# **A SPECIAL REPORT**

# Best Practices for Exploiting the Consumerization of Information Technologies

Leveraging the Benefits, Avoiding the Pitfalls

December 2011



# Best Practices for Exploiting the Consumerization of Information Technologies

# Leveraging the Benefits, Avoiding the Pitfalls

December 2011

Developed by: E-Business Steering Group



© 2011 Aerospace Industries Association of America, Inc.

1000 Wilson Boulevard, Suite 1700, Arlington, Virginia 22209 🗖 www.aia-aerospace.org

# TABLE OF CONTENTS

Executive Summary1	
В	Background
С	Consumerization
ĸ	Key Considerations
Introduction: What Is Consumerization?	
The	Impact of Consumerization
Key Recommendations	
Ν	Managing Sensitive Information
Ρ	Provisioning IT Services
Ρ	Policies and Procedures
Aerospace Industries Association	
А	AIA Member Companies
A	AIA Associate Member Companies

# EXECUTIVE SUMMARY

### Background

The traditional information technology environment in companies of all sizes often comprises a controlled set of selected hardware, software and services to deliver integration and economies of scale. Links between companies are achieved through either individually tailored solutions or flexible standards-based interfaces to provide flexibility. 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. Much of the new technology is coming from the consumer market and not being driven by aerospace industry requirements.

The nature of the aerospace and defense business implies that the industry is one of the most severe test cases for the effective deployment of such technologies, since it also must support the requirements for export control, intellectual property rights protection and national security.

In 2010, AIA published an initial statement of the likely impact of these technologies and the business, technical, cultural, operational and security implications for our industry, with the claimed benefits, risks and mitigations. The report, "Disruptive Information Technologies," [http://www. aia-aerospace.org/assets/report\_ebiz\_2010\_web.pdf] concluded 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 serve to exacerbate those risks. The proposed mitigations should be based on the assessment of the corresponding risks within individual organizations.

These guidelines describe best practices for companies to assess the risks involved in exploiting new technologies and capabilities within their business, and to operate such equipment to deliver benefits.

### Consumerization

The "consumerization" of IT is the ubiquitous use of consumer mobile devices and applications in the workplace. Several scenarios that need to be considered are:

- Employees using personal devices for both business and personal purposes
- Influences of consumer devices on business computing
- 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 the appropriate policies and procedures that are broadly applicable across aerospace industry organizations and the supply network.

## **Key Considerations**

The new consumerized technologies can provide real benefits to IT environments. AIA recommends that companies determine how to incorporate the devices and applications they would like to use in their collection of vetted and approved IT equipment.

If companies wish to take advantage of personal devices within their environment, great care must be taken to protect access to sensitive information and prevent its loss, whether deliberate or inadvertent. AIA recommends that information be tagged, and restrictions should be applied to what can be downloaded or processed on personal devices.

In addition, AIA recommends that personal devices will need to have a company-specified minimum standard configuration to protect the interests of the company, with constraints on network connectivity.

Because these technological precautions are not of themselves sufficient, AIA recommends that they be complemented by restrictive policies and processes to ensure individual responsibility and limit company liability.

Taken together, these precautions can disincentivize the use of personal consumer devices for business purposes. In the absence of suitable precautions, it is recommended that AIA companies keep personal and business devices separate at present.

## INTRODUCTION: WHAT IS CONSUMERIZATION?

As computing technology continues to evolve, devices that become available to the general public are often more powerful than the equivalent corporate standard devices provisioned by businesses within their own corporate architectures to perform the same or similar functions. Smart phones, tablets, laptop computers, netbooks, storage devices and other tools are acquired by individuals to access their personal information in a ubiquitous networking world. There is growing pressure and incentive for single devices to be used for both personal and business purposes, rather than for individuals to carry separate devices. The assumption of this guideline is that consumer devices and applications can be incorporated into the company's selection of approved devices; however, there are risks when there is an integration of personal-use devices with business.

