Cloud Security Readiness Tool

Report created for

SecurityWeek

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Cloud Security Readiness Tool

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

Copyright © 2012 Microsoft Corporation. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Authors

Frank Simorjay
Microsoft Trustworthy Computing

Jeffrey Miller
Microsoft Server & Tools

Joanna Sharpe
Microsoft Trustworthy Computing

Jeff Jones
Microsoft Trustworthy Computing

Contributors

Tracey Ferriss
Microsoft Trustworthy Computing

Marc Lauricella
Microsoft Trustworthy Computing

Kathy Philips
Microsoft Legal and Corporate Affairs

Tim Rains
Microsoft Trustworthy Computing

Sian Suthers
Microsoft Trustworthy Computing

Brian Raffety
Engineering and Community Online

Jason Palmer
Alinean

Paul Henry
Wadeware LLC

Ariel Silverstone
Wadeware LLC

Steve Wacker
Wadeware LLC

Lori Koidahl
Warner Marketing

Introduction

The following report was generated for SecurityWeek to provide insight in a simple-to-read format for SecurityWeek's current IT-related issues. 27 common security, privacy, and reliability issues are explored, and-easy-to-follow recommendations are provided.

The questions were formed using objectives from the Cloud Security Alliance's Cloud Control Matrix (CCM).

The answers use a simplified structure to help SecurityWeek understand key control objectives for managing people, process, and technology issues. Each question or objective is provided in the following format:

- Control objective – An identified important issue that must be addressed in organizations that share information on the Internet.
    - Current state – Provides insight into current difficulties and issues that SecurityWeek is dealing with for the control objective.
    - Recommendation – When possible, a recommendation for improvement is provided. However, a recommendation may not be available for all objectives.
    - Advantage of moving to a SaaS solution – All objectives will be provided a means to use the advantages of a cloud service. This information will not include details on how to implement a cloud service, but why SecurityWeek should care about the cloud service.

Background

Cloud computing is a term that is broadly used to describe the shift of several traditional functions of an IT organization into utility-like services that are provisioned by a service provider. Computing power, storage space, and sometimes applications are made available by the service provider, who performs such functions such as purchasing servers and maintaining data centers, storage environments, and software.

The decision to deploy cloud computing is a strategic one. Many organizations are curious to learn more about their own IT environments and evaluate whether deploying cloud services is appropriate. The overarching consideration is often whether such deployment can be done in a secure manner and whether time, resource, and cost savings can be realized.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Throughout this document, it is essential to understand the roles and responsibilities of both cloud providers and customers. Providers can help reduce risks, but customers will need to ensure that data classification and security policies are in effect and that end-point protection solutions are in place. Customers are also responsible to ensure that they remain compliant with all their local statutory and regulatory obligations.

Figure 1. Cloud provider and customer responsibilities

Service providers should be transparent about how services are managed with security and privacy policies and practices designed to help mitigate customer risk. Customers can use the report to ensure they are asking relevant questions and setting appropriate expectations of cloud providers, and to better understand how they are meeting their own current compliance obligations.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

SecurityWeek's Considerations

Security policies and procedures

Current State

Security policies and an information security management system (ISMS) have been adopted to conform to industry best practices for information security, as defined by PCI DSS v2.0 or other standards.

Recommendation

The ISMS should be integrated with policies and systems for asset management, physical security, access control, and communications and should be updated regularly for operational effectiveness.

Advantage of moving to a SaaS service

A SaaS cloud solution will help you improve of your ISMS practices.

An ISMS is a set of policies that govern information security for an organization. PCI DSS v2.0 provides a model for creating, implementing, and maintaining an ISMS.

SaaS service providers will typically implement centrally managed information security plans that conform to industry best practices regarding security, privacy, and risk; and are integrated with asset management, physical security, and access control policies. Regular audits help ensure effectiveness and conformance. A customer version of the provider's ISMS may be made available to qualifying customers and prospective customers on request. .

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	12.1 Establish, publish, maintain, and disseminate a security policy 12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Security policies review process

Current State

Security policies are reviewed by management to ensure that security incidents can be managed in accordance with the current information security threat landscape.

Recommendation

Management should proactively review security policies. Security policies and the incident review process should be proactively reviewed by management in accordance with the current information security threat landscape.

Advantage of moving to a SaaS service

A SaaS cloud solution would provide improvement to your security.

