Aerospace Industries Association
1000 Wilson Boulevard, Suite 1700
Arlington, VA 22209-3928
703-358-1000
www.aia-aerospace.org

A SPECIAL REPORT

Disruptive Information Technologies

Cloud Computing

Social Networking

Consumerization

Leveraging the benefits, Avoiding the pitfalls

September 2010

Disruptive Information Technologies

Cloud Computing

Social Networking

Consumerization

Leveraging the benefits,

Avoiding the pitfalls

September 2010

Developed by:

E-Business Steering Group

AIA
AEROSPACE INDUSTRIES
ASSOCIATION

Important Disclaimer*: The Aerospace Industries Association of America, Inc. ("AIA") has no intellectual property or other interest in this document. By developing this document and making it freely available to anyone, AIA assumes no responsibility for this use-case scenario's content or use, and disclaims any potential liability associated therewith.*

EXECUTIVE SUMMARY

Background

The traditional information technology (IT) environment in companies of all sizes often comprises a controlled set of selected hardware, software and services to deliver integration and economies of scale. Flexible links between companies are achieved through either individually tailored solutions or flexible standards-based interfaces. These services may be outsourced to third-party providers. This model is challenged by a range of new technologies, characterized by the availability of cheap, powerful consumer devices; virtualization of storage and processors; and Internet connectivity.

During the Fourth Annual Aerospace Industries Association (AIA) Information Leadership Forum in September 2009, a number of new technologies were identified as "disruptive," since they are not currently addressed with industry-wide standards and procedures, and they have the potential to radically alter the way that e-business is undertaken at all levels in the supply network:

- Cloud computing
- Social networking as a corporate collaboration tool
- Consumerization, including the use of personal mobile devices

The nature of the aerospace and defense business makes the industry one of the most severe test cases for the effective deployment of such technologies, since it needs to support requirements for export control, intellectual property rights (IPR) protection and national security.

This report is an initial statement of the likely impact of these technologies and the business, technical, cultural, operational and security implications for our industry. The key characteristics of each technology are described in the following sections along with the claimed benefits, risks and mitigations. Each section provides recommendations to help companies exploit the technologies and proposes supporting actions where it is appropriate for the AIA to act on behalf of the industry.

The Technologies

Cloud Computing

Cloud computing offers flexible access to computing resources, providing both efficiencies and challenges to the aerospace industry where proprietary information not only is business critical but also can be a national security risk if exposed inappropriately.

Cloud computing services may be implemented at several levels of openness:

- Private – within a company firewall
- Community – restricted to a group of organizations
- Public – open to all

The cloud approach presents specific issues related to security, availability and interoperability of the services, which can be mitigated through appropriate action. The current U.S. government focus on cloud initiatives means that industry needs to take a position on the use of such services.

Social Networking

The social networking phenomenon has been established as a new way to communicate across the enterprise and to support enterprise-wide project collaboration. It is the method of choice for the new generation of engineers that we seek to attract into the industry, who are used to open services such as Facebook and more professional networks like LinkedIn. Most social networking services operate in the cloud environment, and the associated risks and mitigations increase as the services become more open. The use of in-house systems similar to those available to the public, such as Facebook, also poses a risk even though they are behind the firewall. Protecting proprietary information that is available to all staff is problematic and should be supported by industry standard security protocols and procedures.

Consumerization

The "consumerization" of IT is the ubiquitous use of external mobile personal devices and applications in the workplace. Several scenarios are addressed:

- Employees using personal devices for both business and private purposes;
- Influences of consumer devices on business computing; and
- External synthesis of data collected from consumer devices such as location and preferences, leading to unsolicited invasions of privacy.

Consumer-based technologies can be used to complement traditional enterprise software to provide value in the workplace. The use of these devices must be supported by appropriate policies and procedures that are broadly applicable across the aerospace industry organizations and the supply network.

Conclusions and Recommendations

The reports conclude that there are business advantages to utilizing these new technologies, provided that appropriate precautions are taken to mitigate the risks. Few of these risks are new, or specific to the technologies, but the capabilities of the new technologies exacerbate those risks. The proposed mitigations should be based on the assessment of the corresponding risks within individual organizations.

It is recommended that AIA should:

- Place the AIA Electronic Enterprise Integration Committee in charge of tracking and adopting (as necessary) cloud computing standards to ensure that they are compatible with and can be used to support the aerospace and defense industry. This should include issues of security, availability and interoperability within and between cloud service providers.

- Advocate with policymakers to ensure that consistent cloud standards are applied across different departments and agencies to facilitate the necessary connectivity to cloud services.
- Press for consistent international cloud service standards for the aerospace and defense industry.
- Consider the business case for establishing an aerospace and defense community environment using an external cloud service provider.
- Generate templates for the policies and codes of conduct to be applied for private, community and public social networking services based on best practices. Encourage member companies to contribute examples of suitable policies and codes.
- Consider the establishment of a secure industry social networking service to support smaller companies in the supply chain.
- Advise member companies keep personal and business devices separate at present.
- Advise member companies to determine how to incorporate the devices and applications they would like to use into their collection of vetted and approved IT equipment.
- Publish best practice guidelines on risk assessment and operation for these technologies.
- Develop template collaborative partner security agreements.

It is fundamental that the industry recognizes that the use of these technologies does not remove its responsibility for understanding their impact including the business, technical, cultural, operational and security implications for our industry.

TABLE OF CONTENTS

CLOUD COMPUTING

Introduction

Cloud computing is being heavily promoted as a disruptive IT model for delivering greater benefit to organizations that require flexibility and agility in their IT provision. Outsourcing the provision of infrastructure, computing power and software with access via a network presents opportunities to drive down costs by paying for these capabilities and services only as required by the business, sharing them with other users and providing open access. With these benefits come a number of potential risks arising from security, availability and interoperability considerations. These opportunities and risks are not new, as they apply to any form of shared computing resource such as virtualization and even mainframes, but the ways in which the cloud can be used throws them into sharper relief. In addition, the requirements of the aerospace and defense industry demand particular care, since proprietary information not only is business critical but also can be a national security risk if exposed inappropriately.

The U.S. Government is seeking to make major use of cloud technology in delivering and consuming its services, which will inevitably affect the aerospace and defense supply chain and its contracts.

Industry considers that the technology is at the peak of the hype cycle, and the AIA eBusiness Steering Group is seeking to provide some authoritative guidance through the currently available definitions, jargon, conferences, webinars and service offerings.

This section introduces the key characteristics of cloud computing, the industrial benefits of the technology, and the risks and mitigations that large and small organizations must recognize as they consider how to exploit the technology. The section also highlights the key requirements for aerospace and defense companies in using the cloud, and recommends specific actions that the AIA can take to facilitate exploitation of the cloud by its members.

What Is Cloud Computing?

Introduction to Cloud Computing Architecture

It is an understatement to say that there is no concise, agreed-upon definition of cloud computing. In its broadest sense, cloud computing refers to any IT service accessed via a network. Typically, this is the public Internet, hence the “cloud” label comes from the symbol usually used to represent the Internet.

Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and other devices on demand, like the electricity grid.

Cloud computing is also an architectural style that leverages key technologies, such as virtualization and service-oriented architecture, in order to sustain the business model of the cloud service providers. It is possible for an organization to design its infrastructure in a similar manner to a cloud service provider and thus provide internal or self-contained cloud services.

While cloud computing emphasizes a new type of development environment and applications, many older Internet-based services also fall under the cloud computing model. As a result, cloud computing can be thought of as a new category of computing services that includes redefinition of existing services and the development of new ones, with the emphasis on the latter. Business process outsourcing often drives the use of clouds.

The National Institute of Standards and Technology (NIST) describes cloud computing as an evolution with three phases. The first, built around networking, leveraged the TCP/IP-based Internet as an abstraction layer providing connectivity between systems supporting these standard network protocols. NIST calls the second phase, built around the World Wide Web and its protocols and display standards, data abstraction or document based. Finally, current and emerging cloud services make the infrastructure more abstract by adding servers and applications to documents and networks.

It is important to remember that with each new development phase, the previous developments have continued to thrive, leading to a situation where nearly every IT resource and function can be supported by a cloud-based computing service.

Characteristics

There are nearly as many lists of cloud computing characteristics as there are definitions of cloud computing. Nevertheless, several key characteristics are responsible for the rapid growth of cloud computing and contribute to its success as a business model for both service providers and service users.