In the past decade, this consumerization of IT assets has grown exponentially, and aerospace and defense as a whole has become comprised of a technologically knowledgeable workforce with a discretionary budget to afford significant investments in IT products and services. These include business-class servers, multi-processor high-resolution graphical workstations, laptops, mobile devices and high-speed processors in gaming platforms, smart phones and tablets, personal digital assistants (PDAs), Computer Aided Design/Computer Aided Manufacturing (CAD/CAM) 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 increase 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, radio frequency identification (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, so that any compromise can be far-reaching. The collection of consumer details provides unparalleled opportunities for a collecting organization to derive information about the consumers, and synthesize this information into new and customized services.

It must also be recognized that over the past few decades, A&D 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.

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

# THE IMPACT OF CONSUMERIZATION

There are at least three aspects of consumerization that require consideration by businesses:

- 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
- Marketeers exploiting the identity and locations of phones/PDAs to synthesize information and deliver unsolicited material and invade privacy over open networks. The increasing availability of integrated GPS and 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.

Consumerization impacts a wide range of devices:

- 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, with associated risks to security and compromises of personal, company or export control restrictions
- Mobile storage devices such as USB thumb drives, disks and/or solid-state memory, which can be used to exfiltrate large quantities of data and permit intermingling of personal and company data
- PCs, smart phones, tablets and mobile devices such as eBook readers also have significant storage capacity and pose similar risks
- Video games (such as flight simulations and UAV controllers) have provided innovation to A&D for years. Products such as the Microsoft XBOX Kinect use a "controller-less system" that employs a camera interface with voice, face and gesture recognition built in. (A game called "Milo and Kate" also adds artificial intelligence technology, as human players interact with "virtual humans and animals" that recognize them and respond with emotionally connected responses in an integrated 3D world.)
- Printers and other multifunction devices function as servers on networks, again with significant storage capacity that can retain copies of documents for extended periods

# KEY RECOMMENDATIONS

### **Managing Sensitive Information**

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

If sensitive, classified or export-controlled information is deliberately or inadvertently loaded (leaked) onto a device owned by a company, it is typically known 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. Therefore, the organization can 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, classified or export-controlled information is leaked to it, the organization 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 and/or issues.

Best practice: Ensure that sensitive and classified information is appropriately tagged, so that it is identifiable. The company may need to apply automated or procedural constraints to the classes of information that can be processed on personal devices.

Best practice: Master copies of company information should not be kept on personal devices – such devices should generally hold only uncontrolled copies of master information.

When an employee disposes of a personal device, there may be no way to make sure it does not have company information on it that the next owner of the device should not see.

Best practice: The company needs to reserve the legal right to ensure that company information can be deleted from personal devices used for company business.

There can also be issues with consumer technology when traveling internationally. When crossing a border, customs officials have the right to examine anything on a computing device being carried. As well as the previous problem related to classified or controlled company information, if any electronic device has mingled personal and company data, it could create additional liabilities to the company if there is something inappropriate on the device, even if it is unrelated to the company data.

Best practice: The company also needs to apply policy constraints to the type of personal information that can be held on personal devices used for company business.

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

Best practice: The company may need to apply automated or procedural constraints to the classes of information that can be held or processed on personal devices.

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

Best practice: The company may need to apply automated checks to information as it is imported from personal devices.

## **Provisioning IT Services**

This section highlights some of the business benefits that can be realized by the employer as a result of the growing consumerization of IT assets.

The business community can realize the benefits of this trend if they can exploit these IT assets and leverage the public infrastructure. Business can reap additional benefits from the increasing influence of standardization, vast economies of scale, high availability and reliability of public infrastructure.

It must be recognized that, some consumer devices are dependent on cloud services and therefore require ubiquitous access to the Internet. Consideration therefore needs to be given to the risks associated with such services as described in the 2010 "Disruptive Information Technologies" report published by AIA. [http://www.aia-aerospace.org/assets/report\_ebiz\_2010\_web.pdf]

Best practice: Where cloud services are used, the company needs to make adequate provision for security of information during storage and transmission, continuity of service against both short- and long-term interruptions, and support for export control, national security and IPR requirements.

In addition, there would appear to be some benefits to using employee personal equipment to defray company IT costs. In general, the real benefit is realized by the business 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. However, consideration should be given to the impact of the failure of personal devices and the possible disruption to service if the individual replaces the equipment.