SaaS service providers typically ensure that information security policies undergo a formal review and update process at regularly scheduled intervals. If a significant change is required in the security requirements, it may be reviewed and updated outside of the regular schedule.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	12.1 Establish, publish, maintain, and disseminate a security policy

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Security program updating

Current State

Implementing a security program with regular updates and including senior management review and approval process conforms to industry best practices for information security, as defined by PCI DSS v2.0 or other standards.

Recommendation

Segregation-of-duty principles should be used to separate production and non-production environments. Movement or copying of non-public data out of the production environment into a non-production environment should be expressly restricted.

Advantage of moving to a SaaS service

A SaaS cloud solution may provide significant improvements to the segregation of your important data and other assets.

Proper network segmentation is vital to ensuring the security of sensitive data. Data in non-production environments, such as test environments, is typically not subject to the same controls that production environments use to maintain data integrity. Data is often at risk of alteration or deletion. Even if a separate copy of production data is made for the non-production environment, it may not be subject to the same policies for data protection, retention, and disposal as production environments are and thus the data may be at increased risk of exposure to unauthorized parties.

A cloud solution will provide strict segregation of production and non-production environments in accordance with widely used technical and/or industry standards. Cloud providers typically have policies that prohibit the movement or copying of customer data from production to non-production environments without customer consent.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	12.1 Establish, publish, maintain, and disseminate a security policy

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Personnel background checks

Current State

There are no requirements to conduct background checks before hiring personnel with access to data. As a result, important assets may be at risk of loss, damage, or unauthorized disclosure.

Recommendation

Regular background checks should be conducted before hiring personnel and especially senior staff who will gain access to corporate data.

Advantage of moving to a SaaS service

A SaaS cloud solution would decrease the level of risk to your important information assets faced by personnel.

The human factor is one of the most important contributors to the success of an information security plan, but also presents one of the biggest risks. Malicious or disgruntled personnel with access to important information assets can be a significant threat to the safety and security of those assets. Even people without malicious intent can pose a danger if they don't clearly understand their information security responsibilities.

Cloud providers typically conduct regular pre-hire and post-hire background checks on their employees.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulation represent a sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Non-disclosure agreement requirements

Current State

Currently personnel are required to sign non-disclosure agreements (NDAs) as a condition of employment or access. However, these agreements are not managed centrally and may not have been reviewed by qualified legal experts recently. As a result, assets may be exposed to unnecessary risk.

Recommendation

NDAs should be vetted and kept current.

Advantage of moving to a SaaS service

A SaaS cloud solution would significantly reduce the risk of unauthorized access and disclosure of your data.

Many organizations require employees, contractors, and other associated parties to sign NDAs before gaining access to sensitive information or resources. These agreements are important tools for enforcing the confidentiality requirements for vital information assets.

Cloud providers usually maintain policies and procedures that define the implementation and execution of NDAs and confidentiality agreements. NDAs are centrally managed and audited at regular intervals, typically on an annual basis.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Access restriction by role

Current State

Physical access to data center environments are controlled through various security mechanisms and limited to authorized personnel whose identities can be verified. A required written request process has been implemented.

Recommendation

Physical access should be centrally managed and access permissions should be reviewed regularly.

Advantage of moving to a SaaS service

A SaaS cloud solution would provide improved physical security for your important data assets.

Maintaining physical security is one of the most important steps any organization can take to protect sensitive information assets. Cloud providers typically conduct operations in high-security facilities protected by a range of mechanisms that control access to sensitive areas. Common security mechanisms include doors secured by biometric or ID badge readers, front desk personnel who are required to positively identify authorized employees and contractors, and policies that require escorts and guest badges for authorized visitors.

Access is restricted by role. Authorizations for access are granted by a relatively small set of trusted staff members and are tracked using a ticketing/access system. A list of authorized personnel are reviewed and updated regularly.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Employee change/termination process

Current State

Revocation may be performed inconsistently or not at all when individuals and other parties separate or change their responsibilities at SecurityWeek.

Recommendation

A written process to remove or change access for employees who leave or are reassigned is needed.

Advantage of moving to a SaaS service

A SaaS cloud solution would provide access control enhancements to the security of your important information assets.

