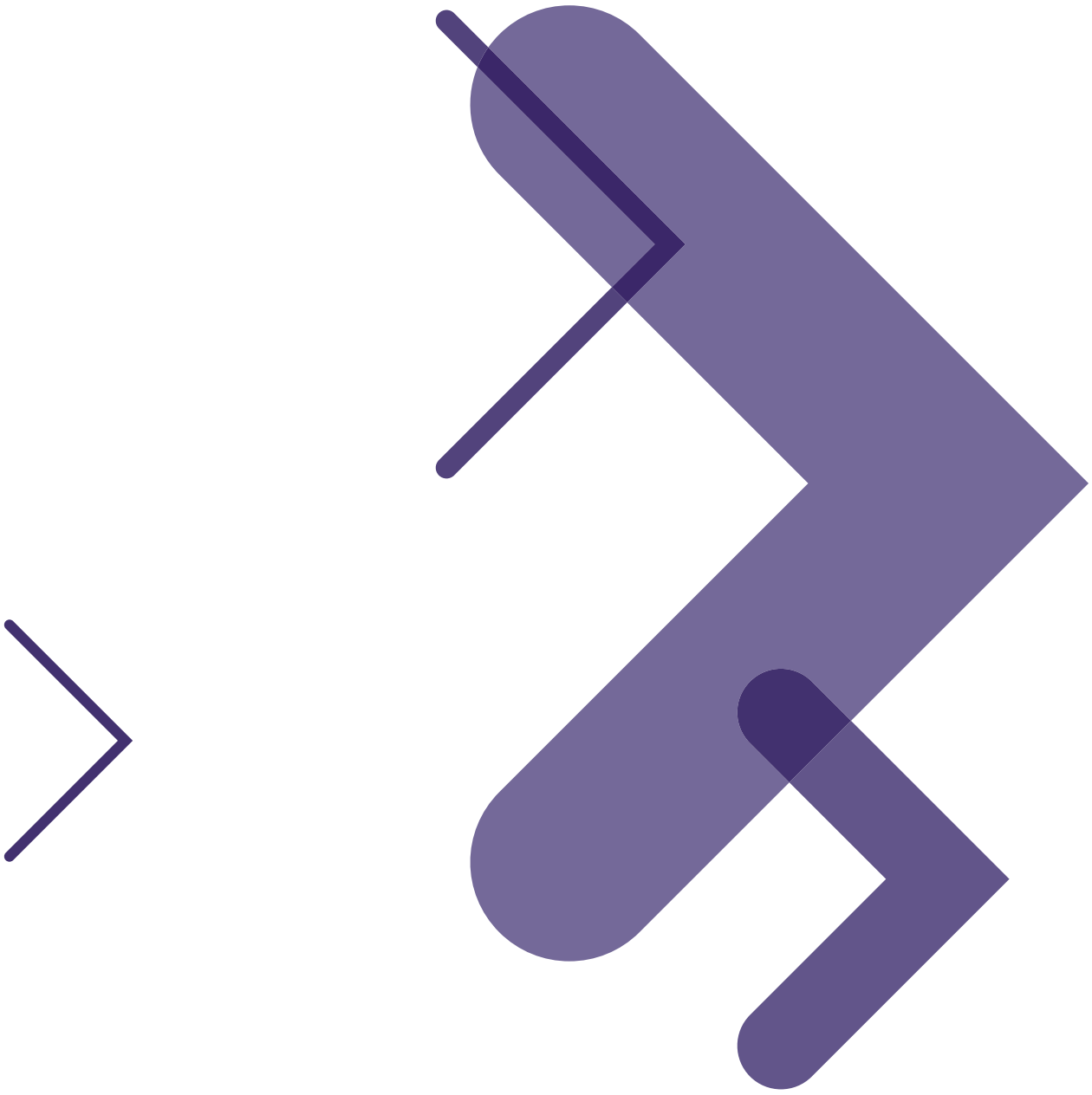
WHITE PAPER

Information Assurance for Private Radio Networks

Information Assurance (IA) secures IP infrastructure and protects radio network assets ensuring operational continuity.



Executive Summary

According to current risk management and security thinking, an Information Assurance (IA) program can ensure the security and resiliency of the IP infrastructure that supports Land Mobile Radio (LMR) operations. For federal agencies, Department of Defense (DoD) enterprises, and state, county or city governments that need secure and compliant networks, Information Assurance offers the following benefits:

- Integration of all the internal departments and disciplines that contribute to a layered defense-in-depth security posture (e.g., risk management, IT operations, information security, physical security, business continuity, business intelligence and human resources)
- Use of advanced risk management metrics to cost-effectively apply just the right amount of security to each information asset
- Integration of all locally relevant regulations, standards, best practices and compliance mandates (e.g., FISMA/FIPS, NIST, DITSCAP, DIACAP, ISO)
- Creation of policies, procedures, processes and security architecture that are needed for rapid certification and accreditation

Traditionally, security has been viewed as a costly and operationally impractical activity that ties the hands of IT users and process owners. Security improves considerably with the use of IA methods that allow security teams to build high levels of operational flexibility and resilience into enterprise sys tems. As a key enabler of IP infrastructure and broad systems interoperability, IA can play a critical, integrative role in an enterprise's planning and decision-making activities, as illustrated in Figure 1.

GLOSSARY OF TERMS

DIACAP: Department of Defense Information Assurance Certification and Accreditation Process

DISA: Defense Information Systems Agency

DITSCAP: Department of Defense Information Technology Security Certification and Accreditation Process

FIPS: Federal Information Processing Standards

FISMA: Federal Information Security Mandate Act

HIPAA: Health Insurance Portability and Accountability Act

ISO: International Organization for Standardization

ITU: International Telecommunication Union

NIST: National Institute of Standards and Technology

NSA: National Security Agency

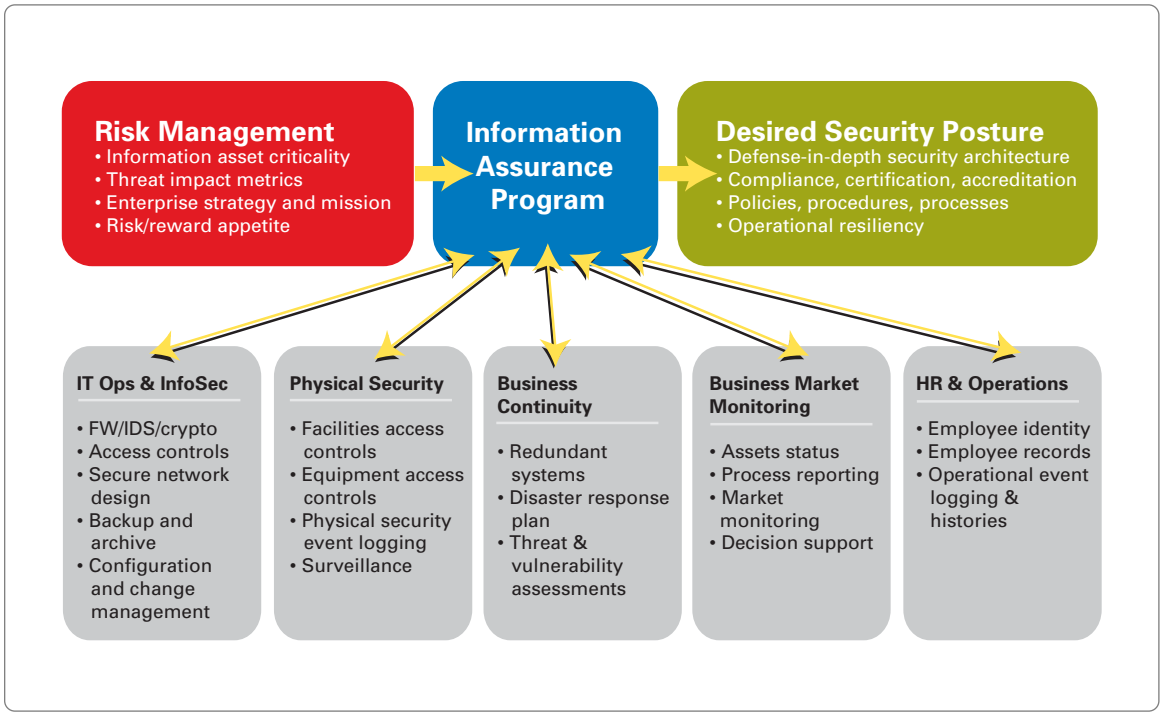


Figure 1. The IA decision-making process and related enterprise impact

Introduction

With the ongoing adoption of IP networking and open IT platforms for critical infrastructure, LMR system managers have had to shift their focus from managing over-the-air technologies toward managing wireline and IT technologies, which comprise an increasing presence in radio network architectures. Moving to IP-based platforms delivers many benefits, such as enabling client-server architectures, creating more flexible interconnectivity, allowing use of IT-based applications and greater scalability. For mission-critical group voice services, Multicast IP allows optimization at the protocol level for the real-time voice performance that is necessary to fulfill the most essential missions. Using an IP-based architecture also provides a long-term foundation for a vast array of current and future messaging, data application, geo-location, multimedia, video, data exchange and interoperable voice communication solutions.