Another benefit can be increased adoption cycles for new technologies since many of the marketing campaigns for these consumer products play upon the impulse buying power of the consumer, especially if the IT asset can have a profound impact on the mobility of the premise-free worker.

The company will undoubtedly incur additional costs for integrating nonstandard personal devices that 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 the use of the device by an individual. In addition, there may be licensing issues for software on the personal device.

Best practice: To take advantage of the benefits of consumer technology, companies should determine how to incorporate the devices and applications they would like to use into their collection of vetted and approved IT equipment.

The employee and/or the company may not have any means of providing malware protection on the device. If it is infected and then connected to the company network, the infection and resulting disruption could spread to many devices on the network.

Best practice: The company should specify a minimum hardware and software configuration for any personal device that is used for company business, covering malware protection, encryption, software versioning and access control.

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.

Best practice: Companies should monitor networks to safeguard against the comingling of internal and external networks and device configurations.

On the basis of the above requirements, it is recommended that AIA companies keep personal and business devices separate at present. There is some technology under development that will provide separation between personal and business information on the same device, but this is applicable to only a restricted set of devices.

### **Policies and Procedures**

The human tendency to view personal productivity over corporate policy is a challenge for companies, especially when new technologies are adopted without any governance. This puts an emphasis on stronger corporate policies unless there is a technical solution to preventing the personal device use. Secure use of personal devices on company business cannot be guaranteed through the use of technology alone. It is necessary to supplement a minimum configuration for personal devices with appropriate policies and procedures to ensure individual responsibility and to limit company liability.

Best practice: Companies should ensure that their IT acceptable use policies cover the use of personal devices in terms of

- Restricting the classes of company information that may be held or processed
- Restricting the personal information on the devices to that which will not incur liability for the company

 Providing additional constraints for devices used on foreign travel, whether on company business or not

Best practice: Companies should ensure that any employee wishing to use a personal device is aware of the risks and provides the company with the necessary legal rights to secure its information in the event of disposal of the device or termination of the employee for any reason.

Another 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.

Best practice: Companies should ensure that they issue approved, policy guidance regarding the accounting of labor, and corresponding effects on payroll when employees use personal devices for company business outside normal working hours.

# AEROSPACE INDUSTRIES ASSOCIATION

Founded in 1919, the Aerospace Industries Association of America is the most authoritative and influential trade association representing the aerospace and defense industry. The association is the leading voice for the industry on Capitol Hill, within the administration, and internationally.

In times like these, AIA's strong representation and advocacy is essential to protecting the business interests of the nation's aerospace and defense industry, while helping to establish new opportunities for growth.

AIA represents nearly 350 aerospace and defense manufacturers and suppliers. The association is at the forefront of critical issues, such as ensuring a strong U.S. industrial base, advocating for defense modernization and acquisition reform, increasing deployment of Next Generation Air Transportation System technologies and equipment, modernizing export controls, and obtaining additional resources for aeronautics research and space exploration.

Unlike many other associations, chief executive officers of member companies and their senior managers define and drive AIA's agenda. Working together, the association shapes regulatory and legislative policies, and is a leader in developing and publishing national aerospace standards that are used in aerospace design and manufacturing across the globe.

The aerospace and defense industry supports and drives our nation's economy. It fuels innovation, creates competition, and employs millions of Americans. AIA is proud to represent our members and our nation.

To learn more about AIA and the benefits of membership, visit www.aia-aerospace.org

#### **AIA Member Companies**

AAR Manufacturing, Inc. Accenture Acutec Precision Machining Aero-Mark, LLC Aerojet AeroVironment, Inc. AGC Aerospace & Defense AirDat LLC Alcoa Defense Align Aerospace, LLC Alion Science & Technology Allfast Fastening Systems, Inc. Alliant Techsystems, Inc. (ATK) Allied Barton Security Services American Pacific Corporation AmSafe Aviation AMT II Corporation Analytical Graphics, Inc. ANSYS, Inc. Aurora Flight Sciences AUSCO, Inc. B&E Group, LLC B/E Aerospace, Inc. BAE Systems Barnes Group Belcan Advanced Engineering and Technologies Boeing Company Bombardier Aerospace Broad Reach Engineering Company **BRS** Aerospace CAE USA Inc.