Controlling access is an important part of information security. Access to important systems, information assets, and data should be reviewed and revised in a timely manner upon any change of status of an employee, contractor, or other individual or entity with access. If unauthorized parties can access sensitive assets, the confidentiality, integrity, and availability of important information could be at risk.

Cloud providers usually maintain strict control over access to important systems. Managers and owners of SaaS applications and data are typically responsible for reviewing who has access on a periodic basis. Regular access reviews audits help ensure that appropriate steps are being taken to manage access. Control of access rights among employees and contractors of the customer organization itself remain the customer's responsibility.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	8.5.4 Immediately revoke access for any terminated users. 8.5.5 Remove/disable inactive user accounts at least every 90 days.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Physical security program

Current State

There is no formal plan for ensuring the physical security of sensitive information assets. Although most employees may represent that they have reviewed and agree to adhere to provided policies, the policies themselves are not enforced by significant physical security mechanisms. Access is free within a location.

Recommendation

Personnel should be required to positively identify authorized individuals, and all guests should be evaluated for admission based on job function.

Advantage of moving to a SaaS service

A SaaS cloud solution would provide significantly improved physical security for your important data assets immediately.

Maintaining physical security is one of the most important steps any organization can take to protect sensitive information assets. Only authorized personnel should have access to data center environments. If a malicious party gains unauthorized access to facilities housing sensitive data, hardware, and networking components, information assets could be subject to serious risk of disclosure, damage, or loss.

Cloud providers typically conduct operations in high-security facilities protected by a range of mechanisms that control access to sensitive areas. Common security mechanisms include doors secured by biometric or ID badge readers, front desk personnel who are required to positively identify authorized employees and contractors, and policies that require escorts and guest badges for authorized visitors.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. 9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible. 9.3 Make sure all visitors are handled as follows: 9.3.1 Authorized before entering areas where cardholder data is processed or maintained. 9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel. 9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration. 9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Equipment support contracts

Current State

A regular process for refreshing equipment exists. This process includes regular reviews of support contract needs and a budget forecasting, this effort should adhere to a capacity planning program.

Recommendation

The equipment refreshment strategy should be integrated with the organization's Disaster Recovery and Business Continuity efforts, as well as adheres to a capacity planning program.

Advantage of moving to a SaaS service

A SaaS solution would improve your service continuity management (SCM).

Keeping equipment up to date and in working order is essential for ensuring continuity of operations. Without current support contracts, obsolete or inoperative equipment can jeopardize the availability of important systems and information.

Cloud providers typically develop and maintain SCM processes that provide for continuity of operations and ensure ongoing security, compliance, and privacy protection. Equipment is refreshed regularly and all systems are kept current and operational. The process usually involves establishing alternate sites to be used in the event of failure of the primary service facility.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Data classification program

Current State

Asset classification is performed by individuals or groups, if at all, and may be inconsistent between different departments.

Recommendation

Sensitive data should be stored in an isolated workspace or share, with limited access.

Advantage of moving to a SaaS service

A SaaS cloud solution would provide your important data with significantly increased security through improved data classification.

Data classification, which involves associating each data asset with a standard set of attributes, can help an organization identify which assets require special handling to provide security and privacy protection.

Cloud providers typically classify data and other assets according to well-defined policies, which dictate a standard set of security and privacy attributes among others. Stores containing customer data are classified as sensitive assets requiring a high level of security, although customers usually retain responsibility for classifying their own data internally.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	9.7.1 Classify media so the sensitivity of the data can be determined. 9.10 Destroy media when it is no longer needed for business or legal reasons. 12.3 Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Data access policy

Current State

Access to data is granted upon request. Employees and contractors may not understand which information assets require protection and what they need to do to help protect information. As a result, important assets are at risk of loss, damage, or unauthorized disclosure.

Recommendation

There should be a written, followed process to grant access to data requiring, at a minimum, a signature in confirmation of reading the policy and agreement to comply. Personnel background checks should be run for senior staff.

Advantage of moving to a SaaS service

A SaaS cloud solution would immediately decrease the level of risk your important information assets face from malicious or untrained personnel.

The human factor is one of the most important contributors to the success of an information security plan, but also one of the biggest risks. Malicious or disgruntled personnel with access to important information assets can be a significant threat to the safety and security of those assets. Even people without malicious intent can pose a danger if they don't clearly understand their information security responsibilities.

