White Paper

Product Development in the Cloud: No Cause for Concern

Sponsored by: Dassault Systèmes SolidWorks

Christopher Holmes Craig Stires

August 2014

IN THIS WHITE PAPER

Companies today are faced with the challenge of a complex and hypercompetitive global market. Aggressive competition from emerging economies coupled with increasing costs in creating continued innovation make product differentiation a challenge. For these companies to thrive globally, they need to look at how they can speed up their internal decision making, and also their integration with partners up and down the value chain so as to enable fast responses to marketplace demands and the development and delivery of innovative products.

The promise of cloud solutions can serve as an integration backbone for inter-enterprise collaboration through virtualization of the IT infrastructure. Data can be exchanged any time and from anywhere between enterprises across the world over the cloud. This enables better and faster decision-making capabilities across trading partners operating in the same value chain, and in turn drives new levels of innovation. However, perceived security concerns continue to be the single most important barrier to cloud adoption. This is a general perception that if the data is not on-premise, it is not secure. However, IDC research also shows that most security breaches come from inside the organization, and having all data in a central repository in a professionally managed cloud environment can in fact provide more security than leaving it to an organization. This is especially so for small and medium-sized businesses (SMBs) which tend to have limited budget and skills to manage security effectively.

This White Paper details the key issues impacting the on-premise and cloud environment for product development. It also discusses how organizations, especially SMBs, are responding to or should address the cloud security dilemma to maintain a competitive advantage.

SITUATION OVERVIEW

Today's business consists of an integrated value chain of globally dispersed small and large companies which work together to deliver a product. This value chain is made up of companies that design, design and manufacture, or manufacture, supported by service companies which provide essential services such as logistics and testing. This value chain is having to compete globally with other value chains, and is facing a number of day-to-day challenges. The first is competition coming from anywhere around the globe. Second, businesses are operating in an environment where customers are demanding cheaper and more innovative products. Third, costs such as labor or utilities are increasing which drives up the cost of manufacturing. And finally, the ability to act quickly and be

able to get products in the marketplace is becoming a key differentiator. For all companies across the value chain, competing and winning in this new environment requires improvements across all parts of the value chain.

In order to address these challenges, all companies across the value chain need to examine the way they operate. They need to look at how they can speed up their internal decision making, and also their integration with their partners up and down the value chain to work together to enable fast responses to marketplace demands and the development and delivery of innovative products. Although process improvement exercises will yield some result, companies must look to technology to deliver significant improvements. While much new technology has been focused at larger organizations, the advent of cloud computing has given small organizations the ability to access data anywhere, to collaborate and to utilize massive computing power.

Technology Challenges of Small and Medium-Sized Businesses

For small and medium-sized businesses, there are a number of challenges in the adoption of technology, most notably the cost and skills required to purchase, implement and maintain the technology. At the outset, the justification of purchasing new technology is especially difficult in smaller companies as the investment money is usually limited, and there are many competing demands for it such as new staff, new equipment and new machines. Any investment in technology would need to justify itself against all the other investment priorities that exist within the organization.

And even if the new technology does justify itself, there are the challenges of implementation and maintenance of the technology to contend with. Within SMBs, it is typical that the role of IT Manager is handled by one of the engineers within the organization who has a passing interest in IT. It is not a full-time role, and the requirements of the role have to compete with the other activities within the organization, which are typically linked directly to revenue generation. Coupled with the human challenges, the IT infrastructure within smaller companies is also extremely limited and often outdated.

THE POWER OF THE CLOUD ACROSS THE VALUE CHAIN

Current Adoption of Cloud

Companies can currently choose among a vast array of cloud deployment models. The three core deployment models researched for the purposes of this IDC Manufacturing Insights White Paper include public, private and hybrid cloud.

- **Public cloud**. This cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Private cloud.** Private cloud is operated solely for an organization. It may be managed by the organization or a third party and may be hosted both on-premise and off-premise.
- **Hybrid cloud.** This can be defined as a composition of the public and private clouds, which remain unique entities but are bound together by standardized or proprietary technology.

The current adoption of cloud technologies has been predominantly focused on IT management activities such as data backup and archiving, as well as enterprise resource applications. However, this is expected to change rapidly over the coming years, with an increasing number of business applications being offered in a cloud model, and organizations increasingly adopting cloud applications.

Advantages of Cloud Adoption

The main advantages of cloud adoption can be split into two categories: the first deals with the business benefits of adopting cloud-based applications, and the second deals with the ease of adoption. Looking at the business value, the key benefits are:

- **Connected.** "Connected" allows for information existing in the cloud to be available anytime and anywhere. Information sitting in a cloud environment can be pulled from any device whether it be a smartphone, tablet or PC.
- **Social.** Information in the cloud can be shared among team members, partners, suppliers and customers. The information sitting in the cloud can be made accessible to anyone granted privileges to view that information.
- **Governance.** Using cloud technologies ensures that everyone has the latest version of the information, coupled with the history of iterations. It also ensures that everyone is running the same version of the software removing possible issues in version conflict.

In terms of the ease of adoption, key benefits include:

- **Scalability of deployment.** The time taken to deploy a cloud-based application is instantaneous. Organizations can therefore scale up quickly. Typically, once payment has been made, the application is made available immediately without the need of getting new hardware and configuring applications. This allows organizations to be more agile.
- **Minimal IT skills/hardware/infrastructure required.** The deployment of cloud requires minimal IT skills to get the application up and running. All that is required is a PC or mobile device and an Internet connection. The cloud provider typically takes care of all the infrastructure requirements such as storage and security.
- **Pay based on what you need.** The traditional model of buying software licenses and paying maintenance for upgrades is being re-thought by organizations. The opportunity to add users and capacity on needs-basis is attractive to many organizations. Consumption-based pricing is a benefit that cloud offers with software as a service (SaaS).

