical data, computer software, and hardware
- **Identify realistic threats:** Determine problems likely to occur, rather than those that could occur and assess organization's position as a possible target for attack. For example, banks and government and military sites are popular targets for hackers.
- **Vulnerability analysis:** Identify weak links in the organization's security program that could be exploited
- **Losses:** Determine the consequences of both tangible (losses that have financial impact) and intangible losses (reputation is harmed, the organization is in an industry where there is great customer sensitivity to security incidents)

8.2 Policy

An organization's security policy reflects the results of the risk assessment. Establishing a computer security policy is the cornerstone of a company's security program and reflects trade-offs between business requirements, such as competing via the Internet, and the need for security. Without written policy, it is difficult to implement a comprehensive security program. Computer security policy describes the following:

- What an organization wishes to protect
- Who may access what information
- What is permitted and prohibited
- Responsibilities of senior management, middle management, information systems staff, and end-users
- Minimum security standards for all information systems and more stringent standards for systems that contain company proprietary data

Every business has policies, procedures, standards, and government mandates that address a range of security issues. Intergraph helps customers review these documents, eliminate redundancy, and identify requirements for physical security, acceptable Internet use, messaging, network tools, computer viruses, and other areas. Intergraph helps customers define prevention, monitoring, and reaction procedures, and plan policy education. By assigning responsibilities, organizations can ensure all their policies and standards are appropriately incorporated and enforced. Through continual review, they can simplify the dynamic policy development process.

With the appropriate policies in place, an ongoing evaluation of security effectiveness becomes an objective, quantifiable process. Intergraph measures actual system security against the criteria established by the policies. Until an organization establishes a corporate information security policy, it is not addressing information assurance and company actions against security incidents remain reactive, rather than preventive.

8.3 Implementation

Selecting technology tools is no easy task given the breadth of products available and the evolving capabilities needed to keep up with changes in network speed and technologies. With broad experience in an array of multiplatform products and systems, Intergraph can help organizations evaluate available technologies, from databases, servers, and network devices to intrusion detection

systems, Internet scanners, and firewalls to Internet, virus detection, or other software. Intergraph can integrate and implement the infrastructure needed to meet precise security needs.

An important step in implementing an IA program is to create a local response team that can deal firsthand with systems security issues and coordinate with regional or divisional organizations. Intergraph has extensive experience in establishing a response team capability, with a specific knowledge of how to approach network/system intrusion response. Intergraph also supports the implementation of management, response, mitigation, and reporting processes. Intergraph helps customers develop monitoring functions and implement daily, weekly, monthly, and quarterly tasks, as well as supporting metrics – all while balancing operational and security needs within realistic budgetary constraints.

8.4 Administration

Once security procedures are in place, Intergraph can support daily onsite administration to minimize risk. Using proven systems engineering methodology, Intergraph helps manage the security process, objectively review results, and update procedures and policies. Intergraph conducts training to educate users about acceptable use, introduce new procedures and policies, and increase security awareness.

Intergraph can also assist IA officers in enforcing procedures, conducting incident investigations, and preparing reports for upper management. If an incident occurs, Intergraph helps minimize the impact of service disruption and information theft or loss for quick recovery. Responding systematically with an Intergraph solution, customers can dramatically reduce the risk of recurrence.

8.5 Audit

The audit phase serves to verify the effectiveness of the security employed. Unfortunately, many organizations fail to follow a continuous improvement and monitoring path after establishing their security programs. Since threats, vulnerabilities, security technologies, and business needs all change on a regular basis, the need to regularly audit the security program is critical. That is why Intergraph helps with assessing the vulnerability of a system through intense penetration testing using the latest hacking methods. Intergraph participates in certification testing of all information systems due for accreditation or re-accreditation. Intergraph also helps establish accreditation criteria and evaluation/certification processes, and maintain a database of accreditation status and schedules.