Cloud providers typically treat security education as an ongoing process, and require their personnel to participate in regular security training and receive periodic security awareness updates when applicable. Employees and contractors are usually required to sign non-disclosure agreements (NDAs) as a condition of employment.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Data retention and recovery program

Current State

Data backup requirement for regular backing up of data has been implemented. However, the backups are not regularly tested for recoverability.

Recommendation

Recoverability of backed up data should be tested regularly to ensure that backed up data can be recovered in a timely manner.

Advantage of moving to a SaaS service

A SaaS cloud solution will provide significantly improved security against data loss.

A data backup and recovery plan defines the approach an organization takes to backup and to recover data in case of need.
Cloud providers typically maintain a data backup and recovery framework that is consistent with industry practices. A typical data backup and recovery plan assigns clear responsibilities to specific personnel and defines objectives for backup and recovery.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Regulation	Control details
PCI DSS v2.0	3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows. 3.1.1 Implement a data retention and disposal policy that includes: - Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements - Processes for secure deletion of data when no longer needed - Specific retention requirements for cardholder data - A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements 3.2 Do not store sensitive authentication data after authorization (even if encrypted). Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely. 9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually. 9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually. 9.6 Physically secure all media. 10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Data destruction

Current State

When electronic or paper records are destroyed, no special effort is taken to prevent recovery so sensitive data can potentially be exposed to unauthorized parties. It is up to the individual employee to decide whether, when, and how to destroy data.

Recommendation

Hard disk drives should be reformatted at the end of use, and paper documents should be destroyed in accordance with a data disposal policy.

Advantage of moving to a SaaS service

A SaaS cloud solution would provide immediate significant benefits for the confidentiality of your important data and other assets in the area of data disposal.

Strong policies that govern the proper disposal of electronic and paper records help prevent sensitive data from unauthorized disclosure. An effective data disposal policy provides guidance on how and where to dispose of data safely and securely, and provides users with the necessary tools for complying with the policy.

Electronic data stored by a cloud provider is typically subject to strong data disposal policies, derived from data classification programs that require disposed media to be destroyed or sanitized as outlined by a data retention and recovery program.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	3.1.1 Implement a data retention and disposal policy that includes: - Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements - Processes for secure deletion of data when no longer needed - Specific retention requirements for cardholder data - A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements 9.10 Destroy media when it is no longer needed for business or legal reasons as follows: 9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed. 9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed. 3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Staging to production requirements

Current State

Changes to the environment may not be adequately planned, tested, or documented.

Recommendation

Planned changes to the environment should be identified and documented in advance. A change management plan is in place and some systems are tested according to this plan.

Advantage of moving to a SaaS service

A SaaS cloud solution will significantly and immediately increase your system's reliability due to a planned change process in place.

An organization that lacks proper change management procedures creates unnecessary risk when deploying changes to a production environment. If new and modified systems are not adequately tested and validated before deployment, data can be unintentionally lost, altered, or disclosed.

Cloud providers use operational change control procedures for system changes. A typical control procedure is communicated to all parties who perform maintenance on the systems. It considers the following actions:

- Identification and documentation of the planned change
- An assessment process of possible change impact
- Change testing in an approved non-production environment
- Change communication plan
- Change management approval process
- Change abort and recovery plan (when applicable)

To ensure that the procedure itself is adequate and effective, management review and approval is typically required. Sufficient notice of potentially disruptive changes is provided with a several day advance notice before any planned maintenance is performed.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Application testing using customer data

Current State

Production and non-production environments may have access to the same data sources as the production environments, or may have access to copies of production data.

Recommendation

Production and non-production environments should be segregated. Movement or copying of non-public data out of the production environment into a non-production environment should be expressly restricted.

Advantage of moving to a SaaS service

A SaaS cloud solution would provide immediate protection benefits to your production data.

Production data should not be used or allowed to leak into non-production environments. Non-production environments, such as test environments, typically are not subject to the same controls that production environments use to maintain data integrity. Even if a separate copy of production data is made for a non-production environment, it may be at increased risk of exposure to unauthorized parties.

Cloud providers typically separate production and non-production environments in accordance with widely used technical and industry standards.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	6.4.3 Production data (live PANs) are not used for testing or development

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Asset inventory program

Current State

Assets inventory is recorded in a manual fashion. Asset management is handled on the department level, if at all, leading to inconsistent practices and inhibiting centralized security and lifecycle management policies.