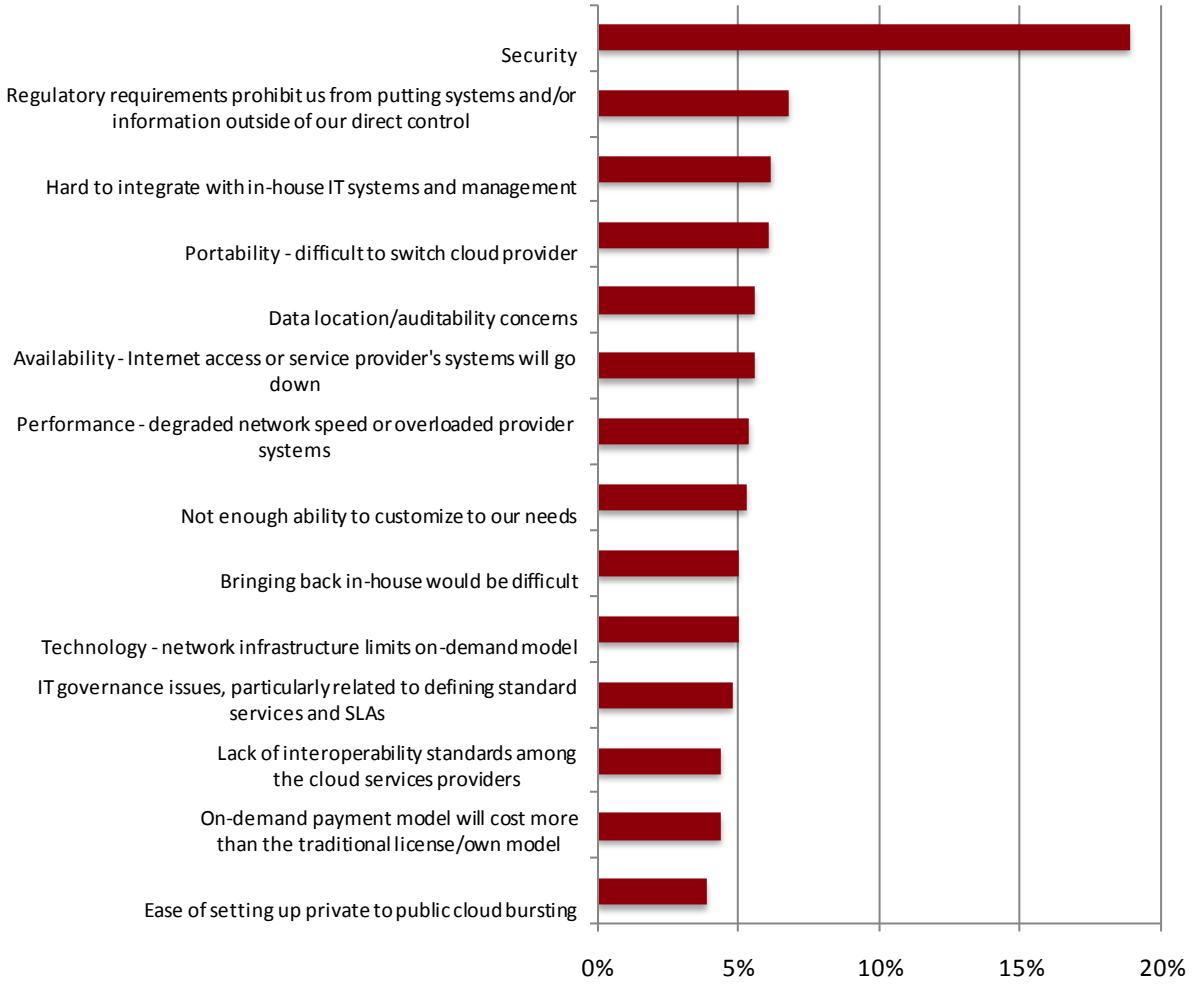
Concerns in Moving to the Cloud

The cloud has evolved through several phases over the past decade to become the services, applications and infrastructure that we see today. However, there are still concerns about moving to the cloud. In Figure 1, we see that security stands out as the top concern about moving to the cloud for manufacturers. The concern here is not just about a security breach, where sensitive information is "hacked", but also about the loss of control of the data. Regulatory requirements, auditability and other governance challenges are issues that organizations need to address.

Other concerns that need to be taken into account when considering moving to the cloud include regulatory requirements that prohibit some companies from putting systems and/or information outside their direct control, or outside of country borders, as well as the difficulty to integrate with in-house IT systems.