To be considered a cloud service, the service must be accessible via a network, often the Internet. This typically results in requirements for ubiquitous high-speed network access for both the service provider and customer. The network provides an abstraction layer that separates the user from the provider. From a technical (but not regulatory) perspective, location becomes irrelevant. As long as network access is available at sufficient bandwidth, the provider and user can be situated anywhere. This removes the need for end users to be co-located with the services they are consuming and allows for a flexible worldwide customer base. It also allows the cloud service provider to be flexible in locating the data centers and other resources.

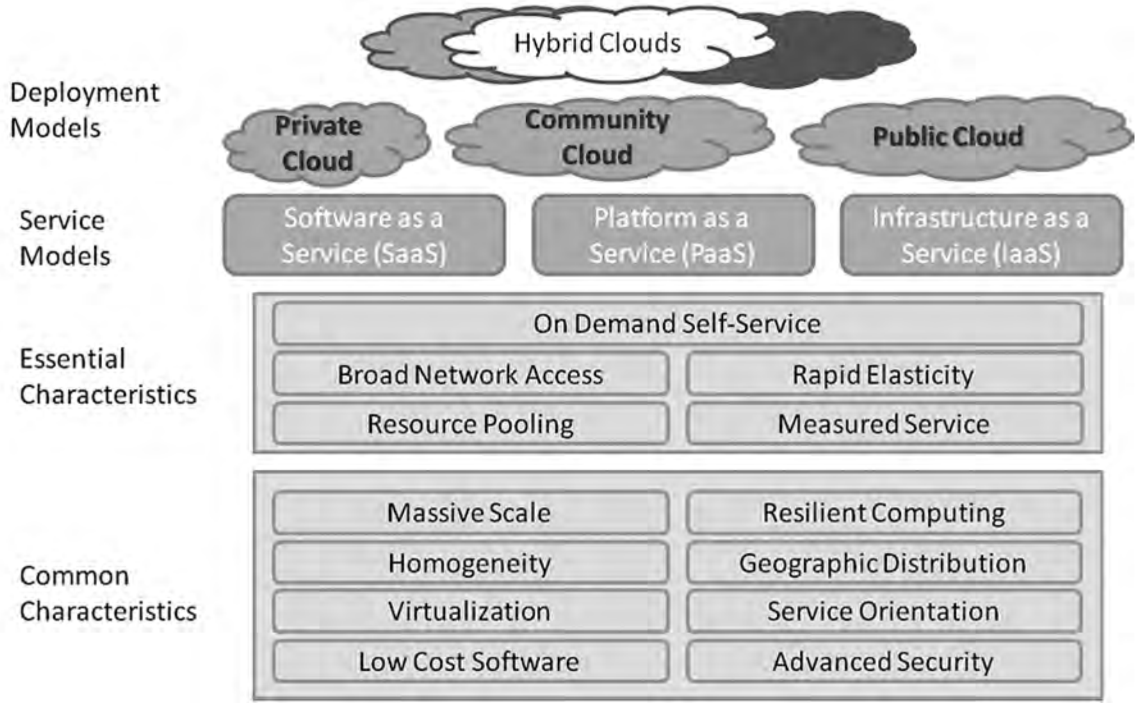
A second characteristic, more common to the newer cloud-based services, is the incremental usage of these services. Users typically do not own any of the infrastructure; they pay only for the computer unit and any application resources they need. Cloud service providers are free to allocate these resources according to demand, which supports a dynamic model for the end users and is especially attractive when they have periods of idleness and periods of high use. The challenge to the service provider is to have enough customers with different business cycles so that its resources are constantly in use and sufficient capacity to cope with the peaks in demand. This capability is marketed with terms such as “on-demand computing,” “pay as you go” or “measured service.” It provides both the supplier and customer with flexibility and more manageable cost models. It can also be implemented internally using private resources, provided that they are organized properly. This dynamic allocation of resources differentiates the cloud from traditional outsourcing services.

Another major difference, related to the one just described, is the service user’s shift from a cost model that includes hardware, software, development and support staff to one that mostly consists of development staff. The service provider is typically responsible for patching software, replacing defective hardware and performing other maintenance operations, freeing the user to focus on application development.

Types of Cloud Services

One of the significant deployment shifts in using cloud services of any type is location. While companies may have outsourced some services in the past, cloud services are much more location-flexible. NIST has defined three types of deployment models, and the Jericho Forum and Cloud Security Alliance have also described cloud characteristics along axes of ownership, physical location, interoperability and isolation—or how "siloed" the implementations are.

Figure 1: The NIST Cloud Definition Framework



Source: National Institute of Standards and Technology

The NIST model describes a private cloud as one that is either owned outright by an enterprise or leased for its exclusive use. A public cloud is one that is sold as a service to any customer or user. Corporations using a public cloud are just purchasing a service and typically are one of many thousands of customers. A community cloud, which is a combination of the two, is one that is supplied by a third party to a limited set of customers or specific community; an example is the "Oregon Health Care Community."

The private cloud service user has complete awareness of the users within its service, whether they are internal users or possible business partners. Members of a community cloud have limited awareness of other users or are conscious only of the types of organizations using the common cloud services. With public cloud services, users have no control over and—potentially more important—no awareness of the other users or their activities.

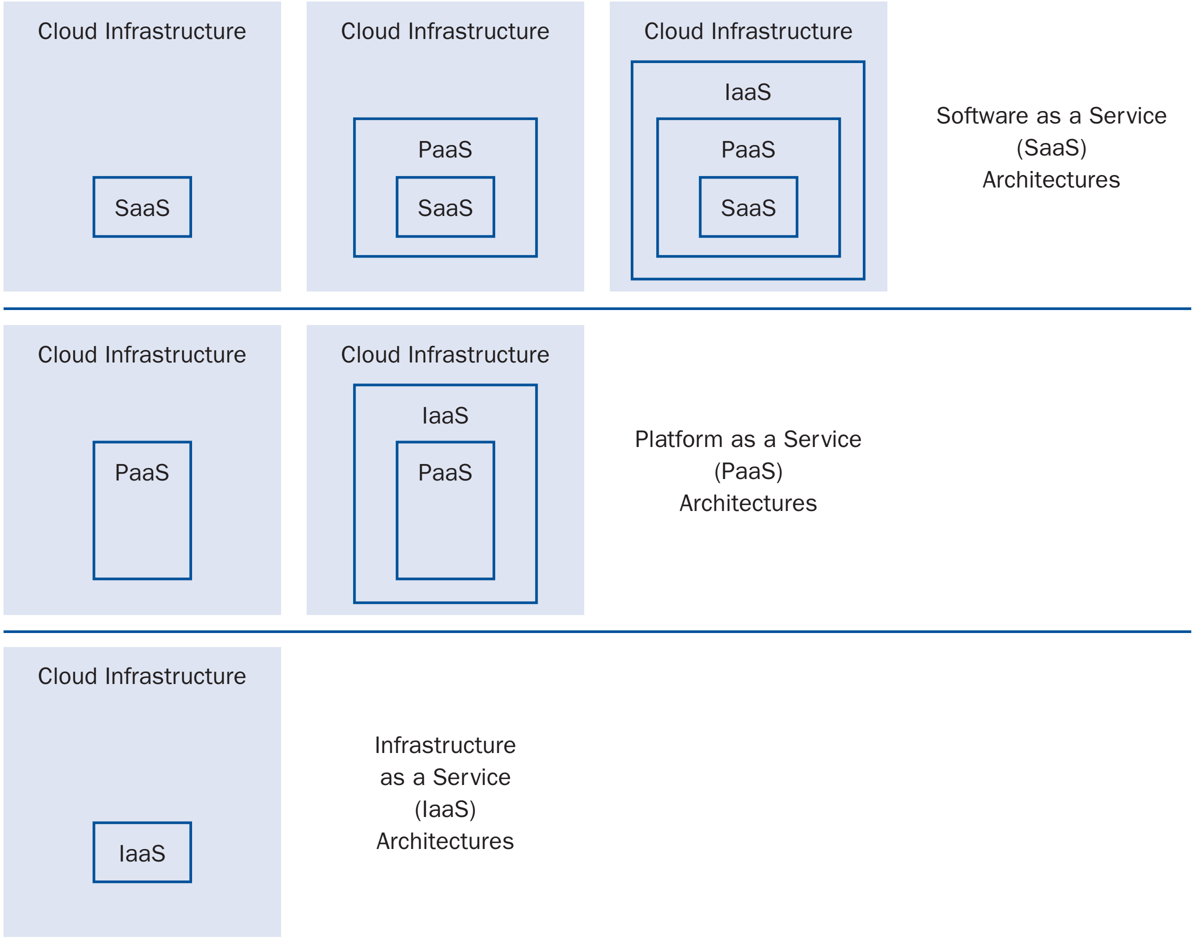
NIST also defines a hybrid cloud as a composition of two or more clouds, each of which could belong to any of the three types described above. These clouds, while still distinct, are connected by technology or standards that allow for applications and information to move between them, a technique sometimes called cloud bursting.