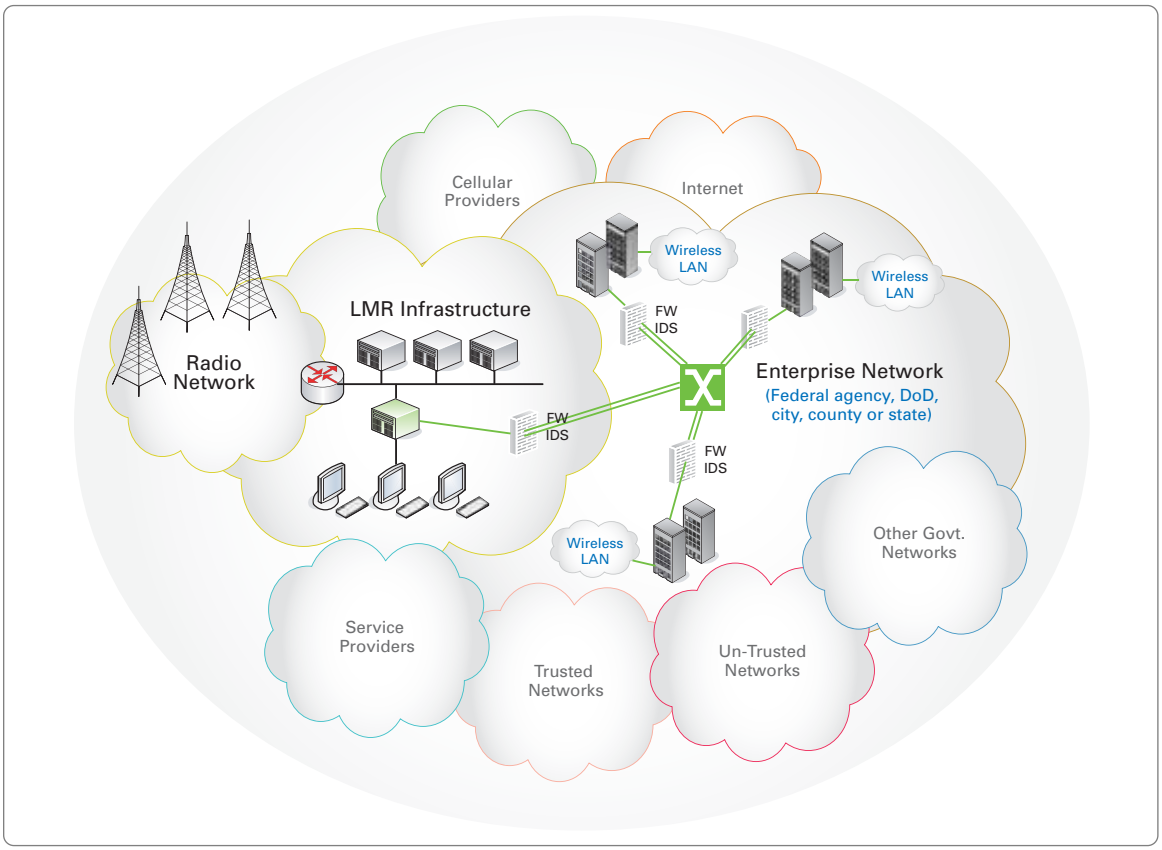


Figure 2. IP infrastructure for LMR and enterprise networks

Asymmetric Threats: A Game Without Rules

"The difficulty is that in the real world, we have people that do not play by the rules. What we are trying to defend has now evolved from a border or theater of operations, which we can array forces around, into a much more ambiguous world of asymmetric warfare. There are people and groups pursuing complex ends inside your perimeter that you do not fully understand and cannot attack with overwhelming force without destroying yourself."

– Richard A. DeMillo, Dean, College of Computing, Georgia Tech University; former CTO, Hewlett-Packard

Asymmetric Threats

The benefits of IP networks are well known, but the openness of IP protocols, platforms and services introduces significant new vulnerabilities into LMR operations and critical infrastructure environments. The rise of IP has coincided with the explosive growth of asymmetrical threats that do not necessarily conform to traditional security and risk management approaches. Traditional threat models were symmetrical, with combatants aligned against each other along a well-defined border or perimeter. But today, the perimeters in physical and cyber warfare are rapidly dissolving under pressure from the dual forces of evolving global sociopolitical threats and highly distributed enterprise computing models.

Asymmetric threats don't conform to clear-cut borders and perimeters, which means they:

- Exist inside and outside the organizational defense perimeter
- Use sophisticated automation to attack up and down the technology stack
- Deploy blended attacks that move freely between physical and cyber assets
- Cascade through networked systems and critical infrastructure
- Exploit human engineering and insider participation

Although traditional circuit-switched LMR networks rely heavily on proprietary implementations, this creates a natural barrier against hackers, viruses and malicious attacks. In contrast, the new IP-based LMR models, while providing many additional benefits, also expose well-known protocols, services and interfaces at many different levels of the network and IT infrastructure—creating a wealth of vulnerabilities.

Given the range and seriousness of the asymmetric threats that IP infrastructure and open platforms bring, there are some who would prefer to turn back the clock to a simpler time when isolated, proprietary networks were the norm. But given the benefits and momentum of IP technologies and standards-based IT, most LMR shops are becoming full partners in IP-based enterprise computing. Fortunately, it is possible to have great IP cost/performance and great security too.

Enter IA, which represents much of the latest thinking and best practices for controlling the vulnerabilities that are targeted by asymmetric threats.

Threats + Vulnerabilities = Risk

The above-mentioned threat vectors would be relatively harmless if it weren't for significant human and technology vulnerabilities that exist in IT-dependent organizations. When senior security engineers conduct security audits of commercial and government IT infrastructure, in most cases,

Department of Veterans Affairs
August 3, 2006
A laptop stolen from an employee's home contained personal information for 26.5 million veterans, including billing records, Social Security numbers, birth dates and addresses. The employee violated local policy by taking information home.

Records containing sensitive personal information involved in security breaches from January 2005 to date: 153,558,451

Source:
Privacy Rights Clearinghouse
(www.privacyrights.org)

they find serious vulnerabilities, including:

- Lack of adequate perimeter defenses and traffic controls
- Lack of physical access controls
- Unpatched and misconfigured devices
- Weak or missing passwords
- Inadequate security reporting, scanning and periodic assessments
- Weak antivirus protections against viruses, Trojan Horses, worms and other malware
- Human errors as a result of poor training and professional development
- Data leaks and inadvertent disclosure of information

These human and system vulnerabilities open the door to a wide range of unauthorized access, service disruptions, data leaks and compliance failures. Without a comprehensive IA approach, attackers, terrorists and criminals will become more and more successful.

What Is Information Assurance?

According to wording culled from a wide range of government information protection mandates:

Information Assurance protects and defends information and information systems by ensuring availability, integrity, authentication, confidentiality and non-repudiation. IA must also provide for the restoration of damaged or compromised information systems by incorporating detection, prevention and response capabilities.

Each key term in this definition points to a useful aspect of IA:

- Availability: Timely and reliable access to data and services for authorized users
- Integrity: Protection against unauthorized modification or destruction of information
- Identification and Authentication: A means of identifying users as recognized entities who can be authenticated (password, fingerprint, voiceprint, PIN) to network and systems elements
- Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes or devices
- Non-Repudiation: Senders and recipients are provided with proof of each other's identities so that neither can later deny having been part of the transaction

In a nutshell, IA is a set of policies, procedures and processes that safeguard:

- Data moving on networks
- Data processed by applications
- Data residing on any sort of digital storage medium

Ultimately, to safeguard digital information in all of its various states, IA has to protect data, the IP network, and any related IT infrastructure.