FIGURE 1

Manufacturers' Concerns about Cloud Adoption (Worldwide)



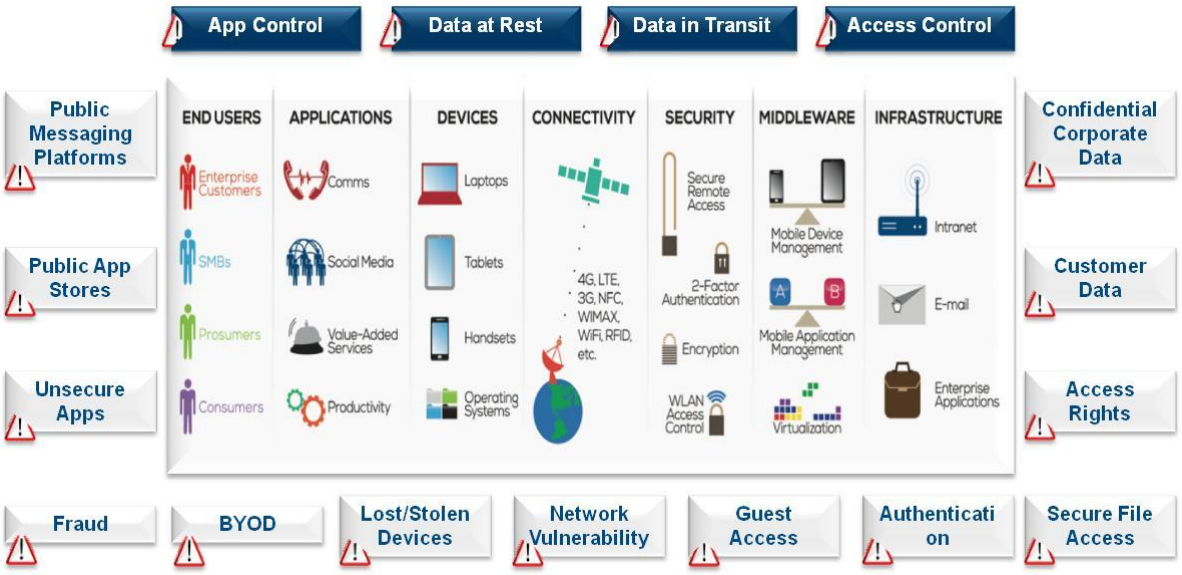
Source: IDC Manufacturing Insights, 2013

Security: A Closer Look

Before getting into IT security we need to look at the entire ecosystem in which today's business operates, no matter how small. The challenge can be seen in Figure 2. Here we have end users working on applications, on devices that are connected to the corporate infrastructure. Within this environment there are numerous security concerns. At the simplest we have lost/stolen devices where a laptop or portable hard disk or USB stick is misplaced, to the more deliberate form of attack where the organization is targeted in an organized attempt to steal data. This type of "espionage" attack is currently on the rise, with a recent Verizon 2014 Data Breach Investigations Report highlighting the increase of espionage type attacks.

FIGURE 2

The (In) Secure Ecosystem



Source: IDC Telecoms Practice, 2013

Looking at the typical product development process, product designs are usually transferred and shared via email or a portable storage device like a hard disk or flash drive. The physical devices are often insecure, by nature, and make it very difficult to enforce access controls for unauthorized individuals. Some limited amount of protection can be added through encryption, but leaves a gap in the larger context of content control. Version control and the ability to track access and usage are lost across email and physical transfer, which breaks an essential component of effective change management of the product design.

On the contrary, having the product design data centrally hosted in the cloud can provide a “single version of truth” of the same design as it progresses along the development process. Central data access control is also more effective through centralized user login access. As the design data only resides in the cloud, only centralized security on the single access point is necessary. This simplifies

and improves the efficiency of security measures. However, there are still security concerns which need to be addressed, such as:

- Availability – is it on? Can I use the product or access the data any time I want?
- Asset management (how to prevent data loss and data destruction) – What if my data is lost? Is there any backup? How can I recover my lost data? How is my data managed?
- Protecting intellectual property (IP) (data being stolen by competition/public) – How easily can competitors and/or the public hack into my data or system? Who has accessed my data?

A "Defense in Depth" Security Strategy

Security is an evolutionary process, not only due to the continuous developments in terms of technology and usage patterns in place, but also because of new security challenges. Organizations today need to therefore adopt a holistic approach to IT security that is often referred to as "defense in depth". A defense in depth strategy embraces a multi-layered approach to security that is enforced independently between each layer. This can involve both endpoint (device) and network security, as well as content and information security, where a breach in one will not have a domino effect on the others. To introduce a defense in depth approach requires implementing technologies such as layered firewalls, domains of trust, enhanced user authentication processes and data protection strategies and tactics.

However, technology is only one part of the overall strategy. People and processes are also essential components. The process element is about having well-planned and documented processes that define the specific actions that need to take place when specific types of security breach occurs, whether it be a misplaced laptop or a hacker attack. This requires having sufficient people available to be able to envision the type of event that may happen (based on the levels of security required by the specific organization) as well as having a response team available that understands what, when and how action and reaction to an unwanted event should it take place. While large organizations can put in place teams to manage the security process, the challenge for smaller organizations is how to put in place acceptable technologies and processes within the company's means.

IT Security

We continue to see a rise in the volume of threat incidents and sophistication of attack vectors. What has been changing over the last few years, according to the Verizon 2014 Data Breach Investigations Report, has been the growth of espionage type of attacks. This was highlighted as the number one type of attack in 2013 for manufacturing organizations, followed by denial of service attacks. With the increase in the number of attacks, the challenge on how to manage security becomes key.

There is a general perception among organizations that if the data is not on-premise, it is not secure. However, while attacks typically come from outside of the organization, many of the vulnerabilities and threats come from within. These internal security incidents can be more difficult to defend against. Examples of internal security incidents include a laptop being lost, a disgruntled employee downloading or deleting some files or a USB stick being misplaced. There is also the issue of hardware (e.g., hard disk drive) failure to be considered, and unless the organization has implemented backup policies, valuable information can be lost.

With this in mind, the idea of having all the data to a central repository – that is professionally managed, accessible from anywhere on any device, and provides more security than currently exists in many organizations today – becomes increasingly attractive. Having a professional cloud service provider (CSP) manage the cloud can offer greater assurance compared to leaving it to an organization, which has limited budget and skills to manage security effectively.