Cloud Service Layers

Cloud service providers offer a number of different services. These can be grouped into layers and are typically shown on a continuum beginning with the simplest services and working up to more complicated services. Three of these services are strongly associated with the newer cloud services:

1. Infrastructure as a Service (IaaS) – This service encompasses the fundamental building blocks of IT such as network, storage and computer processors. The IaaS provider sells the user a set of components that the user can use to construct desirable IT capability.

Figure 2: Service Model Architectures



Source: National Institute of Standards and Technology

2. Platform as a Service (PaaS) – This service is a development layer that consists of a set of interfaces, libraries, programming tools and support for the programming languages themselves. It allows a customer to build applications using these tools and then run them in the cloud environment.

3. Software as a Service (SaaS) – This service consists of applications provided by the cloud service that the user can run over the network interface. The user has little control over these applications beyond moving data into and out of them.

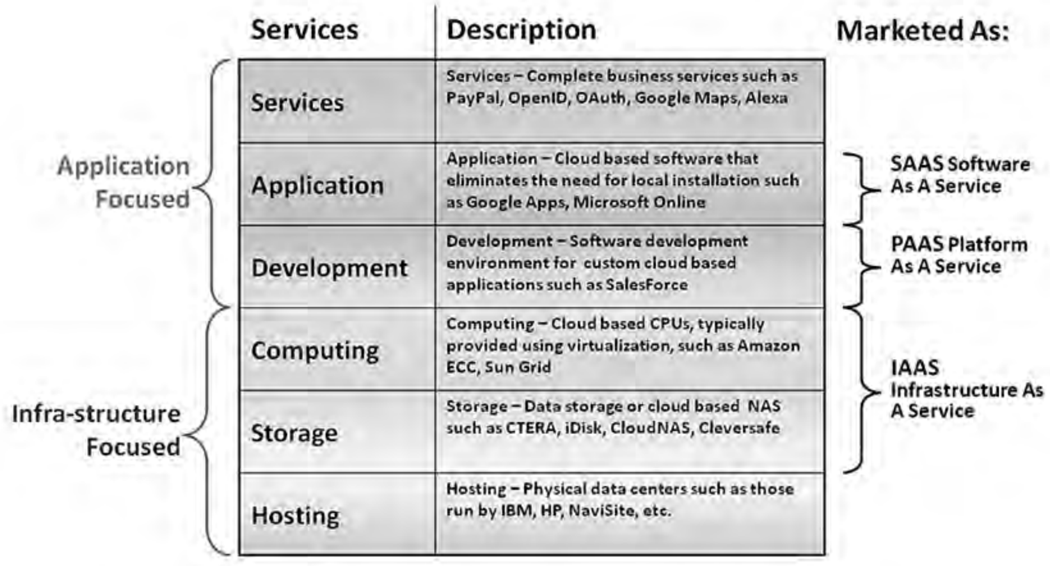
A cloud service provider may sell one or more of the layers. It is common for a provider to supply SaaS architecture along with a PaaS development environment to allow user-developed applications to move from the PaaS development layer to an operational software service after development is complete.

Various industry organizations and individuals have developed models describing these layers. Nearly all models include the layers described above, and may add other layers.

Applications can be grouped together to form more complex services. No one term is used to describe this layer, but the most common one is "Business as a Service." Services at this layer are generally very independent of the customer and operate as turnkey solutions.

Some models also split the IaaS layer, separating the processor from the storage and network. This is because the security model is very different: encryption works well to protect stored information but is not applicable to the use of processor power. Both legacy and new types of cloud storage services are available as well.

Figure 3: Cloud Computing Service Layers

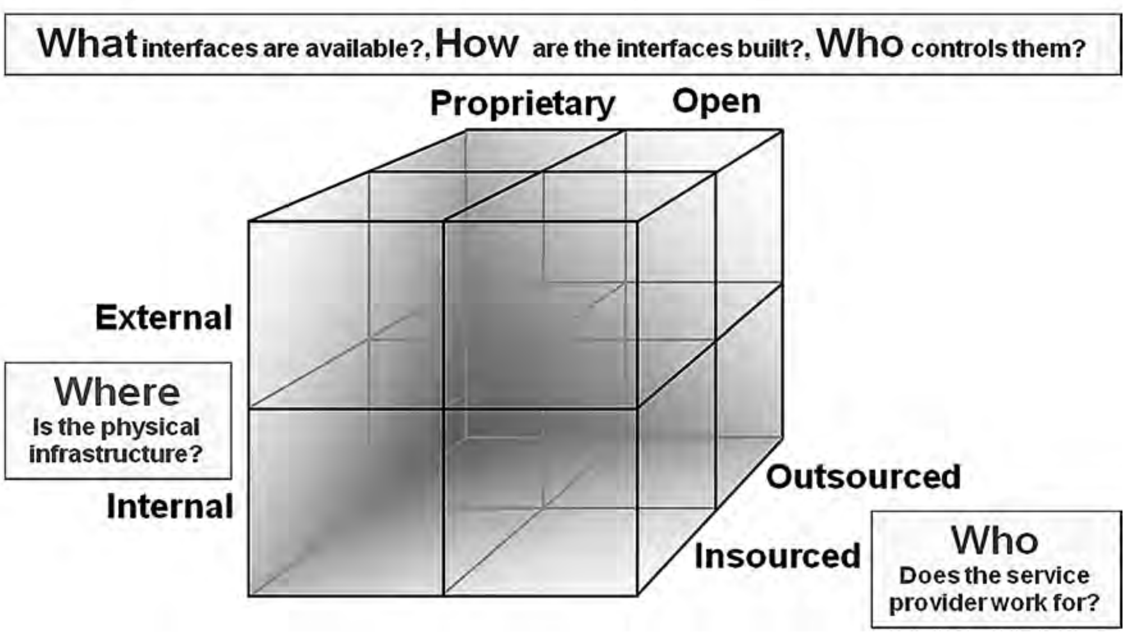


	Services	Description	Marketed As:
Application Focused	Services	Services – Complete business services such as PayPal, OpenID, OAuth, Google Maps, Alexa	
	Application	Application – Cloud based software that eliminates the need for local installation such as Google Apps, Microsoft Online	SAAS Software As A Service
	Development	Development – Software development environment for custom cloud based applications such as SalesForce	PAAS Platform As A Service
Infra-structure Focused	Computing	Computing – Cloud based CPUs, typically provided using virtualization, such as Amazon ECC, Sun Grid	IAAS Infrastructure As A Service
	Storage	Storage – Data storage or cloud based NAS such as CTERA, iDisk, CloudNAS, Cleversafe	
	Hosting	Hosting – Physical data centers such as those run by IBM, HP, NaviSite, etc.	

Source: The Boeing Company

Cloud Property Model

Figure 4: The Jericho Model


What interfaces are available?, How are the interfaces built?, Who controls them?
Proprietary
Open
External
Where
Is the physical infrastructure?
Internal
Outsourced
Insourced
Who
Does the service provider work for?

Source: National Institute of Standards and Technology

Business Impact of Cloud Technology on the Aerospace and Defense Business

Claimed Benefits

The fundamental nature of cloud computing links the user to supporting IT services over a network. This removes the location constraint on both the user and the service provider, giving increased flexibility for both to exploit low-cost environments.

The consumption of infrastructure, computing power and software licenses on an as-required basis can reduce the overall cost of IT support by eliminating the need for the consuming organization to maintain unused capacity to accommodate peaks. In addition, the consumer can rapidly satisfy requirements for increased capacity, although this approach is of course subject to any overall provider limitations. As a result, the consumer capital outlay is minimized and costs are shifted into the operational environment. The provider has the opportunity to optimize the use of its assets, taking advantage of large-scale commodity computing and reducing liability for the consumer. A further opportunity arises for the provider to integrate different commercial off-the-shelf tools, avoiding the individual interface costs that would be incurred by in-house integration.