Although typically very data-centric, IA is not confined to computer systems, and is not limited to information in electronic or machine-readable forms. In the broadest sense, IA applies to all important information and data within the enterprise, in whatever form.

By protecting information, data and IT operations within IP infrastructures, IA uniquely supports cost-effective, reliable LMR operations that are potentially highly interoperable with partner agencies and other relevant first-responder teams, municipalities and enterprises.

To safeguard the production, transport and storage of information within the LMR infrastructure, an IA program deploys a number of policies, processes and procedures that guide an organization's security management efforts and many related areas of IT operations. IA programs are effective to the degree that they enable convergence and integration of some key disciplines, including:

- Regulatory and policy compliance
- IT and network security (InfoSec)
- Physical security
- Business continuity and disaster recovery
- Identity and access management
- IT life cycle and project management
- Intelligence gathering and analysis

When deployed as a strategic initiative, IA becomes an important cross-functional platform for the convergence of various governance, policy and operational capabilities that might otherwise be fragmented and isolated.

IA for a Strong Policy Framework

IA can also serve as the foundation for a policy and best practices framework that is very useful in compliance, certification and accreditation efforts. IA policies can be developed internally, but will likely be heavily influenced by some mix of locally relevant regulations and standards (e.g., FISMA/FIPS, NIST 800, DITSCAP, DIACAP, ISO 27000/17799). For organizations operating under federal and DoD security and risk management mandates, IA offers a structured path to an "Authority to Operate" green light.

Operational risk and resiliency

Operational risk is the risk that results from:

- Failed internal processes
- Inadvertent or deliberate actions of people
- Problems with systems and technology
- External events

Operational resiliency is the organization's ability to sustain the mission in the face of these risks.

Source: CERT - Introduction to Resilience Engineering Framework, November 2006

IA serves as a central organizing force that helps navigate a complex mix of regulations, guidelines and standards. In this role, IA manages or contributes to numerous policy, standard and process areas, including:

- Information risk management policy
- Information classification and handling standard
- User access management standard
- Application security standard
- Network and perimeter security standard
- Platform security standard
- Cryptography standard
- Vulnerability management standard
- Change management standard
- Self-assessment process
- Exception management process
- Awareness training

The importance of policy in IP-based IT environments can't be overemphasized. In many organizations, internal employees, partners and outsourcers who are considered "trusted parties" cause the majority of data breaches. Serious data leaks and internal vulnerabilities are often the result of inadvertent lapses on the part of employees and contractors. A recent IDC study[1] found that, along with viruses, spyware and spam, the threat of unintentional leaks is now one of the top five concerns of enterprise security managers. User education—not expensive technology—is often the best defense against threats that are brought into the network or valuable data that is leaked to the outside. Hence, IA emphasizes people, policy, process and procedural security issues.

IA Enables Operational Resiliency

Traditionally, IT security has been viewed as a restrictive, costly practice that delivers lowered performance, user inconvenience and no measurable upside. But security programs that are based on IA principles result in more positive, intelligent, risk-based security models that deliver measurably higher levels of operational resiliency. IA builds organizational value by formalizing risk management in the areas of physical and cyber security, IT operations and key internal processes. Consequently, IA is a unique enabler of operational resiliency—the degree to which an organization can adapt to changing risk environments (internal and external). By combining disciplines like NIST 800 and ISO 27000, IA makes enterprise processes more policy driven and well structured. Operational resilience is critical for large government and military organizations because the stakes are high, given the context of massive public safety programs and widely distributed critical infrastructure.

Operational resilience is also important for small and midsize organizations. Whereas large organizations have deep redundant resources that make them more naturally resilient, smaller organizations have less resources and, hence, a smaller margin of error. An IA-based security and policy architecture can ensure that small and medium-size enterprises remain resilient in spite of limited IT resources, staff and facilities.

The bottom line: By building and preserving operational resilience, IA helps both large and small organizations keep their information flows intact in the face of global, dynamic and complex asymmetrical threats.

IA and Risk Management

IA draws on risk management calculations to determine the value and criticality of information assets. Risk managers are continually balancing cost of impact against cost of mitigation. Similarly, with IA, it is not always economically practical to mitigate all information threats. Without good risk management practices, it is impossible for IA to determine what assets are at risk. In federal, municipal and DoD organizations, both tangible and intangible assets are equally important. Tangible assets include IT equipment, facilities and network connections. Intangible assets include:

- Citizen trust/community support
- Organizational reputation and public image
- Customer retention and customer relations (customers could be citizens, responder agencies, partners, suppliers, international community, funding agencies)
- Confidence in privacy controls
- Citizen and employee morale and productivity

The ability of IA to safeguard trust, confidence and reputation should not be undervalued. Trust is a necessary ingredient of government, national defense and commerce—a trust failure in any of these spheres could result in disaster. Without trust, communications and information have little or no value. At the highest level, IA goes beyond mere operational soundness by safeguarding trust, reputations, relationships, and other related areas of value production.

[1] Burke, B. & Ryan, R. (2007). *Worldwide Information Protection and Control (IPC) 2007-2011 Forecast and Analysis: Securing the World's New Currency,* IDC: Framingham, MA.

High levels of IA can only be achieved with ongoing application of risk metrics. Once an organization's information assets are identified, they are prioritized in relation to the following key criteria:

- Criticality of asset
- Vulnerability of asset
- Likelihood of threat to asset

IA manages risk by minimizing the impact of threats on vulnerable critical information assets. If an information asset is not critical, then its vulnerabilities are less significant. If an asset is critical, but has no threats, then risk is low. At the intersection of all three factors—high criticality, high vulnerability and high threat—the risk is substantial.

Figure 3. High risk at the intersection of criticality, threat and vulnerability

When IA is allowed to apply this process to all of an organization's information assets, the cost effectiveness of security spending increases dramatically.

The rating of information assets is illustrated in Figure 4 using the Mission Assurance Category (MAC) rating system—a DoD convention that is used to rate the criticality of systems and associated data and applications in relation to the organizational mission. The MAC categories are defined as follows:

- Mission Assurance Category I (MAC I): systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness
- Mission Assurance Category II (MAC II): systems handling information that is important to the support of deployed and contingency forces
- Mission Assurance Category III (MAC III): systems handling information that is necessary to conduct day-to-day business, but does not materially affect support of deployed or contingency forces in the short term

The risk evaluations used by IA result in the application of effective security controls (protections) to the IP infrastructure. These controls are matched to the criticality of assets, exploitable vulnerabilities and specific threats. Controls are also matched to

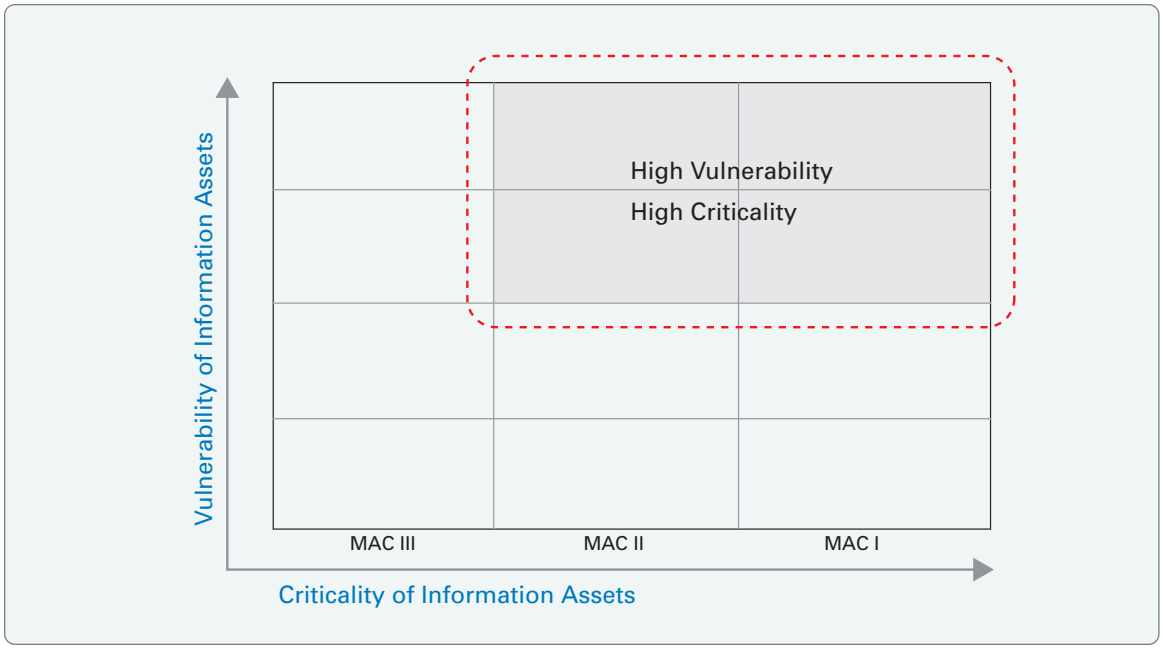


Figure 4. Rating of information assets in terms of mission criticality vs. vulnerability

the resources available to the enterprise. Ideally, IA-directed security controls are deployed in a defense-in-depth security architecture, which is a core set of principles that are deployed in many compliance, standards and best practices frameworks.