Castle Metals Aerospace Celestica Corporation Certon Software, Inc. Chromalloy CIRCOR International Inc. Click Bond, Inc. Cobham Colt Defense, LLC Computer Sciences Corporation (CSC) Comtech AeroAstro, Inc. Crown, Inc. Cubic Defense Applications, Inc. Curtiss-Wright Corporation Curtiss-Wright Controls, Inc. Metal Improvement Company Deloitte Consulting LLP DigitalGlobe Ducommun Incorporated DuPont Company Eaton Corporation Elbit Systems of America Embraer Aircraft Holding Inc. Erickson Air-Crane Incorporated ESI North America ESIS, Inc. Esterline Technologies Exostar LLC Flextronics International USA FlightSafety International Inc. FTG Circuits, Inc.

Galactic Ventures LLC General Atomics Aeronautical Systems, Inc. General Dynamics Corporation General Electric Aviation Gentex Goodrich Corporation Groen Brothers Aviation Inc. Guardsmark, LLC Harris Corporation HCL America **HEICO** Corporation Hexcel Corporation Hi-Shear Technology Corporation HITCO Carbon Composites Honeywell Aerospace HP Enterprise Services, Aerospace Hydra Electric Company **IBM** Corporation IEC Electronics Corp Infotech Integral Systems, Inc. ITT Exelis Jabil Defense & Aerospace Services LLC Kaman Aerospace Corporation KEMET KPMG LLP L-3 Communications Corporation LAI International, Inc. LMI Aerospace Inc. Lockheed Martin Corporation

Lord Corporation Marotta Controls, Inc. Meggitt-USA, Inc Metron Aviation Inc. Micro-Coax, Inc. Moog, Inc. Natel Engineering Co. Inc. NobleTek NORDAM Northrop Grumman Corporation NYLOK Corporation O'Neil & Associates Omega Air, Inc. Oracle USA, Inc. OSI Systems, Inc. Pacifica Engineering, Inc. Pall Aeropower Corporation Paragon Space Development Corporation PARTsolutions, LLC Parker Aerospace Pinkerton Government Services, Inc. Plexus Corporation PPG Aerospace-Sierracin Corporation PRTM, LLC

PTC PWC Aerospace & Defense Advisory Services Qwaltec RAF Tabtronics, LLC Raytheon Company Realization Technologies Inc. Remmele Engineering, Inc. Rhinestahl Corporation **Rix Industries Rockwell Collins** Rolls-Royce North America Inc. RTI International Metals, Inc. Sanmina-SCI Corporation SAP Public Services Satair SCB Training Center, Inc. Science Applications International Corporation Siemens PLM Software Sierra Nevada Corporation, Space Systems SIFCO Industries, Inc. Sila Solutions Group SITA SM&A

Space Exploration Technologies Corporation Sparton Corporation Spirit AeroSystems Tech Manufacturing LLC Textron Inc. The SI Organization, Inc. Therm, Inc. TIMCO Aviation Services Inc. Timken Aerospace Transmissions, LLC Triumph Group, Inc. Aerospace Systems Group Aftermarket Services Group UFC Aerospace United Technologies Corporation Pratt & Whitney Sikorsky Hamilton Sundstrand Valent Aerostructures Vermont Composites Inc. W. L. Gore & Associates, Inc. Wesco Aircraft Hardware Corp. WIPRO Technologies Woodward Governor Company Xerox Corporation

#### **AIA Associate Member Companies**

300 Below 3M Company A.T. Kearney Public Sector & Defense Services LLC Acme Industrial Company ADI American Distributors, Inc. Aeronautical Systems, Inc. Aerospace Alloys, Inc. Aerospace Joint Apprenticeship Committee (AJAC) Aerospacemall.com Air Industries Machining Corporation Airborn Operating L.P. Alcoa Fastening Systems Allen Aircraft Products, Inc. Altemp Alloys, Inc. American Brazing AMI Metals, Inc. APV Manufacturing & Engineering Co. **ARINC Engineering Services** LLC Arkwin Industries, Inc. Asia Pacific Engineering Consulting Services, LLC Astro-Med, Inc. Astronautics Corporation of America ATC Aerospace Athena Manufacturing, LP Banneker Industries, Inc. Benchmark Electronics, Inc. Brogdon Tool & Die, Inc.