The availability of cloud IT services can also allow companies in a supply chain to use them for collaboration, ensuring common software and data storage and eliminating the need for suppliers to invest in tools for a particular contract that will not be utilized full time. This approach can logically be extended into the customer use of common IT services for logistic support, operational feedback and other interactions.

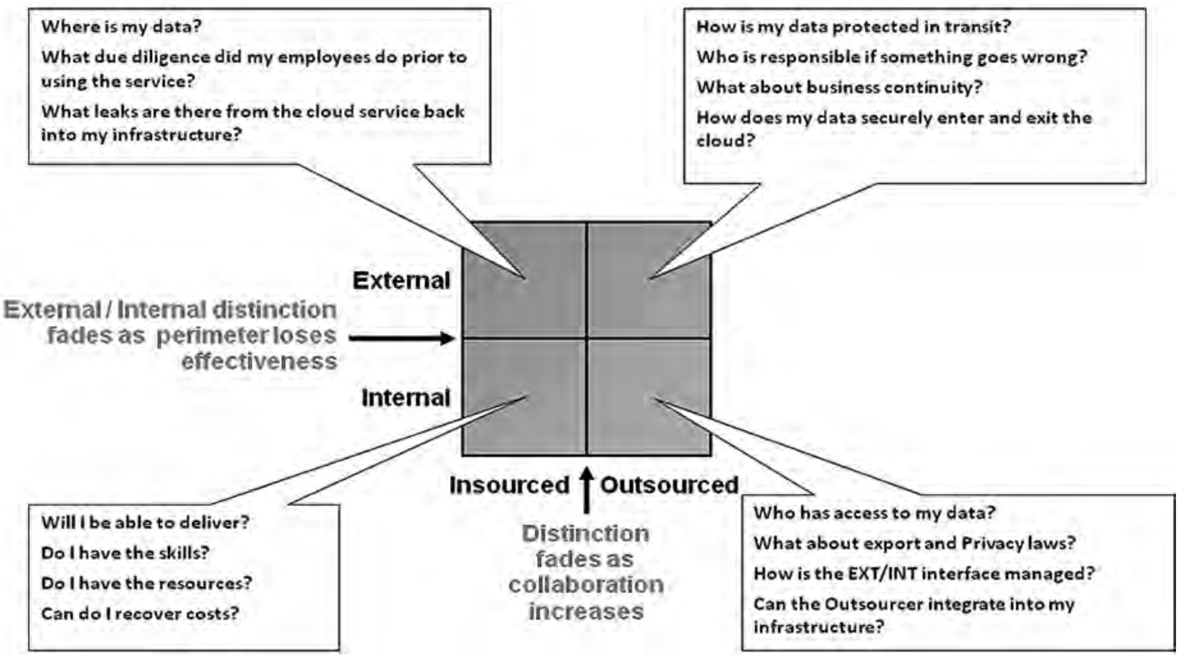
A further consideration is that sharing resources can lead to better utilization of hardware resources such as servers, offering the potential for reduced carbon footprint and emissions as long as loads can be balanced appropriately. Experience has shown that this benefit remains to be proven.

Risks

Security

Cloud computing introduces many questions about "security in the cloud," with solid answers being very dependent on the specific implementation. This section addresses the considerations that must be part of any cloud computing evaluation, but does not attempt to provide answers.

Figure 5: Example Security Questions


Where is my data?
What due diligence did my employees do prior to using the service?
What leaks are there from the cloud service back into my infrastructure?
How is my data protected in transit?
Who is responsible if something goes wrong?
What about business continuity?
How does my data securely enter and exit the cloud?
External
External / Internal distinction fades as perimeter loses effectiveness
Internal
Insourced
Outsourced
Distinction fades as collaboration increases
Will I be able to deliver?
Do I have the skills?
Do I have the resources?
Can do I recover costs?
Who has access to my data?
What about export and Privacy laws?
How is the EXT/INT interface managed?
Can the Outsourcer integrate into my infrastructure?

Source: The Boeing Company

- How does the data get to and from cloud services?
  - This question relates specifically to protecting sensitive information in transit to or from the cloud service. If the service is hosted internally on a corporate network then in most cases it will have the same protections as other internal local, metropolitan or wide area network links. However, if the service is outsourced to a third-party supplier, then consideration must be given to protecting the information in transit via encryption or other methods.
- How is the information protected while "in the cloud"?
  - This consideration also varies depending on whether the cloud is internal or external, but to a lesser degree. Measures need to be in place to allow proper, authenticated access only to specific data being hosted in the cloud and to prevent unauthorized modification of the data. While these are important questions regardless of where the cloud is hosted, the answers may be easier to manage and influence if an internal IT organization is responsible for the implementation. Other access-related questions include how the access is authenticated, how the access decisions are made and how the access is being audited. Authentication can range from a simple user name and password all the way up to public key infrastructure hardware tokens. The bottom line is that the data must be protected from access by those without proper authentication, regardless of where the data is in the cloud and where the cloud is located.
- What separation exists between customers at the application, operating system and disk levels?
  - Depending on the sensitivity of the data in question, logical and physical separation of data in the cloud may be desirable but will come at a price. These separations will defeat some of the positive aspects of the shared resources of cloud computing, but may be necessary and negotiable depending on the situation. At a minimum, it would be optimal to understand what customer separation exists in the cloud infrastructure, if any.
  - Cloud and virtualized servers do not offer the same degree of separation that can be established through physical means.
- What are the regulatory requirements for data protection?
  - Various regulatory requirements protect intellectual property, privacy-protected, export control and national security data. Is the cloud provider well versed in the necessary protections for these types of data, and does their cloud infrastructure support the protections?
  - The service provider must also have the necessary credentials to see data stored on the cloud. For example, the provider must have appropriate credentials for handling classified or International Traffic in Arms Regulations-restricted data.
- Are there unique aerospace and defense industry requirements?
  - The aerospace and defense industry has many unique concerns and requirements that a cloud services vendor will not typically see with other customers, such as concerns related to International Traffic in Arms Regulations/Export Administration Regulations, increased

sensitivity to security concerns, supply chain sensitivities and in some cases the need to separate unclassified and classified information. The service provider must also have the necessary credentials to see data stored on the cloud.

- What are the problems of data spills?
  - Data spills, such as classified data leaking to unclassified systems, present unique challenges in present-day network storage systems such as large Network Attached Storage and Storage Area Network systems. Loss of availability of data to other shared users can be an issue if the systems must be taken offline for cleanup. If cleanup involves the entire storage system, cleanup time can be extensive. The complexity of these issues can multiply exponentially in a cloud environment.
- Can forensic analysis and incident response be conducted in the cloud?
  - Forensic analysis and incident response present unique challenges in a large, distributed, international enterprise environment. Trying to forensically image a multi-terabyte virtualized storage environment or search for malware when the same system is compromised is technically challenging and requires special expertise. Moving this same environment into a cloud infrastructure introduces additional technical challenges.
- What is the audit capability of cloud computing?
  - There is a need to track users and audit access, including machine tracking of utilization and resource cost accounting against contracts.

Service Interruption Risks

While any set of IT services can suffer from outages or loss of availability, cloud-based services have some characteristics that can amplify these risks. This section focuses on the use of public clouds as an example of the worst case. Community and private clouds have the same risks to a lesser degree, depending on their architecture.

Cloud services, by definition, require an Internet connection. Severing that connection shuts down the service. Cloud-based services often also replace traditional IT services that used applications and hardware owned by the users. Moving those to a cloud service creates an additional layer of separation and the end user is less aware of maintenance and other operational issues. Normally, this separation is one of the benefits of cloud computing, but it can also result in less control over routine activities. As more components of the service become external to the user's organization, there is a greater potential for addition points of failure and less opportunity to influence corrective actions.

Leaving out the potential for routine interruptions, there are many ways in which service can be severed without warning. These events can be crudely divided into short-term outages and long-term loss of service.

Short-term Interruptions

Short-term outages typically last from a few hours to one or more days. They can be caused by natural failures or deliberate attacks. Natural failures include both software and hardware incidents. Countering software failures might include rolling back defective patches or adding more virtual machine capacity, while hardware failures would usually be alleviated by troubleshooting and replacing faulty components.