Defense-in-Depth Security

Throughout history, as cities and towns grew in wealth, they became the focus of increasingly sophisticated criminal and military attacks. These attacks hastened the development of layered physical defenses on the perimeter of the town (e.g., walls and moats) that became increasingly concentric (e.g., building guards, high fences, locked gates, strongboxes). Today, a fully secure town or business—much like a fortified Medieval village—is protected by many layers of physical security controls inside the perimeter, including manned checkpoints, video cameras, security patrols, electronic locking systems, biometric access controls, vaults and safes.

The layered approach to security that is so prevalent in the physical world is also increasingly relevant in the cyber security realm, whereby asymmetric attacks can be mounted from anywhere inside or outside of the enterprise, at any level of the infrastructure. Today, an attack can originate from an enterprise's own data center or from the laptop PC of a college student who's halfway around the globe.

A layered "defense-in-depth" approach to information security and data protection is often employed by IA programs to create a fabric of interlocking controls that safeguard IP infrastructure against all aspects of the asymmetric challenge.

Defense-in-Depth Defined

Security experts on Carnegie Mellon University's Computer Emergency Response Team (CERT) define defense-in-depth as follows: "The synergistic integration of layered Information Assurance practices, providing resilient IT services while minimizing failures and intrusions." The university, in a report sponsored by the DoD, further defines defense-in-depth as:

> An IA construct in which multiple related organizational actions and controls are applied to minimize failures and intrusions and their propagation. In essence, it is a multi-pronged protection strategy. When defense-in-depth is achieved, reliability and resilience—the ability of IT systems to withstand attacks with minimal impact on services—also are achieved.[2]

Much work has been done to understand what is required of defense-in-depth security for IT infrastructure. Examples of this work are seen in security frameworks, standards and best practices from NIST, ISO, NSA, DISA, ITU, and other bodies that strive to apply sound policies and security controls at multiple points in the technology stack. Employing concentric layers of security around critical information makes it possible to deter or recover effectively from a wide range of threats. Defense-in-depth lets LMR network owners achieve the right balance between the two conflicting needs they face—open interoperability versus secure and resilient operations.

Defense-in-depth methods are developing constantly. The current thinking in the area includes several key recommendations:

- Divide internal enterprise information assets into *security domains*, which reduces the damage that a single breach can incur.
- Build protection controls into all *vertical layers* of the technology stack.
- *Distribute* applications and services to multiple servers, so there is no central point of failure.
- *Create redundancy*, which allows continued operations even if an attack disables part of the infrastructure.
- *Use diversity* to reduce the attack surface and compartmentalize risk.

The Importance of Diversity

Diversity, an important but often overlooked aspect of security, deploys a mix of different operating platforms and protocols that have different security strengths and weaknesses. Too often, enterprises install several critical applications (e-mail, Web and e-commerce services) on one server. All of these applications will be compromised together if the system crashes or is successfully attacked. Using multiple, distributed servers avoids this.

Another aspect of diversity is choice of operating system. If all the servers and workstations in an enterprise are the same version of the same operating system, then they could all succumb to a cascading attack from a single piece of malware or hacker exploit. In contrast, an enterprise with a mix of operating systems and configurations will be less vulnerable. The key is to choose a balance between diversity and consistency, i.e., use configuration management, disk imaging and automated provisioning within each group of similar systems for high levels of configuration standardization.

Note: *Some of the best practices discussed below may not be specifically relevant to all networks and all organizations. For instance, an LMR operations network with very strong firewall and intrusion controls may not need personal firewalls on host computers inside the LMR security domain. The true value of each security control can only be known after*

[2] May, C. et al. (2006). *Defense in Depth: Foundations for Secure and Resilient IT Enterprises* (sponsored by the U.S. Department of Defense). Carnegie Mellon University: Pittsburgh, PA.

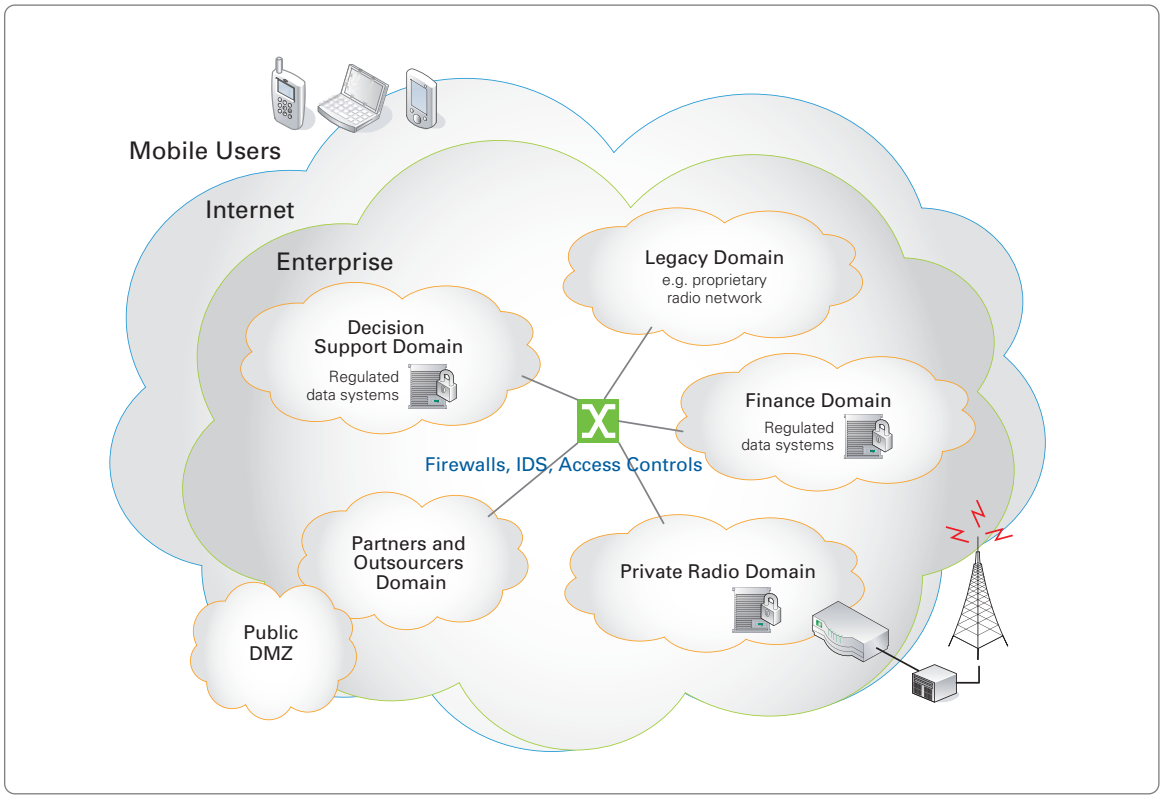


Figure 5. Security domains compartmentalize threats, which can effectively limit and contain the damage associated with any given attack.

a thorough risk assessment process that looks at basic functional requirements for the target network. This assessment process must also balance the risk versus cost of implementing controls. In this context, "cost" can be measured with financial performance, administrative overhead, or other relevant metrics. A good example of a "cost" that is excessive is a banking card PIN with 15 characters. A long ATM card PIN is more secure than the normal four digits, but it is harder to remember. Hence, its cost in terms of support and wasted user time is high. There are, of course, many similar risk/cost trade-offs that must be addressed in the creation of an effective defense-in-depth network security design.