**BRPH** Architects & Engineers **BTC Electronic Components** California Manufacturing Technology Consulting CDG Celltron Inc. Cherokee Nation Distributors **CIT** Aerospace CMC Electronics **Co-Operative Industries** Defense, LLC Coalition Solutions Integrated, Inc. Consolidated Precision Products CPI Aero Crawford & Company (formerly Furniture Resources) Crestwood Technology Group Dassault Systemes Data Conversion Laboratory, Inc. Dayton T. Brown Inc. Electronic/Fasteners, Inc. Embry-Riddle Aeronautical University Emhart Teknologies Black & Decker Company ENSCO, Inc. Essner Manufacturing, L.P. ETA Global, Inc. Exotic Metals Forming Company LLC Freedom Alloys

Frontier Electronic Systems Corporation Future Metals, LLC G.S. Precision, Inc. General Products Glovia International H&S Swansons' Tool Company Haas TCM/Avchem HCL Technologies HDL Research Lab, Inc. Hi-Temp Insulation Inc. Houlihan Lokey Hughes Bros. Aircrafters, Inc. Industrial Metals Intl. Ltd. Infotech Enterprises America Inc. InfoTrust Group Ingenium Inmedius InterConnect Wiring International Technegroup Inc. (TranscenData Division) Intrepid Learning Solutions ITW CIP Janes Capital Partners JRH Electronics, LLC. Kennametal Inc. Kubotek USA Kulite Semiconductor Products, Inc. Lintech Components Co., Inc. Loos & Co., Inc. MAG Industrial Automation Systems, LLC

Maine Machine Products Co., Inc. Materion McCann Aerospace Machining Corporation Meehan Electronics Corporation Meyer Tool Inc. Microsemi Corporation Mid-State Aerospace Inc. Millitech, Inc. Moritz Aerospace, Inc. Monogram Aerospace Fasteners Montana Metal Products, LLC Morris Machine Company, Inc. Morton Manufacturing National Machine Group National Utilities Company New Breed Corporation Norfil Manufacturing, Inc. North Shore Components, Inc. O'Neil & Associates, Inc. Oceanit Ohio Aerospace Institute **Orion Industries** P3 – North America Consulting Limited Parkway Products, Inc. PCC Airfoils, LLC Pelican Products, Inc. Perillo Industries, Inc. Phillips Screw Company Plymouth Engineered Shapes Precision Gear

Precision Tube Bending Premier Precision Group RAM Company **Renaissance Services** Renaissance Strategic Advisors II, LLC **Rocker** Industries Rubbercraft Safran USA Samuel Aerospace Metals Scot Forge Corporation SDL (formerly XyEnterprise) Sea Air Space Machining & Molding (Formerly named North Cape RIM Manufacturing) **SEAKR** Engineering Seal Science, Inc. Sechan Electronics, Inc. SELEX Galileo Inc. Senior Aerospace Serco Inc. Service Steel Aerospace Servotronics, Inc. Shapes Aerospace International Sigma Metals, Inc. SMT Corp Southern Manufacturing Technologies Spincraft Spirit Electronics, Inc. SPX Precision Components Sugasawa Corporation Sulzer Metco (US) Inc. Sunshine Metals, Inc.

Swift Engineering Synchronous Aerospace Group Sypris Electronics Systec Tactair Fluid Controls TCS America TechSolve, Inc. TEK Precision Co. Ltd. **Telephonics** Corporation The Ferco Group The World Academy Thermacore, Inc. ThyssenKrupp Aerospace North America TIGHITCO, Inc. Tiodize Co., Inc. Tri Polus Inc. TSI Group Inc. TSI Plastics, Inc. TTI, Inc. TTM Technologies, Inc. TW Metals **UFP** Technologies Umbra Cuscinetti, Inc. University of Tennessee -Aerospace Defense Clearing House Venture Aircraft, LLC VISTAGY VT Group, Inc. Vulcanium Metals Incorporated Whitcraft LLC Windings, Inc. X-Ray Industries Yarde Metals

#### Aerospace Industries Association

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