In both cases, the potential for outages is not much different than if the software and hardware were owned by the using organization. The operational differences when using a cloud service are related to the increased isolation between the user and the service provider. If the resources are internal, the user has a much more direct process for escalating repairs or doing what is necessary to bring the service back online. On the other hand, a cloud provider with many customers offline may have a larger inventory of spare resources and may act faster. In this example, the user may have less direct control but a cloud provider may have more resources. The net result is that using a cloud provider is different but not always riskier than running the service internally.

The reliance on the Internet does present an increased risk. If the service is entirely internal and the public Internet goes offline, then the service will likely keep running; this is not the case if the service depends on the Internet. While broad Internet failures have caused hardware or software issues, in general there is enough redundancy in the routing infrastructure, backbone networks and Internet service providers that this is a rare occurrence today. The most likely event is not the loss of the Internet itself but a Denial of Service (DoS) attack against the cloud service provider.

DoS attacks require only a few hundred machines; can be politically, financially, or personally motivated; and are relatively easy to perform. The main risk increase of a DoS attack when using a cloud service is that of targeted attacks where the user becomes collateral damage from an attack intended against one of the other customers of the cloud service provider. The risk of attack increases from those related to the end user's public profile to include all other users of the same cloud service.

Even the largest cloud service providers have had such incidents, and they seem to occur every few months. On the positive side, most of these providers recover within a few hours at most. Given this current risk, applications that require continuous connections to services or data are probably not well suited for cloud services without some way to provide continuity under such a situation.

Long-term Loss of Service

Long-term outages might last weeks, months or even be permanent. Ability to switch to an alternate provider may be exacerbated by the lack of application interoperability standards (see the interoperability section) among cloud service providers. A long-term outage can happen suddenly and for various reasons, such as natural disasters, nefarious activity and e-discovery or law enforcement activity.

In some e-discovery cases, the disks used by the cloud provider were seized by law enforcement because of one customer's malfeasance, with the result that other customers had no access to their data for months. It is common for cloud service providers to store data from multiple customers on the same disk. Customers can therefore lose access to their information even though they are not connected to the alleged activity. A recent case in Texas involved the seizure of a provider's disks as part of an IPR dispute. This action affected more than 50 companies, whose operations were shut down or otherwise disrupted. One of the affected companies filed an appeal to get its data back, and lost. Seizures can take place for a variety of reasons in addition to IPR theft, including classified data spills, presence of files containing child pornography or suspicion of use in terrorist activities. The risk introduced by cloud computing is that of sharing these drives with an unknown set of other organizations and individuals whose actions are outside of the user's control and knowledge.

The other major cause of a long-term service interruption is the demise, merger or other permanent loss of the provider itself. This can happen gradually or without warning. In one example, a major archiving service for professional photographers became insolvent and was acquired by another company. The acquiring company posted a notice giving the photographers and news agencies a week to retrieve their photographs, and then shut down and reformatted the disks. The resulting rush by 30,000 individuals and organizations to retrieve their photographs essentially caused a DoS attack on the service, and very little data were retrieved.

While loss of data can be prevented with good backup solutions, the cloud environment creates a new risk: that of the loss of the IT infrastructure. If a user has built a set of applications using the services of one cloud provider and it shuts down, even if the data is retrieved, there is little chance of these custom applications running on another cloud provider's infrastructure. While there are similar risks in an internal IT organization—software or hardware may become obsolete or unsupported by the vendor—often there is significant lead time and notice from the vendors.

End users typically have access to their own libraries, development tools and Application Programming Interfaces as part of their IT environment, giving them the ability to keep operating after vendor support has ceased. In the cloud environment, all of this is virtual to the user, owned by the cloud service provider and accessed only through the Internet. In a similar situation, the user of a cloud service is at the mercy of whatever legacy services the cloud provider wants to maintain. In a total disruption, as in the case of financial failure or merger, the user may have to rebuild the entire suite of applications using a different cloud provider's development environment.

Interoperability

Developing applications in different cloud environments can fragment business operations and bring the risk of incompatible applications that will not interoperate at either the functional or information levels. Different environments can also drive up the costs for application developers, requiring the maintenance of duplicate expertise in the various APIs.

Changing environments may render software inoperable, since there is no guarantee of interoperability testing. There is also the risk that environments will change at different rates, leading to the need to redevelop interfaces as data formats and applications change in a manner that is beyond the user's control. The use of a single environment or information standards may reduce this risk, but there is no guarantee of interoperability, particularly between software delivered as a service and the results of a development environment.

IPR Ownership: Data and Applications

The use of a cloud environment opens the potential for a user to create a joint work under copyright law, which is a collaboration between two or more authors in which their contributions are joined into a single cohesive work. Each author of a joint work has equal rights to register and enforce the copyright regardless of how their shares in the work are divided. So if the service provider makes a contribution of content in terms of applications software or information, they may have some rights over your data or application.

The openness of the cloud leads to a risk that IPR may be disseminated as the result of a security breach. Clear definition of liability should be established between the user and a provider in the service level agreement (SLA), with appropriate provision for damages.

Risk of the Status Quo Approach

Organizations are constantly reviewing their risk models in order to stay competitive in the aerospace and defense industry. New approaches should be considered because investments in innovation can yield high returns. As the cloud computing requirements of government contract work evolve, businesses must adapt to the direction ahead. However, many organizations may not be prepared for the cost of the transition. Detailed regulations that government contractors must adhere to can result in an extensive time commitment. Alternately, government contracting consultants could look for partnerships with those who are already on the leading edge of cloud computing technology.

The government's goal of advancing electronic data and information exchange has pushed businesses to align their strategies and processes to provide information faster. Conventional methods will be enhanced by more robust management information systems. IT organizations that are reviewing projects to enable the exchange of information need to consider cloud computing as a viable option.

Conclusions and Recommendations

From the perspective of the aerospace and defense industry, the following requirements apply to any cloud environment:

- Electronic and physical documents must be tagged in order to recognize export, security and IPR controls.
- A clear SLA and liability for loss of service must be established for both internal and external providers.
- The environment must support encryption of data during transfer outside the business.
- Encryption of data stored outside of the business must be supported. It is best to encrypt the data before it enters the cloud and decrypt it when it arrives at the recipient's device.
- The environment needs to recognize the location of an information requester—whether it is a person, organization or service—for any information that is subject to export control or national security constraints.
- The location of any information that is subject to export control or national security constraints must be ensured.
- The environment must keep records for five to 15 years with suitable archiving/recovery systems.
    - Provenance: Producer source/consumer destination identification
    - Tracking access

- Users must assess actual power, space and cooling requirements when setting up a cloud infrastructure.

It is fundamental that the industry recognize that the use of cloud technology does not remove the responsibility for considering information and its supporting technology and business considerations.

Recommendations

Large Companies

Large companies often invest substantial internal or outsourced resources to maintain IT services, so they can establish internal clouds or exploit community and public clouds for appropriate services. Business process outsourcing can often drive individual functions to a cloud environment.

The risks and appropriate mitigations listed below should be assessed for any service and class of data to be placed in a cloud environment. Different strategies may be established depending on the value and sensitivity to the business.

Risk	Mitigation Strategy
Data compromised when in the cloud because of unauthorized access or modification	Establish an SLA between the cloud provider and company that details how the access is gained and who has authority to access. The SLA should address the following questions: • How is access authenticated? • Ensure that the provider has secure access control through its own or a federated identity management system. • How are access decisions made? • Provide the criteria for who gets access to what based on the business context, the sensitivity of the data and the characteristics of the user population. • How is access audited? • The service provider must be capable of providing any evidence of who has accessed the cloud through the duration of the contract. • What separation exists between customers at the application, operating system and disk levels? • There is the potential of an active attack via shared infrastructure. Within the cloud, separation schemes should be employed between data belonging to different enterprises. • What methods are used to protect data in the event of a breach? Data should be encrypted when at rest and the SLA should specify the encryption methods and encryption strength for data stored in the cloud.