Secure Domains Compartmentalize Threats

A defense-in-depth security architecture can mitigate internal and external threats by dividing the IT infrastructure into domains—each with a unique mix of traffic controls, firewalls, intrusion protection, antivirus services, etc. Domains are created by grouping a concise set of assets (data, users and systems) that are related in a functional, geographical or organizational sense (e.g., part of the same workflow or process). Assets can also be grouped in terms of their value (customer records, financial records, classified documents, etc.). Domains can have their own policies if need be. Ideally, domains are created with risk management methods that start by prioritizing the relative value of assets in relation to the mission of the organization and its compliance requirements. Certain general-purpose office automation assets can go into relatively insecure domains. Systems that contain personal identities, financial information, and other key data assets are grouped in highly secure domains that are protected by strong network traffic management, encryption and access controls.

When an IA program includes a domain approach to security, it facilitates improved compliance with relevant regulations, including the FISMA/NIST standards, DoD certification and accreditation requirements, general financial controls, privacy laws, and related regulations and audit exposure. IA policies and procedures apply to each domain, enforcing compliance by design.

Compared to a monolithic external defense perimeter, domains represent a greatly improved approach to information confidentiality and data integrity, allowing stricter control over the storage and disclosure of sensitive and valuable digital assets. Authentication can be tied to domains in such a way that users can receive different access rights for each domain. The contained scope of domains can facilitate policy approval and enforcement, i.e., it's easier to enact policy in a single domain versus the whole enterprise.

Protecting IP Infrastructure

Today's attackers are looking for vulnerabilities from the top to the bottom of the vertical technology stack, including:

- Attacks on physical facilities and equipment
- Eavesdropping, masquerading and denial of service at the network level
- Corruption and control of applications and operating systems
- Violation of the confidentiality, integrity and availability of user data

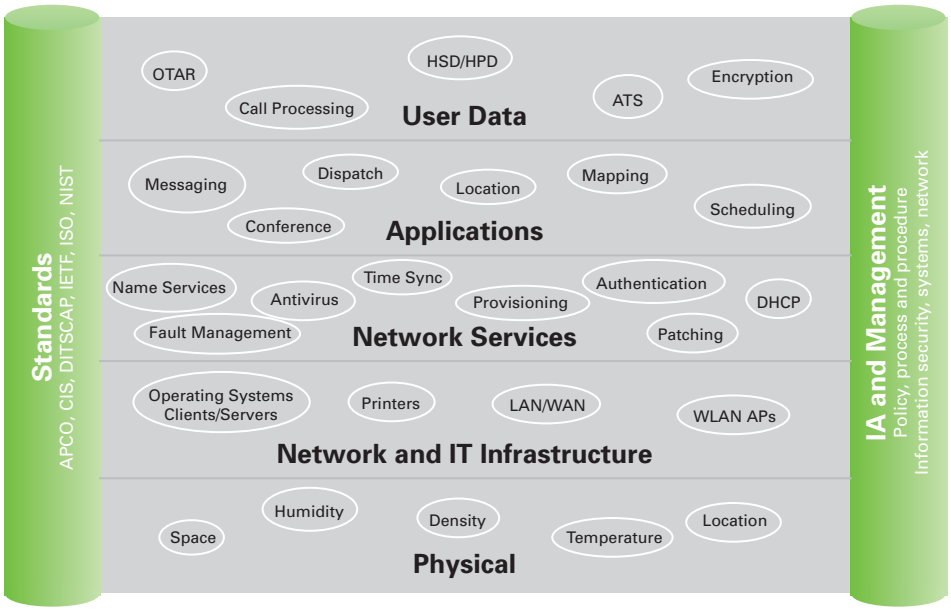


Figure 6. In a defense-in-depth security architecture, IA policies and controls are applied at all levels of the technology stack.

In the LMR environment, user data includes voice call processing, key signaling, and private radio data services, as well as critical dispatch and supporting office automation functions.

Network-Based Controls

Network-based controls provide protection at the perimeter of the network boundary and at the border of any secure domains that are defined within the enterprise. All of the major network protection technologies (DMZ, firewall, IDS) work together to detect and block internal or external network-based attacks. Since IP protocols and services are well known and often "open" by default, it is mandatory to close unnecessary ports on network devices and filter all traffic if vulnerabilities are to be controlled.

Network firewalls use a set of traffic-forwarding rules to determine what data is allowed to pass between networks. In traditional network security, a firewall is only applied to traffic that travels from the outside to the inside of the enterprise network, as in external perimeter defense. But in more advanced defense-in-depth security architectures, firewalls can be deployed inside the enterprise to create security domains, each with its own set of information and IT assets. Some firewalls have the intelligence to protect specific types of assets, such

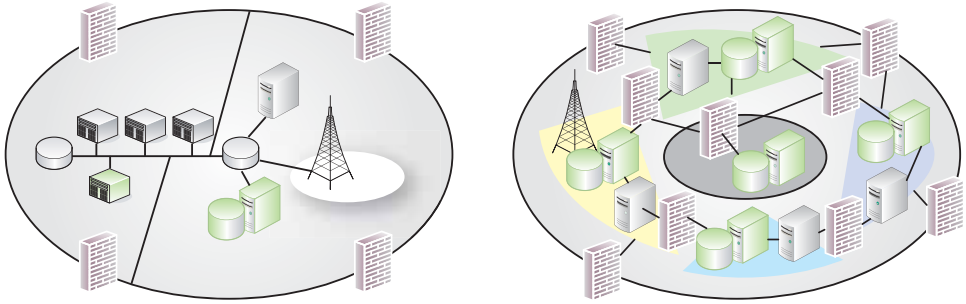


Figure 7. Traditional firewall perimeters are increasingly pierced by connections for remote employees, external partners, outsourcers, customers, and extranet/Internet access. The defense-in-depth solution is created with internal firewalls and a domain-based security architecture.

Open vs. Closed LMR Networks

Even in cases where the LMR operations are run in a closed or "nearly closed" modality, the presence of open platforms, open protocols and IP can still introduce a wide range of vulnerabilities. These weaknesses are based on the types of protocols and platforms residing on the networks—not whether it is nominally open or closed. As senior security engineers know from experience, mission-threatening vulnerabilities are found in nearly every so-called closed network they evaluate.

Consider this "closed network" scenario: A government employee surreptitiously takes a laptop computer home where a child uses it to surf a Web site that automatically installs a Trojan Horse that is part of a "drive-by download" exploit. The next day, the laptop device is taken back to the office and interfaced with "closed" IP infrastructure (through Ethernet, removable storage, USB file transfer, Bluetooth, etc.). As a result, the malware infection is transmitted into the so-called "closed" system.

as messaging servers, mobile application gateways, telecommunications switches and databases. In some cases, a firewall can be placed directly in front of a key server (or built into the server) to enable dedicated protection.

One of the most common vulnerabilities at the network level is lack of traffic controls. In too many cases, IP traffic is allowed to travel unrestricted to any part of the enterprise. This is due, in part, to a tendency to run router and switch devices on a default "permit all" setting. One of the primary goals of a defense-in-depth security approach is to use router access control lists (ACLs), firewall rules, vLANs, and other network traffic filtering and network segmentation methods to ensure that traffic only goes where it is absolutely needed and no further.

Network interface isolation should be conducted on important IT system and network nodes, which means that each network interface is hardened with filters and traffic blocking so that they only talk to specific approved network partners. For instance, the Ethernet interface of a database server could be hardened and isolated so that it is only accessible from downstream application servers and not the general client device population.

Common sense dictates that traffic should be strictly controlled as it enters the enterprise or a secure domain perimeter—referred to as "ingress filtering." Many security experts agree that traffic should be filtered in the outbound direction as well. Egress filtering can make it harder for internal employees to intentionally or accidentally leak sensitive or confidential data to outside parties. Egress filtering also makes it harder for Trojan Horses, worms, rootkits and bots to transmit valuable data, passwords, screenshots and key strokes outside of the enterprise.