Having data on-premise is not a guaranteed protection and can pose some risk, as we have seen in a number of high-profile cases in which companies were hacked and sensitive data stolen, such as those of Sony, Target, Honda, American Express and Facebook. To combat the threats posed by hackers, it is important to note that there are several types of hackers.

1. **Hacktivist.** This type of hacker tends to look for attention in the media or among their peers. Their attacks may be to deface or otherwise embarrass an organization. Although their attacks can be damaging, the nature of their attack tends to be loud and easy to recognize. This means that organizations are aware that an incident has occurred and can start to contain the threat and mitigate damages. The exfiltration of data is often in large volumes and happens as quickly as possible. This is more likely to be recognized by data loss prevention systems and is more likely to be blocked. Hactivists may act in isolation or as part of a greater collective.
2. **State-sponsored.** These well-organized and well-funded groups are a significant threat to organizations, particularly in certain industries. Manufacturers, energy companies, defense contractors and utility providers are some of the most intensely attacked organizations by these types of hackers. The structure of these hacking groups often falls within the intelligence agency of the host nation. This lends itself to having a broad spectrum of hacking resources, including the people, the objectives and the equipment. The objectives often include stealing IP to gain advantage over competing nations. This includes channeling industrial research and development design into domestic companies. It also includes spying on commercial discussions to gain advantage in negotiations. The exfiltration of data tends to be slow, careful, intricate and very difficult to detect.
3. **Specialist.** Hackers who seek to make money. This group hacks into companies with the sole intent of stealing data, and then selling it. Typically, this group focuses on banks and retailers or any other company that has personal information combined with financial information. This group will steal the data and then sell it. In the case of discrete manufacturers, the product design is only of value when it is of the full design of the finished product and not of the parts only. With product design data and information, a designer's implicit knowledge of the product design is essential and for hackers to obtain such design information, it is a challenge beyond just stealing the raw product data. Moreover, such acts can also be deterred and pursued for compensation through legal means. Another threat that comes from this group of hackers is the creation of botnets. This is the process of infecting a large group of computers and taking them over for coordinated illegal activity. This often includes the activation of a distributed denial of service (DDoS) attack against a target entity.

CLOUD SECURITY

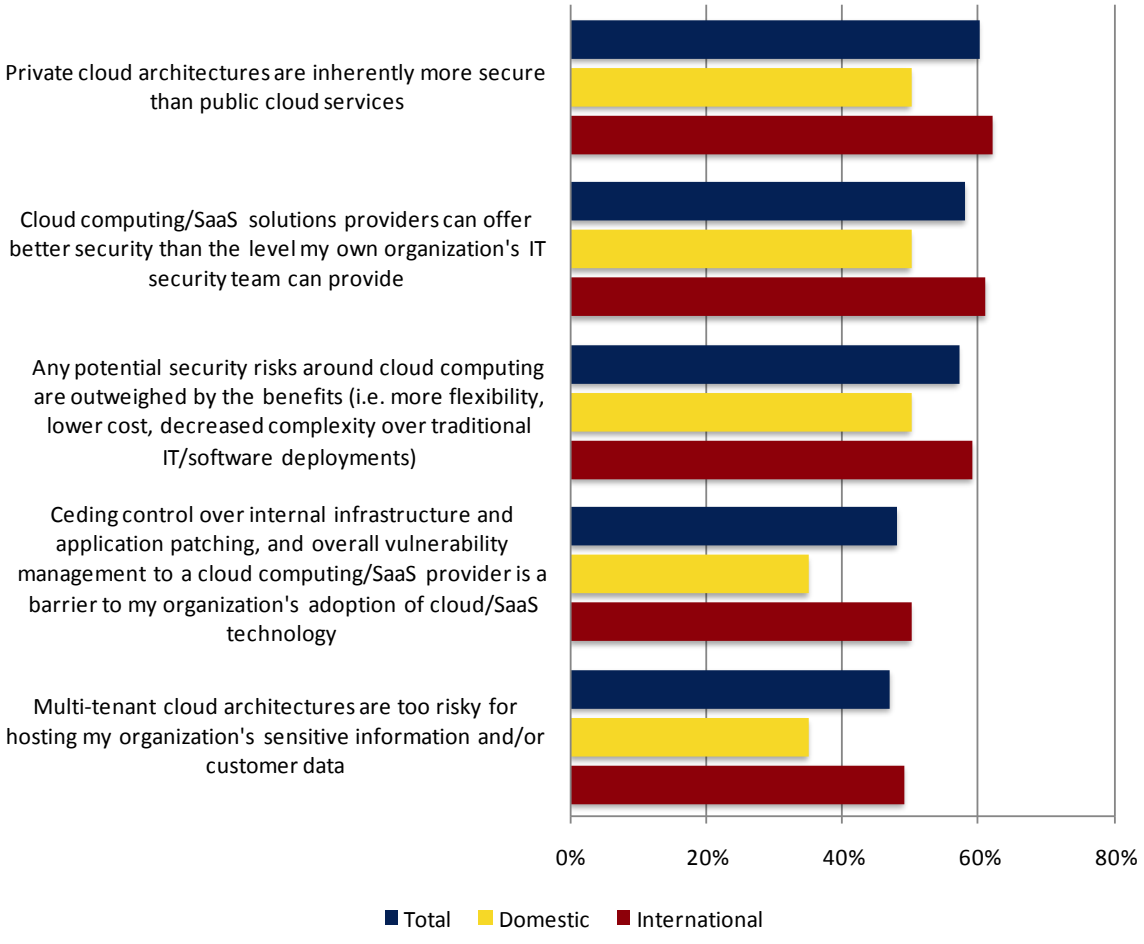
A recent survey (see Figure 3) by IDC highlighted that security offered by cloud providers is positive, with 60% of organizations agreeing that cloud service providers could offer better security than their own IT organizations.