Risk	Mitigation Strategy
Data redirected and/or read by a third party during transfer to and from the cloud.	Establish a SLA between the cloud provider and company that details how data are protected when in transit. The SLA should address the following issues: • The cloud application must identify itself so the company's employees and systems know that they are connected to the correct site. • The cloud application must encrypt data when in transit between the company's systems and the cloud.
The company is exposed to regulatory noncompliance due to using the cloud.	Below are mitigation strategies for different kinds of regulatory issues:
Privacy laws	See the mitigations for unauthorized access and/or modification above.
Export control/ITAR restrictions	Include an agreement in the SLA to ensure that the data remains in the country of origin.
Classified information	Do not put classified data in the cloud.
IPR	Protect IPR using the mitigations for unauthorized access and modification above. If information is moving through more than one organization (e.g., a supply chain), the mitigations may need to be applied to multiple interfaces, cloud services or organizations.
Forensic analysis related to incident response or law enforcement. For example, what do you do if disks are impounded owing to criminal activity by other cloud users or a data spill of sensitive or classified information?	Include in the SLA a disaster recovery plan for recovering from backups the data that are confiscated or impounded due to an incident or investigation.
The cloud is unavailable for a short time (hours or days). Short-term outages can be caused by software or hardware failures or denial of service (DoS) attacks.	The mitigation strategy will depend on how a short-term outage affects the business process using the cloud. • Processes that cannot tolerate even a short outage should not be run in the cloud. • All other mission-critical processes should include a recovery plan, a failover mechanism (to another cloud or to an internal backup system) or a manual work-around for dealing with short-term outages.
The cloud is unavailable for a long time (months or years). For example, what happens if you build applications in cloud service A, and it goes out of business or is bought by company B, which then shuts down the service?	• Employ a data warehousing strategy and Extract, Transform, Load capability that is application agnostic, so you can store your critical data separate from a cloud service and be able to move it to another cloud service. • Employ a backup strategy that stores your data in a standard form. • Include contractual risk mitigation clauses, such as the right to use software in perpetuity. • Design your internal and cloud-based systems using service-oriented architecture so that you can replace parts and pieces as needed.
Applications and/or data in the cloud may be incompatible or inconsistent with each other.	• Establish an enterprise architecture practice that will govern and manage standards across your company. • Participate in establishing standards for cloud interoperability and select cloud services that employ them. • Design your internal and cloud-based systems using service-oriented architecture and include common services that follow data or API standards and/or translate between cloud services.

Risk	Mitigation Strategy
Applications developed using cloud tools and/or platforms might be considered a "joint work" between your company and the cloud provider, giving the cloud provider part ownership of the application.	• Consider legal action. • Include in the SLA a clause that releases you from any ownership claims by the cloud provider on the applications you build.

Many mitigation strategies depend on agreements between a company and the cloud provider. Violations of the agreements must have appropriate consequences in order to provide the motivation and just compensation needed to truly mitigate the risks.

Small Companies

Small and medium-sized companies typically have few resources for building and maintaining IT systems, so cloud systems present an attractive alternative to internal systems. The risks of using a public cloud like Amazon or Google, however, can be even higher for these smaller companies than for large companies. An unauthorized release of classified or sensitive data could cost the company its key contracts, putting the company's very existence in jeopardy. Therefore, the prospect of using cloud computing for small companies is a high-risk/high-reward proposition.

When defining mitigation strategies, smaller companies often do not have the team of lawyers or the economic clout of larger companies to modify a cloud provider's standard SLA, so the risk mitigations we offer here are descriptions of what to look for when selecting a cloud provider.

Risk	Mitigation Strategy
Data compromised when in the cloud because of unauthorized access or modification	The cloud provider's SLA or other documentation should address the following questions: • How is access authenticated? • Ensure that the provider has secure access control through its own or a federated identity management system. • How is access audited? • The service provider needs to be able to provide evidence of who has accessed the cloud through the duration of the contract. • How are customers separated at the application, operating system and disk levels? • There is the potential of an active attack via shared infrastructure. Within the cloud, separation schemes should be employed between data belonging to different enterprises. Separation schemes could be physical (such as separate disks) or logical (such as encryption and secure partitioning). • What methods are used to protect data in the event of a breach? • Data should be encrypted when at rest and the providers should specify the encryption methods and encryption strength for data stored in the cloud. The company should then put in place access criteria based on the business context, the sensitivity of the data and the characteristics of the system's user population.

Risk	Mitigation Strategy
Data redirected and/or read by a third party during transfer to and from the cloud.	Look for the following features in the cloud provider's offerings: • The cloud application must positively identify itself so the company's employees and systems know that they are connected to the correct site. • The cloud application must encrypt data when in transit between the company's systems and the cloud. The public key certificate methods used for HTTPS/SSL are the most common approaches to providing these features.
The company is exposed to regulatory noncompliance when using the cloud	Below are mitigation strategies for different kinds of regulatory issues.
Privacy laws	See the mitigations for unauthorized access and modification above.
Export control /ITAR restrictions	Most cloud providers will not guarantee that the data stored in the cloud remains in the country of origin. Unless you find one that will do so, do not put export-controlled information in the cloud.
Classified information	Do not put classified data in the cloud.
IPR	Protect IPR using the mitigations for unauthorized access and modification above. If information is moving through more than one organization (e.g., a supply chain), the mitigations may need to be applied to multiple interfaces, cloud services or organizations.
Forensic analysis related to incident response or law enforcement. For example, what do you do if disks are impounded owing to criminal activity by other cloud users or to a data spill of sensitive or classified information?	Try to select a cloud provider that has a plan for recovering from backups any data confiscated or impounded because of an incident or investigation. See also the mitigation for long-term unavailability below.
The cloud is unavailable for a short time (hours or days). Short-term outages can be caused by network, software or hardware failures, or by DoS attacks.	Do some "what-if" thinking. The mitigation strategy will depend on how a short-term outage would affect the business process using the cloud. • All mission-critical processes should include a recovery plan, a failover mechanism (to another cloud or an internal backup system) or a manual work-around for dealing with short-term outages.
The cloud is unavailable for a long time (months or years). For example, what happens if you build applications in cloud service A, and it goes out of business or is bought by company B, which then shuts down the service?	• Employ a backup strategy that stores your data in a standard form in a location that is accessible even if the cloud provider is unavailable. • Design internal and cloud-based systems using service-oriented architecture so that you can replace parts and pieces as needed.
Applications or data in the cloud may be incompatible or inconsistent.	• When available, select cloud services that employ standards for cloud interoperability. • Design your internal and cloud-based systems using service-oriented architecture and include common services that follow data or API standards and/or translate between cloud services.
Applications developed using cloud tools and/or platforms might be considered a "joint work" between your company and the cloud provider, giving the provider part ownership of the application.	Look for a clause in the cloud provider's SLA that releases you from any ownership claims by the cloud provider on the applications you build.

Many of the mitigation strategies depend on the security provided by the cloud provider. Carefully weigh the risk of exposing information that could cost you your business before moving to the cloud.

AIA Actions

It is recommended that the AIA Electronic Enterprise Integration Committee take action to track the development of cloud computing standards to ensure that they can be used to support the aerospace and defense industry requirements listed above. This research should address issues of security, availability and interoperability within and between cloud service providers.

In particular, security protocols for information should be designed to be compatible with the work of the Transglobal Secure Collaboration Program, such as tagging requirements. As standards and protocols related to cloud computing technologies are developed, AIA needs to monitor and adopt these new developments as appropriate.

It is recommended that AIA advocate with policymakers to ensure that consistent cloud standards are applied across different departments and agencies to facilitate the necessary connectivity to cloud services. AIA should also press for consistent international standards for the aerospace and defense industry.

It is recommended that AIA consider the business case for establishing an aerospace and defense community environment using an external cloud service provider.

SOCIAL NETWORKING

Introduction

Social networking is recognized as a disruptive IT component in an organization, since it offers new, spontaneous and ungoverned and uncontrolled capabilities to acquire and synthesize information in an innovative manner. Most social networking services operate in a cloud environment, independent of location, so all the risks and mitigations for the various classes of cloud-based services also apply to social networking. The specific requirements of the aerospace and defense industry demand particular care, since proprietary information not only is business critical but also can be a national security risk if exposed inappropriately.

Industry considers that the technology is widespread and pervasive, and the AIA eBusiness Steering Group is seeking to provide some authoritative guidance on how these services can be used to benefit businesses without compromising their security.

This section introduces the key characteristics of social networking, the industrial benefits of the technology and the risks and mitigations that large and small organizations must recognize as they consider how to exploit the technology. The section also highlights the key requirements for aerospace and defense companies in using social networking, and recommends specific actions for the AIA to allow its members to exploit social networks.