Demilitarized Zones (DMZs) are security partitions that serve as a barrier between an internal network and an external network. Public-facing servers and applications can be put in the DMZ to compartmentalize any threats or attacks from external networks. The firewalls and routers that create the DMZ can provide Network Address Translation (NAT) between networks, which means that only the systems in the DMZ have public IP addresses; systems in other areas have private addresses, which aren't easily reachable by external attackers.

Intrusion Detection Systems (IDS) can look at traffic moving into and through the enterprise to scan for unusual or suspicious activity. Whereas antivirus products typically look for known virus and malware signatures, intrusion detection/protection systems can look for anomalous patterns in network traffic and online user behaviors. IDS devices create alarms and block traffic when traffic and usage patterns do not match expected baseline levels. As with firewalls, IDS systems were traditionally used to analyze traffic on major incoming links. More recently, IDS systems have become increasingly specialized and suitable for granular protection activities across the enterprise—in specific domains or in conjunction with specific servers or applications.

Typical threats detected by IDS include:

- Domain Name System (DNS) requests from unauthorized hosts
- Web scripting attacks directed at Web servers
- SQL injection attacks directed at database servers
- Buffer overflow attacks against hosts
- Worm propagation
- Various brute force and Denial of Service attacks that create anomalous network loading and traffic patterns

Securing Insecure Protocols and Services

Many of the most successful attacks on IP infrastructure have focused on well-known protocols and services that have documented vulnerabilities. For instance, attackers have been known to attack DNS servers, which can cause denial of service and serious network traffic disruption. In some cases, Simple Network Management Protocol (SNMP) agents can be exploited to take control of systems. In general, numerous insecure network services come standard with popular clients, servers and operating systems. Some of the most vulnerable services include telnet, rlogin, rsh, ftp, rsync, rcp and tftp. The elimination of insecure network services and protocol usage is necessary to sustain Authority to Operate (ATO) certification for U.S. federal systems and DoD compliance.

Many default insecure services can be replaced by Secure Shell (SSH), an encrypted authentication protocol that supports secure telnet, rlogin, rsh, ftp, rsync, rcp and tftp services. SSH allows secure remote execution, file transfers, strong authentication, and secure client/server communication using AES 128-bit encryption. SSH contributes to the protection of networks from malicious IP spoofing, IP source routing, and DNS spoofing attacks.

Host-Based Controls

Host-based controls are an important aspect of a layered defense-in-depth approach. Host controls protect individual computers on the network from

direct attack. Protection methods for hosts can target the physical aspects of hosts (lockdown), software applications or the operating system. Host-centric security controls include:

- Antivirus software
- Hard disk encryption
- Application data and session encryption
- Operating system hardening
- Configuration management
- Periodic audits
- Host-based firewalls (where applicable)

Host-based (personal) firewalls are typically deployed as operating or application software that filters and blocks incoming and outgoing traffic. Host firewalls are usually configured on a per-application basis, allowing the user or administrator to specify which applications and services gain access to the network. Host-based firewalls are a valuable defense-in-depth tool because they allow a defense perimeter close proximity to the user data.

Although host firewalls can be highly effective, they don't eliminate the need to harden well-known ports and services on each host. One approach to host hardening is to turn off all open services of the operating system and application software until the host is fully secured. Then, network ports and services are progressively unhardened to the point at which the host operates correctly using the most secure possible configuration.

For custom-designed application programs, software engineers should conduct hardening of the codebase, which can greatly reduce vulnerabilities. So-called "design time" and "compile time" hardening involve such strategies as:

- Removing unused/dead code
- Killing temporary memory objects deleted when application exits
- Providing validation of all input data
- Detecting and controlling buffer overflows
- Building in explicit error and fault handling
- Eliminating hard-coded passwords or network addresses in code/memory

Identity and Access Management

To achieve efficient IT and security management, a central identity and authentication authority should uniquely identify each user on the enterprise network. This ensures accountability for actions of all users and strict access control for all information assets. With traditional IT and security systems, identity systems are often fragmented and nonintegrated. The existence of multiple nonintegrated identity and access control systems means extra work, redundant resources, and a lack of global view for access controls and security forensics.

An IA program and regulatory compliance are easier to implement if user IDs are consistent across an entire network. Centralized policies for identity and access management enable this consistency. Identity and access policies ensure that users are uniformly:

- Authorized and trained
- Assigned appropriate rights and privileges
- Verified as current employees or contractors

Poor password management is one of the most prevalent recurring vulnerabilities in IP infrastructure. Weak passwords are often guessed by human attackers and easily broken by automated brute force password hacking programs. Good password management practices include using strong alphanumeric phrases and changing passwords at regular intervals.

A number of commercial operating and network software vendors offer role-based user access controls that greatly streamline and organize the identity/access challenge. In the role-based approach, administrators define standard roles based on common application usage and workflow activities within the enterprise. Each role is given a set of baseline access rights to applications and data. When a new user is added to the system, the user is given an enterprise-wide identity, which is mapped to one or more access roles. When the user is removed from the system, a single identity instance is deleted, which eliminates the common problem of too many different logins and identities on different systems throughout the enterprise. Considering that IA is a policy-oriented approach to security, centralized identity and access controls are an invaluable means of policy enforcement.

Audit and Event Management

All of the hosts, network devices and identity/access systems in an enterprise are potentially capable of generating and logging event data. Event logging and reporting are important aspects of compliance, audits and security forensics. Without logging, determining the origin of a threat and what damage occurred is difficult or impossible. IA operational policy can define a standard set of events for all key devices on the

network. Collected events are stored on a central server that is available to compliance, audit and forensic activities. Network administrators can conduct regular log reviews that look for unusual or suspicious activity. After an attack occurs, logs are reviewed for forensics to determine the nature and source of the attack.

Cryptography

Given the open and well-known nature of IP infrastructure, the trend toward data encryption is increasing. Modern cryptographic methods are highly effective, particularly the latest AES 256-bit encryption, which is extremely difficult to crack, even for the typical blackhat or criminal. Encryption can be applied at many points in the defense-in-depth security architecture, including the network level, the host level and the application level.

At the network level, encryption of traffic between routers and between major sites can be accomplished with virtual private networks (VPNs) and related IPsec encryption and authentication services. Network layer encryption typically protects traffic from the user's computer to a security gateway in an enterprise data center (e.g., remote VPN access). VPN encryption can also be applied between two remote enterprise sites (e.g., LAN-to-LAN VPN).

At the host level, SSH and related encrypted session-level utilities can be used to protect end-to-end traffic between two hosts. A range of products is emerging on the market to meet host-to-host encryption needs, which are getting more visibility as enterprise perimeters decline in effectiveness.

At the application level, traffic can be encrypted between application cryptography that is built into the application itself. Pretty Good Privacy (PGP) encryption of e-mail and office documents provides examples of this. In some cases, databases have the ability to encrypt individual records or a range of records.

Disaster Recovery and Business Continuity

Traditionally, IT organizations addressed security, data backup and business continuity as separate issues. But with the converged IA approach to security, these areas now require some coordination, at least at the policy level.

For instance, business continuity planning addresses continuity needs in the event of a disaster. Planners are adept at balancing business restoration needs with investment in technology and resources. These are important functions. As such, the definition of what constitutes a disaster now must include the information protection issues that the IA team assesses. Consequently, there may well be a need for the IA team to have direct input into the disaster recovery and continuity plan. For example, if a specific server or dataset is particularly vulnerable, then the IA team can point this out, and the business continuity planners can build more redundancy and failsafe capabilities into this area of the infrastructure.

Likewise, the IA team should have input into the IT operations policy for central backup and archiving. With the help of IA, the backup and archive administrator will have a better understanding of the relative vulnerability of internal systems and applications. IA participation allows the operations staff to more effectively back up volatile, non-derivative data to a central server using appropriate backup intervals. This approach enables more reliable recovery of data in the event of a failure.

Central provisioning is a related capability that can greatly speed the resilience of IT operations. Central provisioning of IT elements as well as O/S configurations and patches from a central location allow IT administrators to rebuild the IT infrastructure rapidly in the case of failures and disruptions due to cyber or physical attacks.