Recommendation

There should be a process to manage assets according to a policy, with particular emphasis on protecting sensitive assets.

Advantage of moving to a SaaS service

A SaaS solution would provide you with improved information security through effective asset management.

Asset management makes it possible to keep track of important information about IT assets, including ownership, location, changes, and age. A comprehensive asset management program is an important prerequisite for ensuring that facilities and equipment remain secure and operational.

Cloud providers typically use formal asset management policies that require all assets to be accounted for and have designated asset owners. Asset owners are responsible for classifying and protecting their assets, and maintaining up-to-date information regarding asset management, location, and security. The provider maintains an inventory of major hardware assets used in the cloud infrastructure environment, and conducts regular audits to verify the inventory.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually. 12.3.3 A list of all such devices and personnel with access 12.3.4 Labeling of devices to determine owner, contact information and purpose

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Conducting risk assessments

Current State

Risk assessments are done to investigate and document the threats faced by SecurityWeek. Risk assessment help to mitigate, manage, and resolve identified risks.

Recommendation

Risk assessments should be conducted at least annually. Mitigation plans should be used to minimize the risk from identified threats and to recover critical business processes if a loss should occur regularly for all IT projects.

Advantage of moving to a SaaS service

A SaaS cloud solution may provide you with significantly improved information risk protection immediately.

Conducting a regular risk assessment can help an organization keep track of how sensitive data is stored and transmitted across applications, databases, servers, and networks. It aids compliance with defined retention periods and end-of-life disposal requirements; and helps protect data from unauthorized use, access, loss, destruction, and falsification.

Cloud providers typically conduct regular risk assessments that evaluate threats to the confidentiality, integrity, and availability of data and other assets under their control. Mitigation plans are used to minimize the risk from identified threats and to recover critical business processes if a loss should occur.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or athoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	12.1 Establish, publish, maintain, and disseminate a security policy

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Risk acceptance process

Current State

No enterprise risk management (ERM) framework is in place to manage risks. Risks are not measured.

Recommendation

An information risk management framework should be implemented that is built around a the concept of a “plan, do, check, act" (PDCA) approach as employed by PCI DSS v2.0and other well-known management system standards.

Advantage of moving to a SaaS service

A SaaS solution would provide you with significantly improved risk management capabilities for your important assets.

An information security plan is most effective when integrated with a larger information risk management framework.
Cloud providers typically use centrally managed information risk management frameworks built upon versions of the "plan, do, check, act" approach.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	12.1 Establish, publish, maintain, and disseminate a security policy

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Incident response program

Current State

Personnel are required to report security incidents promptly, according to documented policies, processes, and procedures.

SecurityWeek's personnel are aware of their responsibility to report all incidents in a timely manner through predefined communication channels.

Recommendation

Incident reporting processes should by regularly tested and updated.

Advantage of moving to a SaaS service

A SaaS cloud solution would help you improve incident response reporting for security incidents that put your important information assets at risk.

When a security incident occurs, proper and timely reporting can mean the difference between containing the damage and suffering a major breach or loss of important information assets. Effective response can only occur if information security events are reported to the appropriate parties promptly and clearly.

Cloud providers typically require their personnel to report any security incidents, weaknesses, and malfunctions immediately using well-documented and tested procedures.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	12.5.2 Technical review of applications after operating system changes.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Disaster recovery plan

Current State

There is no established business continuity program, which can expose your organization to security risks from disruptions.

Recommendation

Establishing a formal, approved and budgeted Disaster Recovery plan will ensure:

•Assignment of key resource responsibilities
• Notification, escalation and declaration processes
• Recovery time objectives and recovery point objectives

The plan also includes provisions for training and maintenance, and establishes a revision process system.

Advantage of moving to a SaaS service

A SaaS cloud solution will provide your important information assets with significantly improved availability in the event of a disruption.

A disaster recovery plan defines the approach and steps an organization will take to resume operations under adverse conditions such as natural disasters, attacks, or unrest.

Cloud providers typically maintain a disaster recovery framework that is consistent with industry practices. A typical disaster recovery plan assigns clear responsibilities to specific personnel; defines objectives for recovery; delineates standards for notification, escalation, and deceleration; and provides for training all appropriate parties.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Capacity planning program

Current State

A formal capacity or resource planning effort has not been run. Increased demand for resources may overtax critical systems and cause decreased availability of important assets.