What Is Social Networking?

A social network service focuses on building and reflecting social networks or social relations among people (i.e., those who share interests and/or activities). A social network service (also known as one of the defining capabilities of "Web 2.0") essentially consists of a representation of each user (often a profile); their social links to other people, organizations and events; and a variety of additional services for communicating, playing, sharing and discovering. Most social network services are web-based and allow users to interact over the Internet, such as through e-mail and instant messaging. Although online community services are sometimes considered as social network services in a broader sense, a social network service usually refers to services focused on individuals whereas online community services are group-centered.

Social networks can be established in domains that are restricted to the whole or part of an organization or to a community of interest across multiple organizations, or they can be completely open to the public. It is also possible to establish social network services "behind the firewall," now commonly referred to as "Enterprise 2.0."

Business Impact of Social Networking Technology on the Aerospace and Defense Business

Recent Events

A number of key events and changes have precipitated consideration of social networking as a disruptive technology for the traditional computing environment in the aerospace industry. The availability of tools such as Facebook and LinkedIn has generated a new expectations for accessing information through people in an individual's network, which may extend outside a single organization. There is some debate over the assumption that new recruits to the industry expect the freedom to use such tools without restraint, despite the restrictions of export control, IPR and copyright. The recent DOD decision to permit military personnel to use social networks (subject to particular operational constraints) provides another impetus for broader use of the technology.

Opportunities

Social networking provides a number of opportunities to improve company productivity by connecting people with each other and to make more information available when and where it is needed.

- For example, some companies are using social networking technologies within their own domain to help employees network with subject matter experts, build internal communities of interest/practice and facilitate knowledge sharing between retiring workers and their successors. By making the senior members of an organization more visible and available, technology can flatten organizational hierarchies, enhance knowledge workers' productivity and improve overall business agility.
- A social networking tool can pull discussions and debates out of people's e-mail in-boxes and make the information visible to anyone on the networking service (not just in a particular group) or to the whole company. This kind of visibility can facilitate "viral" innovation, improving the speed of information flow, innovation and branding, but also risks data spill if the domain extends beyond the company.
- Public social networks can also be used to attract and recruit the talent your company needs and to draw in new customers. They can be used to discuss topics that are relevant to communities of interest or practice that include people from different organizations, companies or even countries.
- A social network can become a treasure chest of organizational knowledge that can be reused in any number of ways. For example, technologies such as mashups, composition of web services or composite applications can leverage a social network to combine the information stored there to discover new insights or to form new teams to address a particular need. The same openness can be exploited by the service provider to synthesize information; this is generally part of the business model. For example, Facebook will compare the lists of friends of individuals and offer suggestions to expand the network.

Threats

As noted above, all the risks and mitigations associated with private, community and public clouds apply to social networking services operating in those environments.

Since the purpose of social networks is to make people and information visible, there are a number of risks that come with using them. It must be emphasized that these risks are not unique to social networking, although the technology can increase the level of risk. Below is a table of risks and recommended mitigation strategies to address them. Internal networks are synonymous with private implementations, and external networks may be community or public.

Risk	Mitigations
Sensitive or classified information may be posted on internal or external social networks, making it visible to those who are not authorized to view it and creating a liability to the company through violations of security, export control, insider trading and IPR restrictions. There are also implications for ediscovery in litigation, particularly for material exposed on external networks.	• Establish company policies on what can and cannot be shared on internal and external social networks. Provide that policy to employees and make it visible to them when they enter social networking sites. • Include in the policy a clear definition of who can access external networks from the workplace and for what purpose. Enforce the access policy using automated controls. • For internal social networks, provide a capability to tag information as sensitive and to limit who can view information that has a "sensitive" tag. • For internal social networks, determine if you can provide sufficient controls to protect export-controlled information from being shared or stored in violation of export control laws. If you cannot, forbid export-controlled information from being posted to the site. • Establish "spill response" procedures for addressing the cleanup of unauthorized sharing of sensitive information. • Inform users that classified information should never be posted to any kind of social network. • Ensure that company material is protected by copyright.
Employees may speak on behalf of the company when they are not authorized to do so, sharing information that is not fully accurate or not consistent with company policies or branding	• Designate who can speak on behalf of the company. • Require others to include a "personal opinion" disclaimer on their social network posts and to avoid making statements about company policies or plans.
People can post false information, defame your people or company, or do other damage to your company's brand or reputation.	• Limit participation in external social networking sites to communities that include only employees of AIA companies in order to limit exposure. • Employ image or brand management techniques—regularly search for your company's name on social network sites and respond to any damaging information—either through dialogue or by having site administrators remove it.

Risk	Mitigations
Social networks may reduce productivity for some employees. For example, senior employees and subject matter experts may lose control of some of their time because they are more available to others. Some employees may spend too much time responding to the latest discussion post, and there is always the risk of social networking intrusively interrupting workflow.	Establish and communicate clear policies on appropriate use of social networks, providing guidance on etiquette, time charging and "response time" expectations.
Social networking can enable the aggregation of previously unlinked information. There may also be a question over who owns the IPR of the result, since there is no contractual environment.	Establish company policies on what can and cannot be shared on internal and external social networks. Provide that policy to employees and make it visible to them when they enter social networking sites.
Uncontrolled use of external sites may absorb significant network bandwidth.	Establish and communicate clear policies on appropriate use of social networks, providing guidance on etiquette, time charging and "response time" expectations.
Access to external sites risks the interaction and intermingling of personal and business transactions and information.	Establish company policies on what can and cannot be shared on external social networks. Provide that policy to employees and make it visible to them when they enter social networking sites.

Conclusions and Recommendations

The use of social networking tools can undoubtedly bring increased agility and capabilities to access and synthesize information within an organization, across a community or beyond. The increasingly pervasive nature of the technology implies that all organizations need to address the issue, regardless of their size.

The risks arising from social networking do not differ significantly from any other form of interaction between the members of an organization and external communities, but they can be exacerbated by the use of the technology. These risks can be mitigated by a combination of policies and operational constraints, imposed by technical means where appropriate. The required extent of mitigation should be assessed by individual organizations against the risks highlighted above, depending on the extent of the domain in which they operate.

Aerospace and Defense Company Private Networking: Private Clouds

Companies operating a social network within their own IT domain should implement the following components to mitigate risk:

- Establish a clear policy defining the objectives for the use of the service.
- Establish a code of conduct for using the service, covering rules for IPR, export control, security and appropriate use, etiquette and content.
- Tag information that is controlled by export, security or other restrictions to reduce the likelihood of inadvertent release for IPR.
- Provide initial training and continuing education to staff.

- Establish a governance role function for the service as a focus for monitoring usage and issues, involving representatives from groups responsible for security, legal (including IPR), human resources, export and import control, operations, ethics and IT

Community Cloud Social Networking

In addition to the components required for private social networks, companies using a community social network hosted outside their domain should implement the following components to mitigate risk:

- Extend the policy to include provisions that control the release of information, including nondisclosure agreement controls.
- Extend the code of conduct to include guidance on appropriate external use, such as including disclaimers and avoiding statements on organization policies and plans.
- Restrict access controls to the external community to particular individuals.

Public Social Networking

In addition to the components required for private and community social networks, companies using a public social network hosted outside their domain should implement the following components to mitigate risk

- Extend the policy to include provisions that control the release of information into the public domain and to address different types of usage.
  - Within company network
    - Specific approvals for access
    - Monitoring employee activity
  - Outside the company network with attribution to the company
    - Monitoring employee activity
  - At home as an individual
    - Monitoring employee activity
- Extend the code of conduct to include the extensions of policy for public activity
- Ensure that employees take responsibility for their actions
  - Within company network
    - Specific approvals
    - Monitoring employee activity
  - At home with attribution
    - Monitoring employee activity

- At home without attribution
  - Monitoring employee activity

Recommendations for AIA Action

It is recommended that AIA generate templates for the policies and codes of conduct for private, community and public social networking services, based on best practices. Companies have already started to create and apply policies and codes to exploit social networking and manage the risk of its use in various domains. Member companies should be invited to contribute examples of suitable policies and codes to act as the basis for this work.

It is recommended that the AIA consider establishing an industry social network service to support smaller companies in the supply chain with a secure social networking service. This service would enable sharing of appropriate knowledge that is not covered by individual company IPR, such as the registration of hazardous substances under REACh. The group has not made specific recommendations on the uses of such a service because one of the benefits of social networking is that uses will emerge from the community itself, within the policies established above.