In all backup, recovery and disaster planning exercises, IA can play a key role in defining:

- Information assets that need protection
- Vulnerability of assets
- Compliance and regulatory requirements
- Expected threats and business impacts

Life Cycle and Configuration Management

Baseline configuration management is the process of applying a consistent set of configurations across a population of systems and applications. To control vulnerabilities, commercial off-the-shelf operating system and application configurations should be managed throughout the system deployment, runtime and replacement phases of their life cycles. Hackers exploit vulnerabilities soon after disclosure. Out-of-date software versions and slow patching are prime contributors to IP infrastructure vulnerabilities. With configuration management and patch automation tools, updates, bug fixes and remediations can be applied quickly to a large population of systems. Configuration management tools and standard configurations enable greater security through consistency and efficiency. Configuration management can help enforce consistent IA policies to ensure that:

- Windows machines have the correct service pack installed
- Linux machines have a specific kernel running
- Security patches are up to date
- Hosts have a personal firewall installed
- Host antivirus signatures are up to date
- Hosts are hardened and configured correctly

Often, vulnerability is introduced if a large number of hosts have the same configuration and the same operating system. In this scenario, an attacker can discover a vulnerability and exploit it across all systems. While this is true to some extent, the absence of common/standard configurations also decreases the likelihood of remediating vulnerabilities effectively, which increases the overall risk of the network. The key is to create some diversity of configurations and then standardize as much as possible within each group of similar machines and applications.

Vulnerability Scanning and Security Audits

An ever-increasing number of security products target network vulnerabilities, including IDS, IPS, firewalls, antivirus, VPN appliances and proxy servers. Although keeping up with security technologies is important, experienced security professionals know that technology alone does not solve all IP infrastructure security challenges. People and processes cause the majority of security incidents, not technologies. The policies and procedures enforced by a good IA program go a long way toward eliminating the human factors of security. But there will always be lapses. Periodic vulnerability assessments are one way to reduce the impact of policy violations and human error.

Automated vulnerability scanning can be conducted from within the enterprise and/or by an outside service residing in a remote Security Operations Center (SOC). Modern vulnerability scanners use automation to non-intrusively probe every network and host device within the IP infrastructure—searching for open ports and services, and installed malware. Vulnerability scanners can even check for patch levels and configuration mistakes so that the IT staff can shut down weaknesses before the attackers find them.

Automated vulnerability scanning is an important part of IA, but some vulnerabilities can only be unearthed by a thorough hands-on security audit conducted by senior security engineers. An onsite security audit focuses specifically on network and human touch points, policies and procedures, allowing security experts to "think ahead" of malicious attackers and potentially damaging threats. Security auditors can check on compliance issues and conduct "what if" war games that anticipate the future exploits of blackhats, criminals and extremists.

People and Process Issues

To be highly effective, an IA program must implement numerous process and policy improvements, many of which affect the human aspect of IT operations and workflows. Given the increasing trend of human-engineered attacks, user training has become a primary and critical means of defense. If users are educated about the nature of phishing threats, infected Web sites, Trojan Horses, and various identity-based exploits, then the IP infrastructure will be much more secure. Training programs should include:

- Daily computer operations user training
- Advanced security practices for administrators
- Secure coding training for developers
- Risk management for managers and executives

Situational awareness training ensures that users and managers are aware of threats to physical facilities, equipment, and all kinds of information assets.

Cross-training security and operations staff helps achieve synergy among different disciplines. If the InfoSec staff is trained on physical protection systems (i.e., facilities access controls and video surveillance), then security practices and forensics may synergistically cross the physical and cyber realms (e.g., physical and cyber event logging and monitoring combine to create a much clearer picture of blended exploits and attacks).

Another area of people and process improvement relates to remediation and incidence response planning. In our current security climate, attacks strike with little or no warning, making it necessary to plan ahead. When a significant threat or anomaly is detected, incidence response must quickly escalate the event so that it becomes visible to security specialists with the appropriate remediation skills. With planned and tested remediation/response procedures in place, threats will not have a tendency to cascade through the infrastructure and cause huge amounts of damage before they are controlled. Given this challenge, it is beneficial if the IA program drives strong training, planning and incident response capabilities.

Strategic and Operational Benefits

The traditional model for enterprise security is fragmented, whereby diverse security activities are conducted in an uncoordinated way by InfoSec, PhySec, IT Ops, Human Resources, Business Continuity and Risk Management teams. Security in this outdated model tends to be reactive, costly, tactical, and either too much or too little. In the new

IA security model, all stakeholders and specialists work together in a synergistic way that uses risk management metrics to apply the right level of protection controls to each information asset and each IT resource. Ideally, IA is a strategic endeavor that creates policies with the support of an organization's senior executives and managers. When adequately supported, IA becomes a source of operational resilience that allows an organization to fulfill its mission in a sustained and economical manner.

Information Assurance for Government and Department of Defense Networks

Information Assurance is a powerful strategic and operational tool for all kinds of private and public sector organizations. The following sections discuss key implementation and compliance issues for federal, state, local and DoD organizations, including:

- Federal certification and accreditation
- Information classification and handling
- FISMA, NIST 800, DITSCAP/DIACAP
- IA for city, state and local governments

Strong Security Is Now Standard Operating Procedure

The U.S. Federal Government and military branches now require compliance to security standards for all operational networks. Consequently, IP network infrastructure that supports LMR operations must comply with FISMA/NIST or DISA standards and receive certification.

A well-designed Information Assurance (IA) program defines the policies, processes and procedures that greatly facilitate federal information security compliance and DoD accreditation and certification. Compliance involves complex arrangements of people, process and technology. IA is a powerful platform for addressing compliance requirements because it drives integrative, cross-discipline planning and coordination between security, operations, risk, continuity and enterprise process owners. An IA policy framework mediates planning and operations at the intersection of:

- Strategic enterprise goals and mandates
- Applicable security regulations (FISMA, DITSCAP, DIACAP, HIPAA, etc.)
- Applicable standards and best practices (NIST, NSA, ISO, etc.)
- Internal risk management metrics

Since IA is based on risk metrics, federal, municipal and military entities are motivated to identify all information assets that need protection and assign vulnerabilities and threats to those assets. Once

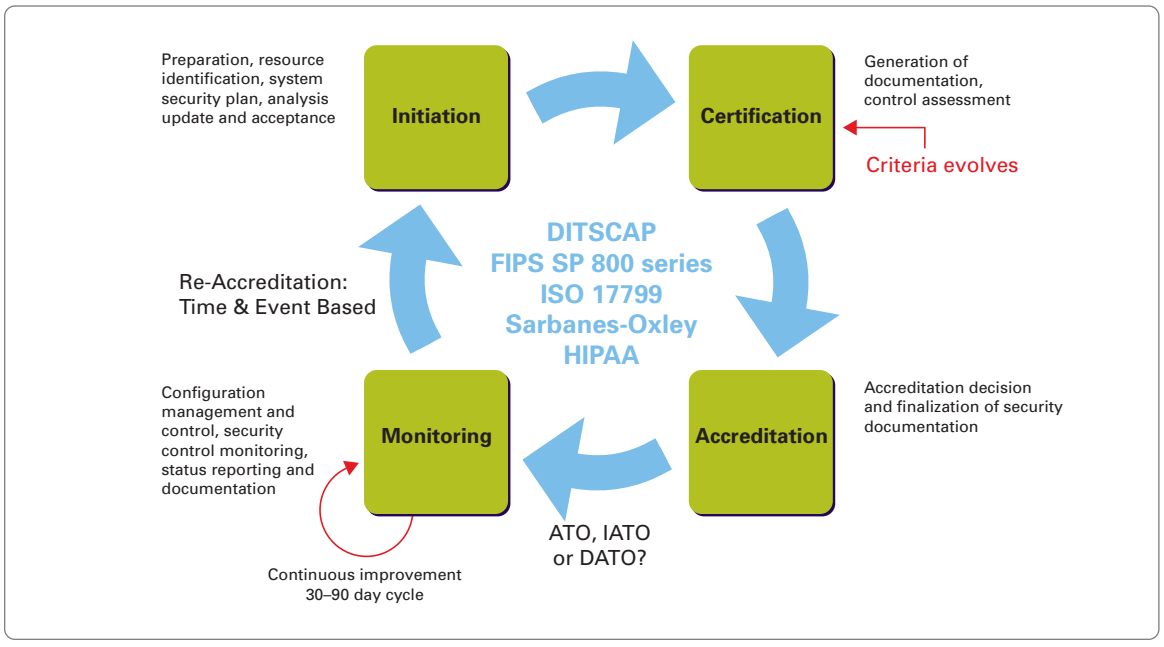


Figure 8. Certification and accreditation are part of a cyclical process that is greatly facilitated by a comprehensive IA program and related defense-in-depth protection methods.

assets, vulnerability and threats are understood, it is much easier to apply federally mandated security controls. The IA approach avoids the too-common "Band-Aid" syndrome, whereby compliance is superficially applied for appearances without any real improvement in security posture or operational resilience.