Recommendation

A procedure needs to be implemented that will ensure resources are available when needed and provide usage forecasting and growth estimation efforts.

Advantage of moving to a SaaS service

A SaaS solution would provide significantly improved capacity and resource planning to help maintain the availability of your important information assets.

Effective capacity and resource planning are integral to ensuring the availability of information assets. This process attempts to anticipate and prepare for future resource needs to maintain system availability, and is therefore an important contributor to information security.

Cloud providers typically maintain operational processes for governing proactive capacity management based on defined thresholds or events. Hardware and software subsystem monitoring helps ensure acceptable service performance, CPU utilization, storage utilization, and network latency. A service health dashboard provides customers and prospective customers with quick web-based access to information about the availability of different cloud resources. Customers usually retain responsibility for monitoring and planning the capacity needs of their own applications and virtual resources.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Selecting data center locations

Current State

Equipment has been deployed at isolated locations within each facility, which are designed to provide protection against environmental risks. Data centers are located according to a risk avoidance plan, avoiding such areas known for tornadoes, earthquakes and other naturally avoidable risks when possible.

Recommendation

The data center should be located according to a risk analysis of related factors such as earthquakes or tornadoes. Within the data center, equipment should be placed according to its redundancy needs and factors such as physical access and fire exposure.

Advantage of moving to a SaaS service

A SaaS cloud solution may provide your important information assets with improved protection from environmental hazards.

Environmental hazards such as fire, vibration, and natural disasters can threaten systems that store and process important information assets. Whenever possible, these systems should be installed in locations with minimal exposure to these hazards.

Cloud providers typically place equipment in environments that have been specifically selected and engineered to protect the equipment from environmental risks such as fire, smoke, water, dust, vibration, earthquakes, and electrical interference.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. 9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually. 9.6 Physically secure all media. 9.9 Maintain strict control over the storage and accessibility of media. 9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Redundancy plan in case of utility service outages

Current State

The data center power systems is designed to be adequate for daily needs. The data center operations center monitors for power failures.

Recommendation

Data center power is monitored by a facility operations center to ensure continued operation. Power should be provided by dedicated uninterruptable power supplies (UPS) in the case of a limited power interruption event.

Advantage of moving to a SaaS service

A SaaS solution may provide your important data assets with improved availability through redundant systems.

Redundant systems provide continuity of operations in the event of a disruption. Without redundancy, a data center can become a single point of failure that threatens the normal operation of an organization.

Cloud providers typically have dedicated facility operations centers that monitor critical support systems like power. Power systems use dedicated 24x7 uninterruptible power supply (UPS) equipment and backup generators, and all critical electrical components are constantly monitored.

Power systems, including all critical electrical components – generators, transfer switch, main switchgear, power management module and uninterruptible power supply equipment.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	NA

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Patch management processes

Current State

Automated tools are used to manage patches and deployment. Security updates are tested and deployed, and critical patches are deployed as rapidly as possible.

Recommendation

Patches are automatically deployed in a regular, documented, timeframe after they become available. The environment is regularly scanned for vulnerabilities and tracked. Any vulnerabilities discovered should be quickly addressed with security updates or mitigations. Security updates should be tested and deployed when they become available. Critical updates should be deployed automatically by a trusted system.

Advantage of moving to a SaaS service

A SaaS solution would increase your protection from software vulnerabilities.

Malware outbreaks often begin when an attacker successfully exploits vulnerability in an operating system, application, or browser plug-in on a victim's computer. Most of these exploit attempts can be foiled by ensuring that security updates from the affected software vendors are quickly deployed, after they are published, to all computers across the IT environment.

Cloud providers typically use automated tools and procedures to scan systems for vulnerabilities, using the latest information available from software vendors and security experts. When vulnerabilities are discovered, mitigations and workarounds are applied to reduce the risk they pose to systems and data.

Regular vulnerability/penetration assessments are performed to identify possible vulnerabilities and verify that key logical controls are operating effectively. Security updates are tested to ensure that they do not pose a risk to important assets, then deployed as quickly as possible. Also regular compatibility testing is performed to protect against patching incompatibilities issues.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Regulation	Control details
PCI DSS v2.0	2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. 6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. 6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. 6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. 6.4 Follow change control processes and procedures for all changes to system components. 6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes. 6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks. 11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Antimalware/antivirus solution

Current State

An enterprise-wide selection and implementation of AV software from a reputable vendor has been deployed and is updated regularly.