As with all collaborative technologies, as soon as information is shared, there is a chance of losing control of the information. However, over half (57%) of enterprises agreed that the potential security risks incurred by moving to the cloud are outweighed by the benefits. Among domestic firms, 51% agreed with this, while 59.1% of international enterprises agreed. This indicates that multinational organizations in particular recognize the benefits of using the cloud.

The trend toward outsourcing activities where an outside provider can do a better job for less cost than an employee within the organization is also recognized. Security costs money, in skills, time and material. Many enterprises are also more at ease with the idea of sharing ownership of security with external providers.

FIGURE 3

Perceptions on Cloud Security



Source: IDC U.S. Cloud Security Survey, 2013

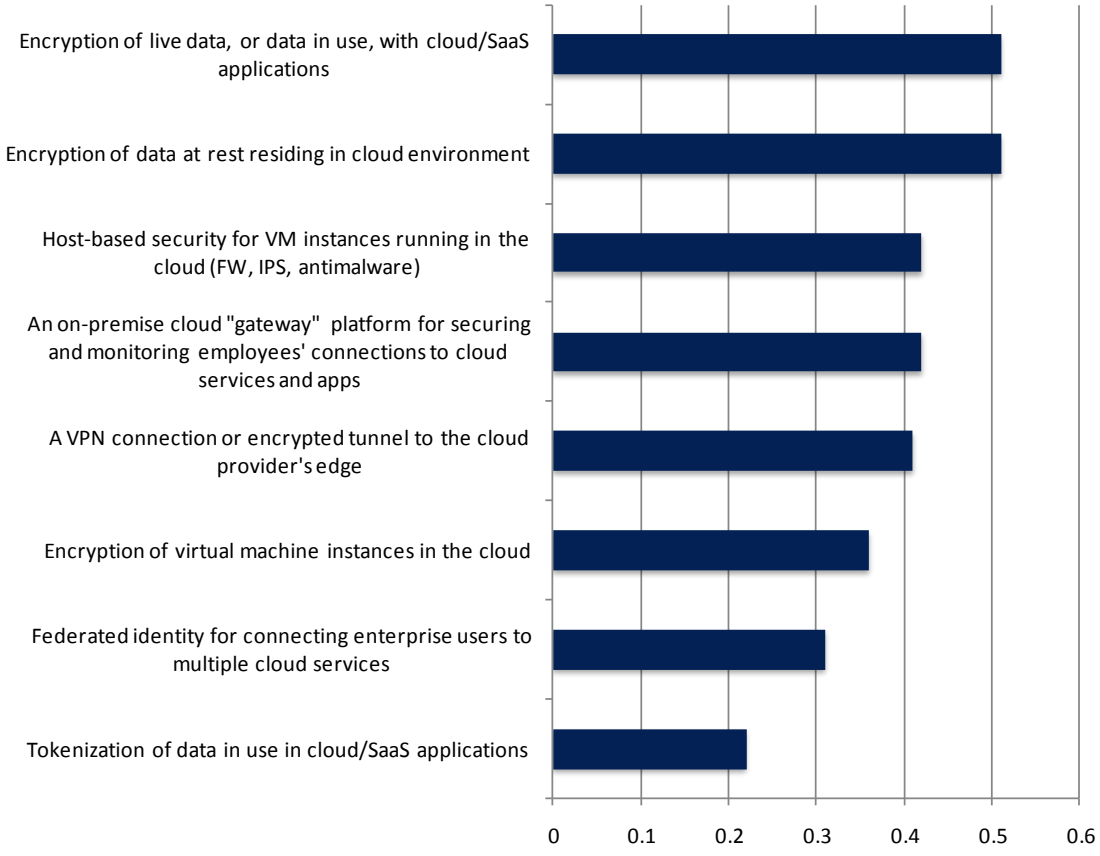
Cloud Security Starts with Encryption

This section looks at the technical details of cloud security, and what organizations expect from their cloud partner. Figure 4 shows the expectations of organizations in terms of the security approaches of vendors. In general, enterprises deploying cloud services recognize data encryption as a top priority.

It is important to note that data encryption can be implemented to protect while at rest, in motion and in use. Cloud service providers are expected to provide protection for all three forms. Organizations can have some direct control over the encryption of stored data, but rely on the cloud provider to protect data in motion.

FIGURE 4

Security Requirements Expected from Cloud Providers



Source: IDC, 2013

However, it must be remembered that while encryption is an effective tool for securing data in untrusted environments, it can be burdensome, and can slow down the access and use of applications. This is something organizations need to be aware of, if the application on the cloud is slow to respond, people will stop using it and resort to other tools. Security while essential, should not get in the way of an effective and efficient business process. Market-leading solutions on cloud should seek to ensure performance without compromising on security.