Compliance is, of course, not a one-shot effort. The security landscape is always changing and evolving, which means there must be ongoing improvements and management adjustments that ensure future compliance, certification and accreditation.

Information Classification and Handling

All federal and DoD information system environments are required to apply security classifications and related handling procedures to all internal information and data. As part of the process of identifying and prioritizing assets, an IA program is the ideal mechanism for creating:

- Definition of classification/handling roles
- Information ownership role
- System custodian role
- Classification levels
- Marking requirements
- Standards for printed and electronic forms
- Storage requirements for each classification level

The precise approach to classification and handling varies from enterprise to enterprise, depending on the type of data and threats that are present. In general, IA addresses classification and handling compliance requirements as a byproduct of information asset evaluation and vulnerability management activities.

FISMA

The Federal Information Security Management Act (FISMA) requires that federal agencies implement an information security program to protect information and information systems that are critical to agency operations and assets, including information assets provided by other agencies, contractors or outsourcers. FISMA mandates security controls based on National Institute of Standards and Technology (NIST) standards (see below). As can be seen from FISMA mission statements, the language and intent of FISMA are remarkably similar to IA concepts discussed throughout this paper. The goal in the case of both FISMA and IA is to protect the confidentiality, integrity and availability of agency information and data, wherever it may be.

NIST 800

The National Institute of Standards and Technology (NIST) publishes Federal Information Processing Standards (FIPS) that are useful to enterprises engaged in IA programs. FISMA requires compliance with NIST-defined security and risk management practices. Many defense-in-depth and integrative security best practices are aggregated in FIPS 199: Standards for Security Categorization of Federal Information and Information Systems. FIPS gives federal agencies and other regulated enterprises a baseline for security controls and risk management. Of particular interest for organizations complying with FISMA and FIPS 199 is the so-called "NIST 800 series" standards, which are highly relevant to the creation of IA policies, processes and procedures:

- SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model
- HSP 800-26 Security Self-Assessment Guide for IT Systems
- HSP 800-30 Risk Management Guide for Information Systems
- HSP 800-33 Underlying Technical Models for Information Technology Security
- HSP 800-50 Building an IT Security Awareness and Training Program
- HSP 800-53 Recommended Security Controls for Federal Information Systems
- HSP 800-55 Security Metrics Guide for IT Systems
- HSP 800-66 Introductory Resource Guide for Implementing the HIPAA Security

DITSCAP/DIACAP

Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and the more recent Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) specification are standard DoD-wide definitions of target processes, activities, general tasks and management structures that are required for certification and accreditation of DoD information systems that operate within the Defense information infrastructure.

IA concepts are prominently embedded in DoD information security mandates. As in the discussions throughout this paper, the goal of DITSCAP/DIACAP is to ensure that IT infrastructure meets and

sustains DoD availability, confidentiality and integrity requirements, and to ensure the infrastructure does not present additional risks to connected systems. To accomplish these goals, DITSCAP/DIACAP certified agencies must be able to:

- Identify all risks and vulnerabilities within the information system boundary
- Ensure that effective mitigations and compensating controls are in place to minimize risk presented by ongoing system operation
- Ensure that the system is secure from threats that could allow unauthorized access to information and cause disruption or denial of service

Information Assurance for City, State and Local Governments

State, local and city government entities have a mandate to protect and defend mission-critical IP infrastructure and private radio networks, and ensure they can fully support public safety and first-responder operations. Security industry accounts and news reports indicate that hackers, criminals and blackhats often have a preference for smaller, less-resourced enterprises, in hopes that it will be easier to find vulnerabilities. In an environment of high threat levels and limited resources, an IA program can provide a uniquely effective and economical path to increased control over IP infrastructure. IA can help ensure that state, municipal and county enterprises maintain confidentiality, integrity and availability of information assets.

For municipalities and other governmental bodies, IA is a fast track to operational resilience and compliance with all locally relevant regulations and legal requirements. Even in the case of limited IT resources, a well-crafted IA program can establish the policies, procedures, processes, internal standards and security controls that are fully compliant and yet fully customized for the enterprise's specific needs.

Motorola ASTRO® 25 Integrated Voice and Data Network

ASTRO 25 Integrated Voice and Data Network is Motorola's advanced digital wireless solution for mission-critical private radio applications and first-responder communications. ASTRO 25 is fully supported by a Motorola services portfolio that delivers optimal solutions in the form of design, integration, and professional security services.

ASTRO 25 Design and Integration

Motorola leverages its global leadership in mission-critical private radio technology to deliver end-to-end network design and integration services that are uniquely able to meet the requirements of LMR applications and supporting IP networks. As a major stakeholder in the public safety and critical infrastructure communities, Motorola design and integration ensure that the level of security protection required by each customer is built into the settings of network and host devices, including:

- Firewalls and intrusion detection that only permit valid, identified radio, dispatch and LMR support traffic
- Demilitarized Zones that create a buffer between enterprise and radio networks
- Antivirus software to prevent infections from malicious code should authentication features be added
- Event Logging to detect events of significance on the network
- Central Authentication to ensure users are uniquely identified and managed
- Encryption solutions at multiple layers within the network
- Operating systems hardened to meet customers needs
- Port Security to ensure only authorized devices are present on the network
- Zone Core Protection that allows the system to have differing trust boundaries

Security Assessment

Motorola offers a team of senior security engineers who have a track record of successful engagements with owners of mission-critical network infrastructure around the globe. The Motorola Security Services (MSS) team designs and implements IA programs and defense-in-depth security architectures that guard ASTRO 25 networks against the full spectrum of threats from government and DoD IP infrastructures. As a cornerstone of the MSS approach, we use a holistic security framework that operationalizes security across the people, process, policy and technology aspects of each organization. MSS can safeguard your organization's entire wireless/wired infrastructure with:

- Onsite security assessments of LMR network and related IP and wireless LAN/WAN infrastructure, including physical network assets and facilities
- Design of defense-in-depth threat protection systems for IP wired and wireless networks

- Interface of ASTRO 25 networks to enterprise IP infrastructure
- Policy design, incident response planning and risk management
- Regulatory compliance strategies

Network Monitoring

Motorola provides ASTRO 25 private radio networks and responder teams with around-the-clock monitoring and incidence response through our Security Operations Center (SOC). Motorola's SOC-based managed security includes a multi-million dollar test facility for pre-testing security updates, configurations and patches. Other key SOC capabilities include:

- 24x7 incident response team
- Senior-level radio, IT and security expertise
- "Push" of pre-tested software updates for A/V and IDS
- Weekly notifications of security updates, or within 24 hours if urgent
- Rapid restore and recover capabilities
- Case management/escalations
- Performance reporting

About Motorola

With 75+ years of experience in the area of critical network infrastructure and public safety, Motorola is a leading provider of interoperable communication systems for first responders, DoD and government agencies. Motorola enables public safety agencies to confidently take the next step in the evolution of mission-critical communications… beyond the basics to technology that is second nature and seamlessly delivers real-time information into the hands of first responders. Motorola is a trusted, long-term partner to public safety agencies, providing the most reliable and innovative wireless solutions that help save lives and protect communities. Our experience along with our skills, people, partnerships and alliances allow us to build innovative, fully integrated technologies that offer the following benefits:

- A communications infrastructure that delivers real-time information to first responders so they can more effectively detect, prevent and respond
- Established track record of delivery, design and implementation of complex infrastructure networks
- Seamless connectivity across multiple mission-critical voice, broadband data and public networks
- A comprehensive suite of public safety applications
- Mission critical-grade, user-specific devices that are rugged, reliable, smart, and ergonomically designed for ease of use.

Motorola understands the mission-critical requirements of your private radio network, and we have the MOTOA4 Mission-Critical Portfolio to move you into the future and support your responder teams with the best-in-class communications tools that they deserve.

Better information. Better decisions.
Better outcomes.

MOTOROLA

Motorola, Inc.
www.motorola.com

0907ASTRO25