9. Conclusion

While there are serious risks associated with operating in a globally connected world, an effective IA solution can mitigate these risks. Using proper security solutions, an organization can develop a sound strategy to thrive in today's electronic business world. As an expectation of shareholders and a necessity for IS personnel, senior managers should play a major role in developing and supporting their organization's security program. Through comprehensive, tailored IA solutions, Intergraph can create the security plans organizations need to be successful.

10. Footnotes

1) “The 2000 Information Security Industry Survey,” *Information Security*, September 2000

2) Machefsky, Ira. “Fifth Annual Security Survey,” *Information Week*, September 8, 1997

3) Computer Industry Almanac Inc.

4) epaynews.com

5) “2005 Computer Crime and Security Survey,” Computer Security Institute

6) Buttman, Barbara. et al, An Introduction to Computer Security: The NIST Handbook, October, 1995

11. Appendix A: Organizational Security Assessment

The following assessment provides questions managers should use to assess their security status. As management reads through each question, they should use the Typical Answers and Rating columns as a guide to determine their security status. Using the information provided, respond to each question and rate your answer according to the template provided, where "+" signifies a good rating, "0" signifies an average rating, and "–" signifies a poor rating.

Questions	Typical Answers	Rating
1.What corporate information and information systems are considered mission-critical? How is it currently protected? Who has access to it? [These crucial questions identify what must be protected and the value of assets – the greater the value, the greater the need to protect].	This has been determined via a formal risk assessment process. We can make well-informed guesses to answer these questions. We're not sure, we've never attempted to answer these questions.	+ 0 –
2. What would be the impact (financial, competitive, public relations) if this information were compromised?	This has been determined via a formal risk assessment process. We can make well-informed guesses to answer these questions. We're not sure; we've never attempted to answer these questions.	+ 0 –
3. What were the results of our most recent security audit? Have we ever had an external audit?	We have had a comprehensive audit within the last 12 months and are implementing its recommendations. We have had a comprehensive audit within the last three years. We have never had a comprehensive audit.	+ 0 –
4. Do we have a written corporate security policy?	We have written, up-to-date policy, which is the basis for our security planning. We have written policy, but do not heavily rely on it. We have no written policy.	+ 0 –
5. How much time per week does our IS staff spend on security? What is our level of security expertise?	We have dedicated resources for IS support that are adequate to meet the objectives specified in our security policy. We do dedicate some resources to security, but they are not adequate to meet our stated objectives. We do work on security matters when time permits, but have no dedicated security resources.	+ 0 –
6. How confident are we in the security countermeasures we currently have in	Because we conduct vulnerability assessments regularly, we are reasonably confident in our security posture.	+

place? What are we less confident about?	We are reasonably confident in our security posture, but don't regularly test to confirm this. We know our security posture can be improved because we have not devoted the time and resources to this need.	0 –
7. What computer incidents have we had over the past year? Did internal or external parties cause them?	We have had both internal and external incidents, but we quickly detected them and have since corrected the vulnerabilities that caused them. We have had both internal and external incidents and are working to correct the corresponding vulnerabilities. We have discovered incidents and are concerned about undetected ones.	+ 0 –
8. What security awareness training do we conduct?	We have a formal program with training scheduled for the next 12 months. We have some irregularly held training. We have no training program.	+ 0 –
9. Do we have a business continuity (disaster recovery) plan?	We have a written plan and countermeasures that we regularly test. We have some written procedures and countermeasures in place. We have no plan.	+ 0 –
10. What computer virus protection have we implemented? Have we had recent problems with viruses?	We have a formal virus protection plan and countermeasures in place that has been very effective. We have virus protection countermeasures in place, but not a formal plan. We have some virus protection countermeasures in place, but viruses are still a problem for us.	+ 0 –

Headquarters
Intergraph Corporation
170 Graphics Drive
Madison, AL 35758

For more information about Information Assurance, visit our Web site at www.intergraph.com/sgi.

 DDFS011A0