CONSUMERIZATION

Introduction

With the increasing power and sophistication of computing devices, and reduced costs, more and more individuals are investing in personal devices that are often significantly better than equipment that they use in their working lives and offer less restricted connectivity to networks. There is growing pressure and incentive for such devices to be used for both personal and business purposes, rather than individuals carrying separate devices.

It must also be recognized that over the past few decades, the aerospace and defense industry has ceased to be the leading edge for IT development and exploitation, with high-performance gaming machines and immersive environments being exploited by, rather than pioneered by, our industry.

Industry considers that the blending of business and personal devices and the associated information will continue, and the AIA eBusiness Steering Group is seeking to provide some authoritative guidance on how these trends can be used to benefit the industry without compromising businesses or their security.

This impact section introduces the key features and industrial benefits of consumerization and the risks and mitigations that large and small organizations must recognize as they consider how to exploit the technology. The section also highlights the key requirements for aerospace and defense companies in taking advantage of all types of consumerization, and recommends specific actions for the AIA to facilitate exploitation of IT consumerization by its members.

What Is Consumerization?

As computing technology continues to evolve, devices that become available to the general public are often more powerful than the equivalent devices provided by businesses to perform the same or similar functions. Individuals use smartphones, laptop computers, netbooks, storage devices and other tools to access personal information in a ubiquitous networking world. As personal investment in technology continues, employees of aerospace and defense companies expect, and in some cases demand, to utilize the same advanced capabilities and devices in the business setting that they use in their personal lives.

Types of Consumerization

Business need to consider at least three aspects of this consumerization process:

- Employees using personal devices for both business and personal purposes, mixing applications and data on the same device.
- Influences of consumer devices on business computing, trading enhanced capabilities against possible extra risks.
- Marketers exploiting the identity and locations of phones and personal digital assistants (PDAs) to synthesize information and deliver unsolicited material and invade privacy over

open networks. The increasing availability of integrated Global Positioning System and radio-frequency identification (RFID) capability presents growing opportunities for others to detect this information and process it to their own advantage. The positive contribution is that such capabilities may be leveraged to improve communications within a business for tasks such as crisis management.

Device Consumerization

- Audio, image and video recording devices—it is almost impossible to obtain phones and other devices that do not include cameras that can record audio and video as well as images. These devices pose security risks and may compromise personal, company or export control restrictions.
- Mobile storage devices such as USB thumb drives, disks or solid-state memory can be used to exfiltrate large quantities of data and also permit intermingling of personal and company data.
- Computers, smartphones, some MP3 players and similar mobile devices such as e-book readers also have significant storage capacity and pose similar risks.
- Video games (such as flight simulations and UAV controllers) have been providing aerospace and defense innovation for years. A future example of this technology from Microsoft is the Xbox Kinect, which uses a "controller-less system" using a camera interface with built-in voice, face and gesture recognition. Artificial intelligence technology appears in a game called "Milo and Kate," where human players interact with "virtual humans and animals" that recognize them and respond with emotionally connected responses in an integrated three-dimensional world.
- Printers and other multifunction devices that act as servers on networks also have significant storage capacity and can retain copies of documents for extended periods.

Business Impact of Consumerization on the Aerospace and Defense Business

Recent Events

In the recent decade, the consumerization of IT assets has grown exponentially. The aerospace and defense industry as a whole has a technologically knowledgable workforce with a discretionary budget to afford significant investments in IT products and services. This workforce has access to IT infrastructure and computing resources on par with or of even higher quality than the IT departments currently provide to their employees.

The aerospace and defense workforce tends to make significant personal investments in business-class servers, multiprocessor high-resolution graphical workstations, laptops, mobile devices and high-speed processors in gaming platforms, smartphones and netbook-style computers, PDAs, networks and computer-assisted design programs, and modeling and project management software. This workforce also routinely leverages collaboration and social media services offered in the public cloud. The motivation for this consumerization can be increased productivity, mobility options and even peer pressure to keep up with the latest trends.

These devices deliver to individuals an unprecedented range of capabilities and connections through wireless, RFID and other routes. These connections also give away the location and transactions of the user, and open up new opportunities for collecting and synthesizing information; as a result, any data compromise can be far-reaching. The collection of consumer details provides unparalleled opportunities for the collecting organization to derive information about the consumers; security breaches such as the one suffered by TJ Maxx in 2007 can reveal personal and financial information that can be exploited unscrupulously. The cost of recovering from the loss of credit card details in this case was estimated at more than $4 billion.

Increasing dependency by individuals and organizations on such devices places increased emphasis on the quality of information. Examples such as the growing use of third-party services for logistics are particularly susceptible to data corruption.

Opportunities

This section highlights some of the business benefits that employers can realize through the growing consumerization of IT assets.

The business community can realize the benefits of this trend if they can exploit these IT assets, leverage the public infrastructure and defray their own IT costs by diverting a portion of their IT costs to the employee. Business can reap additional benefits from the increasing influence of standardization, vast economies of scale, high availability and reliability of public infrastructure. The other benefit or opportunity of consumerization is that the highly connected worker is likely to work longer hours, and during holidays and vacations, as a result of the blurring between work and personal life. Another benefit can be increased adoption cycles for new technologies, since many of the marketing campaigns for these consumer products play on the impulse buying power of the consumer, especially if the IT asset can have a profound impact on worker mobility.

In general, the business will realize the real benefit if the employee invests in dual use IT assets and services and the employer does not have to incur the expenses or manage the IT assets.

Threats

In the aerospace industry, we work with information that, if compromised, can lead to much more serious consequences than a compromise of typical business information. Therefore, the threats caused by using personal consumer electronics on the job can be severe.

If sensitive or classified information is leaked to a device owned by the company, we typically know who owns the device, what software is on it, how it can be wiped clean, how to locate the device and how to protect it from malware. We can therefore respond appropriately and protect the information from falling into the wrong hands. If, however, a personal device is connected to the company network and sensitive or classified information is leaked to it, we may not have any way to locate, clean, secure or recover the device. The owner of the device may be required to relinquish it to the company's security department with the possibility of it not being returned. Even if classified information is not leaked to a personal device, there can be similar concerns or issues regarding company data residing on the device.

Distribution of information to personal devices also has serious consequences for electronic discovery of information in legal cases. Uncontrolled duplication offers additional opportunities for e-discovery. In extreme cases, individual personal devices may be confiscated by the authorities as part of a company event.

The company will undoubtedly incur additional costs for integrating nonstandard personal devices, which may have multiple versions and configurations of both hardware and software, into the standard network and applications. The effort required to integrate such devices may well outweigh any performance benefits from an individual's use of the device. In addition, there may be licensing issues for software on the personal device.

The employee and the company may not have any means of providing malware protection on the device. If a device is infected and then connected to the company network, the infection and resulting disruption could spread to many devices on the network. Connection to external networks can easily compromise the personal device and offer opportunities for loss of company data. Wireless access can inadvertently create an unprotected breach into the company network.

When an employee disposes of a personal device, there may be no way to ensure that it does not have sensitive company information on it.

There can also be issues with consumer technology when traveling internationally. When crossing the border, customs officials have the right to examine anything on a computing device. If any electronic device has mingled personal and company data, it could create additional liabilities to the company if something inappropriate is found on the device.

It should also be recognized that many of the same risks that apply to cloud computing can also be recognized when a personal device effectively becomes part of the "corporate cloud."

Conclusions and Recommendations

It is recommended that AIA companies keep personal and business devices separate at present. Some technology under development will provide separation between personal and business information on the same device, but this is applicable only to a restricted set of devices. To take advantage of the benefits of consumer technology, we recommend that companies determine how to incorporate the devices and applications they would like to use into their collection of vetted and approved IT equipment.

It is recommended that AIA publish best practice guidelines on risk assessment and operation, covering implications to procedures that are implied by this disruptive technology; implications for IT provisioning, including capacity planning; and extension to controls on sensitive information.

It is also recommended that AIA develop template collaborative partner security agreements that can also cover the proposed Defense Federal Acquisition Regulation Supplement rule on safeguarding unclassified information, contains terms and conditions to effectively manage and validate the compliance for transfer of ITAR/sensitive information; and differentiates between large and small companies based on the existence of a nominated individual with responsibility for risk management and compliance.