Recommendation

A centrally managed enterprise AV solution should be used to deploy software to computers in SecurityWeek's environment and to keep them up to date with the latest signature files.

Advantage of moving to a SaaS service

A SaaS solution would provide you with increased protection from malicious software.

Deploying an effective antivirus software package from a reputable vendor and ensuring that it is kept up to date, is one of the most important steps any organization can do to defend against malicious software (malware) attacks.

Cloud providers typically run multiple layers of antivirus software from different vendors to ensure adequate coverage. Malware protection is often integrated into different workflows as appropriate. For example, the platform may be configured to automatically scan any files uploaded by end users or transmitted by email. In addition to the real-time protection this provides, scheduled scans are frequently performed to ensure that all systems remain free from malware.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). 5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. 5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Firewall protection solution

Current State

A stateful firewall should be implemented to isolate environments from each other and from other networks, following basic policies and procedures. The firewall should be managed and monitored to provide real-time protection against threats.

Recommendation

Segregation-of-duty principles should be used to separate production and non-production environments. Monitoring of activity should aggregate with a security information management system (SIMS).

Advantage of moving to a SaaS service

A SaaS cloud solution may provide significant improvements to the protection of your important data assets.

System and network environments should be separated by firewalls to protect and isolate sensitive data; meet business, customer, and security requirements; and comply with any relevant legislative, regulatory, and contractual requirements.

Cloud providers typically create multiple separate network segments with comprehensive firewall technologies to provide physical separation of critical back-end servers and storage devices from public-facing services. Monitoring is managed using a comprehensive data aggregation solution that can intelligently alert on critical issues.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	1.1 Establish firewall and router configuration standards 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment. 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

System time setting policies

Current State

Network Time Protocol (NTP) is used to synchronize system clocks throughout the environment.

Recommendation

For accurate reporting detail in event logging and monitoring processes and records, time should be synchronized with approved time sources.

Advantage of moving to a SaaS service

A SaaS cloud solution would provide immediate compliance benefits through the use of time synchronization.

Precise time synchronization is important for effective investigation of security events that affect multiple computers. Many regulation and best practices require that investigators be able to compare event log timestamps to determine the source of a security incident, such as a breach, or understand how a malware infection spreads to multiple computers. If the system clocks on the affected computers are not synchronized, reconstructing the sequence of events can be difficult or impossible, which can make responding to the incident much more difficult.

Cloud providers typically use Network Time Protocol (NTP) to regularly synchronize system clocks with a central, widely accepted time source.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved Model Version: 2 Report Version: V1.2

Control mapping

The following regulations represent sample control objective definitions. This list is not complete or authoritative, and should only be used as a discussion point to consider when moving services to a cloud solution. Control for SecurityWeek as a media / entertainment industry member should consider PCI DSS v2.0.

Regulation	Control details
PCI DSS v2.0	10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Conclusion

For SecurityWeek, decisions about how to gain the maximum benefits from cloud computing are important. These decisions are especially important in the Media / Entertainment sector, as other organizations are seeing the benefits of cloud computing and are harnessing this model in earnest – whether to take advantage of rapid deployment and provisioning or just for cost reduction. There are benefits to service delivery models as cloud computing becomes more agile and cost effective for organizations that want to optimize time, funds, and resources.

We hope SecurityWeek finds the **Cloud Security Readiness Tool** results useful and appreciate the opportunity to address some possible concerns around the successful deployment of cloud computing.

References for additional reading

- **Microsoft Trusted Cloud**
  - TwC trusted cloud
- **Trust Centers**
  - Office 365
  - Windows Azure
  - Dynamics
- **Related Links**
- Microsoft Global Foundation Services
- CSA Security, Trust & Assurance Registry (STAR Program)
- Microsoft Privacy in the Cloud Site
- Microsoft Privacy Information
- Trusted Cloud Frequently Asked Questions

Copyright ©2001-2012 Alinean, Inc. and Microsoft. All rights reserved

Microsoft

One Microsoft Way
Redmond, WA 98052-6399
microsoft.com/security