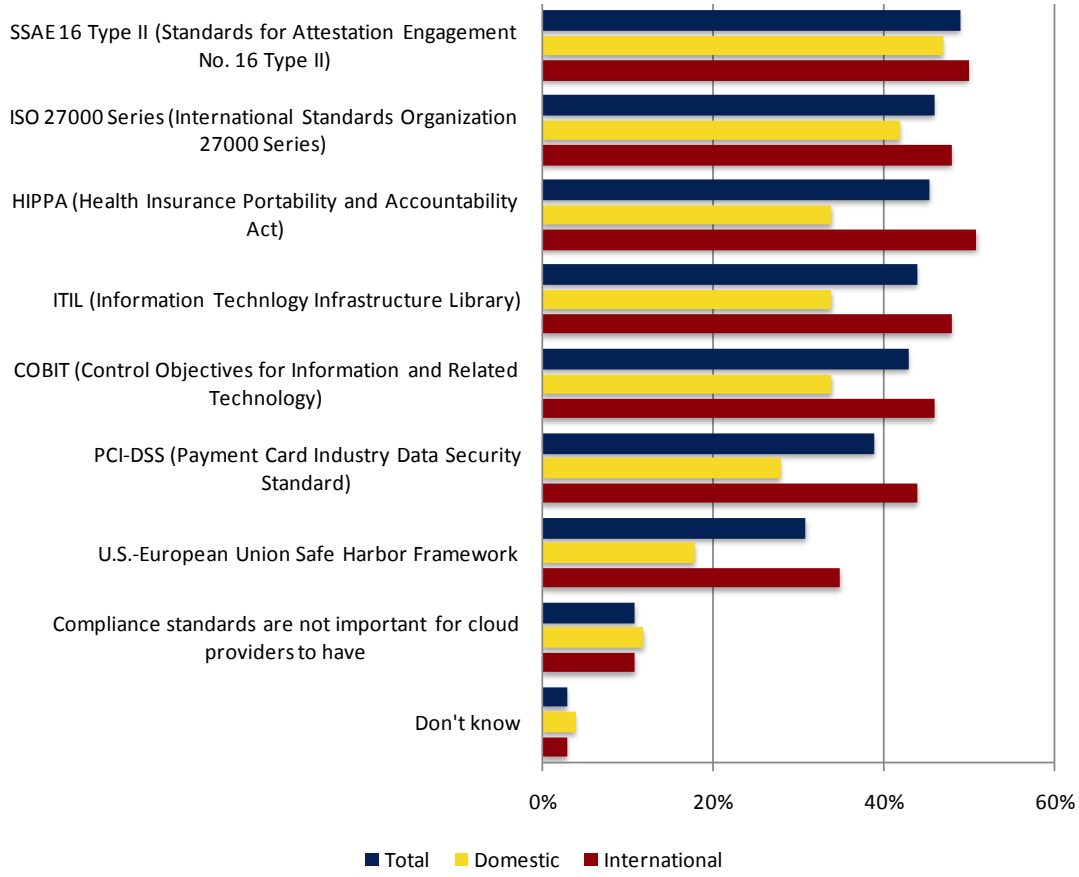
Another important standard for application security is the open web application security project (OWASP). This organization is a non-commercial group that enjoys broad international participation and sets the standard for the design and implementation of application security. Organizations that are looking to ensure a high level of security will need to assess the security compliance of the CSP as well as the application that is being hosted. Checking for full OWASP compliance is a good benchmark for assuring the security design of the application being considered.

Cloud Security Certification

As cloud technologies and standards continue to evolve, there are already a number of certifications that are available to cloud providers to demonstrate their security. Figure 5 shows the key certifications that companies would like to see their providers have in place. While some of these are industry specific, if the cloud provider is operating across a number of different industries, their investment to offer certification can be seen as advantageous as they have put in place the various processes and technologies to achieve a certified level of security.

FIGURE 5

Desired Security Certification for Cloud Providers



Source: IDC U.S. Cloud Security Survey, 2013

Industry certifications and frameworks for cloud service providers were generally more desired among international firms than domestic firms (55% versus 41%, respectively). International firms have more interest over all types of security measures cited. While there are many security certifications, not all are applicable to enterprises involved in manufacturing and associated services. Table 1 gives a description of the various certifications and their application for the manufacturing sector and value chain. Enterprises show strong demand for leading regulatory standards certifications and industry frameworks, including SAS 70, ISO 27000, HIPPA and ITIL; each of these regulatory compliance certifications was cited by more than 45% of enterprises.

TABLE 1

Certification and Standards Applicability for Manufacturers and Associated Services

Industry Certification/ Framework	Description	Impact for Manufacturing and Associated Services Selecting a Cloud Provider
ISO 27000/ SAS 70	**Framework** - The ISO 27000 series of standards are focused on information security matters. ISO (International Organization for Standardization) is the largest developer of standards in the world. Its membership comprises the National Standards Bodies of countries around the world.	**HIGH** - Can apply to a broad range of verticals as these two certifications reflect general best practices for how service providers in general follow explicit procedures to reduce risk and comply with security and IT best practices. While not perfect, these standards appear to have emerged as the most popular among enterprises as firms seek more of a baseline of official best practices and standards from potential CSP partners.
HIPAA	**Security Certification** - Health Insurance Portability and Accountability Act. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers.	**HIGH (medical devices only)** - Companies that service medical devices and have access to the patient information they contain are now considered business associates. And the new rule clarifies that all BAs must comply with the HIPAA Security Rule. Medical device servicers will need to implement a patch management program to protect against viruses.
ITIL	**Framework** - Information Technology Infrastructure Library (ITIL) is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.	**HIGH** - The ITIL security management process describes the structured fitting of security in the management organization. ITIL security management is based on the ISO 27001 standard.
SSAE16	**Framework** - Statement on Standards for Attestation Engagements 16 (SSAE16) is a regulation created by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) for redefining and updating how service companies report on compliance controls.	**HIGH** - SSAE 16 requires the management of the service company to provide a written assertion to the auditor that their description accurately represents their organizational "system". The organization's system description consists of the services provided by the organization and any and all operational activities that affect the service's customers. In addition, the organization must also assert that their description honestly describes their control objectives and the time

Industry Certification/ Framework	Description	Impact for Manufacturing and Associated Services Selecting a Cloud Provider
		period in which they are meant to be evaluated.
COBIT	**Framework** - COBIT is a set of resources that contains all the information an organization needs to adopt an IT governance.	**MEDIUM** - COBIT standards and processes that businesses can use to ensure that IT is working as effectively as possible to minimize IT-related risks and maximize the benefits of cloud. The security focus of using COBIT with the cloud include: customer compliance, selected authentication methods, customizable access control, enforcement of 4-eyes authorization (real-time monitoring and auditing capabilities), and forensics and contracts.
PCI DSS	**Framework** - The PCI Data Security Standard (PCI DSS) provides a framework for developing payment card data security process - including prevention, detection and appropriate reaction to security incidents.	**LOW** - Only applicable if payments for products/services are transacted online, using payment cards.
U.S.-EU Safe Harbor Framework	**Framework** - The U.S.-EU Safe Harbor framework is a cross-border data transfer mechanism that enables certified organizations to transfer personal data from the EU to the U.S. in compliance with European data protection laws.	**LOW** - Unless the organization is transmitting personal data.

Source: IDC Manufacturing Insights, 2014

SSAE 16 and ISO 27000 certifications for cloud services can apply to a broad range of verticals as these two certifications reflect general best practices for how service providers in general follow explicit procedures to reduce risk and comply with security and IT best practices. While not perfect, these standards appear to have emerged as the most popular among enterprises as firms seek more of a baseline of official best practices and standards from potential cloud service provider partners.

Hosting confidential data with cloud service providers involves the transfer of a considerable amount of an organization's control over data security to the provider. Organizations should therefore ensure that their cloud service provider fulfills their data privacy and security needs. Organizations should also choose the necessary industry certification standards for their needs.

IMPLEMENTING SECURITY AND THE CLOUD

Implementing security is all about trade off, regardless of deployment model – security versus connectivity versus performance. As mentioned previously, within the IDC stance on security is a defense in depth strategy – making it as difficult as possible and limiting the damage through independent security layers in the face of a hacking situation. The following are some guidance on implementing security on the cloud:

- Although concentration of computing resources and users in a cloud computing environment represents a concentration of security threats, this single point of entry or access also makes the management of security easier. Access controls, vulnerability assessment practices, and patch and configuration management controls can then be easily and adequately implemented over well-defined boundaries to protect your data.
- Internet connectivity is a major risk to business continuity in a cloud environment. Understand what controls are in place to ensure Internet connectivity is guaranteed. If a vulnerability is identified, check if you can isolate and terminate access until the vulnerability is rectified without impacting the whole network.
- If your business is subject to record retention requirements, understand what they are and how they can be met. Hosting your computing resources and data in the cloud makes the cloud provider's disaster recovery capabilities vitally important to your company's disaster recovery plans. Understand these disaster recovery capabilities and check if they have been tested.

On-Premise vs Cloud

Table 2 shows the advantages and disadvantages of adopting on-premise or cloud-based security solutions against the differing types of security threats.

TABLE 2

Comparing On-Premise and Cloud-Based Security Solutions

Risk	On-Premise		Cloud-Based	
	Pros	Cons	Pros	Cons
Hackers and Virus Attacks	▪ No shared infrastructure	▪ Need to ensure anti-virus is up to date ▪ Intrusion detection and data loss prevention systems expensive to implement and maintain ▪ Security skill required internally ▪ Speed of response to a security breach	▪ Points of entry into systems are well-defined and typically better protected ▪ Speed of response to a security breach	▪ Incident detection and handling is dependent on the effectiveness of a particular CSP
Data Privacy and Security	▪ Sensitive systems can be air-gapped	▪ Difficult to keep up with changing regulation	▪ Provider manages all regulatory requirements	▪ Lack of control as data resides out of own premise
Data Availability and Business Continuity	▪ Full control of systems and data	▪ Management of all devices and access points ▪ Manual update of storage/backup ▪ Self provision of disaster recovery	▪ Distributed infrastructure designed to provide 100% service availability ▪ Safeguard against loss from disaster onsite	▪ Potential challenge to enforce data governance, including compliance and auditability

Source: IDC Manufacturing Insights, 2014

In summary, the key advantage of moving to cloud-based security is the outsourcing of security. This has a number of benefits:

- **Reduction in IT skills.** For SMBs the advantages of moving to a cloud approach means that the security skills do not need to be maintained within the organization. This is a key advantage as security threats and technology are changing every day, and getting ever more complex, as more devices and technology are introduced.
- **Speed of response.** Should an attack be successful and the security layer be breached, the speed of response is critical to minimize damage. For smaller companies, the speed of response will typically be limited by the number of people that can be marshaled to address the issue; however, with a cloud model, the cloud provider typically has significantly more resources to be able to deploy to address the issue.
- **Auditing and monitoring of security.** The cloud provider is expected to continuously monitor the cloud environment for signs of attack, and provides regular updates to the security application, keeping security up to date.
- **Tested deployment of security.** The cloud provider will test security deployments before implementation, ensuring that applications continue to run, and that there is no loss of service due to security and application incompatibilities.

Government Legislation/Data Security Act: A Global Perspective

There is a wide variety of privacy laws and data protection regulations that can make it challenging for companies to know what they should and must do to protect themselves and their data. This section gives an overview of different countries and their legislation. One of the things to note is that great importance is placed on personal information, where any form of personal information that is collected requires significant attention to the country or region where it is being collected and processed to ensure that all laws are adhered too. As for industrial information such as design or intellectual property, the protection is not anywhere as severe, with legislation protection against the unauthorized access of the data, and also the possibility of intellectual property infringement.

USA

- Federal Laws and Regulations. The United States does not have a comprehensive privacy and data protection law. It relies on a mix of legislation, regulation and self-regulation resulting in a patchwork of federal laws covering some specifics such as personal information including financial records and vehicle registration.
- U.S. State Security Breach Notification Laws. Forty-six states have enacted legislation requiring notification of security breaches involving personal information. Typically personal information relates to a person's name and other sensitive information such as social security number, drivers' license information, credit card information, etc.
- Laws on the Interception of Communications. These laws that were originally designed to protect oral communication are now being extended to situations where individuals are monitoring/recording voice, digital, email or other electronic communications.

European Union

The European Union's (EU) Data Protection Directive is a directive adopted by the EU to protect privacy and all personal data collected for or about citizens in the EU. It encompasses all key elements from Article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life.

The recommendations are based on seven principles:

1. Notice: Subjects whose data is being collected should be given notice of such collection.
2. Purpose: Data collected should be used only for stated purpose(s) and for no other purposes.
3. Consent: Personal data should not be disclosed or shared with third parties without consent from its subject(s).
4. Security: Once collected, personal data should be kept safe and secure from potential abuse, theft or loss.
5. Disclosure: Subjects whose personal data is being collected should be informed as to the party or parties collecting such data.
6. Access: Subjects should be granted access to their personal data and allowed to correct any inaccuracies.
7. Accountability: Subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.

What is also worthy of note regarding the EU directive is that it is applicable to not only when the organization is established or operates within the EU, but whenever the organization uses equipment located inside the EU to process personal data. Hence, organizations outside the EU which process personal data inside the EU must also comply with this directive (Directive 95/46/EC).

Asia

China

Currently, China does not have an overarching national-level law on personal data protection. However, there is a national standard related to personal information – the Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information Systems. Although the Guideline is not mandatorily binding, it provides more details on personal data protection. There are many laws, regulations and local ordinances that can be applied. These include:

- The PRC Constitution which lists the rights that academics interpret as establishing an individual right to personal data. Article 40 establishes a citizen's freedom of communications and provides legal protection to private communications. Article 38 sets out a general right of citizens to be free from infringements on their dignity and protects them from defamation, false accusations and insults.
- The seventh amendment to the PRC criminal law adds the criminal offence of illegal provision and use of personal data.

- The General Principles of the civil law of the PRC (Article 120) protect a citizen's personal name, portrait, reputation and honor.
- Provisions of computer-related and Internet-related laws require that the contents of particular databases must be kept confidential, must be protected by security measures and must not be breached, altered or distributed.
- The Law of the PRC on Resident Identity Cards stipulates that public security organs and police forces must keep confidential citizens' personal information obtained through making, issuing, examining or seizing resident identity cards and that the police must not disclose personal information obtained through examining identity cards.
- The Postal Law guarantees the protection of freedom and privacy of correspondence and the safety of email.
- The Social Insurance Law prohibits governmental authorities and other organizations, as well as their staff, from disclosing personal information which they may obtain in the course of their work.
- The Provisions on Protecting the Personal Information of Telecommunications and Internet Users regulates the collection and use of the personal information of telecommunications and Internet users.

India

Right to privacy has long been read into Article 21 (right to life and personal liberty) of the Constitution of India. The concepts of "data privacy" and "data protection" have started demanding greater attention and were introduced in the Information Technology Act, 2000 (Act) through Section 43-A (Compensation for failure to protect data) and Section 72-A (Punishment for disclosure of information in breach of lawful contract). This has been further refined in the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information (SPDI).

CONCLUSION

The use of cloud-based applications is going to increase, as the financial and business benefits are compelling for organizations, particularly for SMBs. Cloud can serve as an integration backbone for inter-enterprise collaboration, enabling data to be exchanged any time and from anywhere between enterprises across the world through virtualized IT infrastructure. This enables better and faster decision-making capabilities across trading partners operating in the same value chain, and in turn drives effective innovation within a connected enterprise social network over the cloud.

As has been highlighted in this White Paper, the key concern among organizations is that of security. However, as we have discussed through this White Paper, moving to the cloud can enhance data security. In summary:

- **Availability assurance.** Business data must be available to organizations at all times, with recovery and disaster prevention as a non-negotiable service. Organizations will also want to understand their options for moving their data out from the cloud, or more likely, porting to a different cloud service provider.

- **Protecting of IP.** A defense-in-depth strategy is strongly recommended for organizations to adopt. For many organizations, their IP is one of the most important assets to protect. Doing this effectively requires investing in the right people, processes and technologies.
- **More complete security for SMBs.** For small and medium-sized businesses, cloud-based applications are more secure than those hosted on-premise. Security costs money, in skills, time and material. A cloud service provider has more dedicated resources and can do a better job for less compared with using in-house resources.
- **Data protection and data security is enhanced by the use of cloud providers**. A cloud provider manages all the security associated with the application, and the security element is built into the application, rather than a separate activity within the organization. It is important for organizations to be aware of the security and compliance certifications required in their industry, and to ensure their cloud service provider is properly credentialed.
- **More comprehensive business capability with SaaS.** This trend will continue as more business systems move to the cloud and more vendors offer cloud-based solutions.

All of these points hold true if the cloud provider is true to his word and offers the security functionality identified in this White Paper, ensuring product development in the cloud is no cause for concern.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1000 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For more than 48 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.988.7900
Twitter: @IDC
idc-insights-community.com
www.idc.com