45% do not use standardized data classification

40% still use paper nondisclosure agreements (NDAs) and use them inconsistently

36% do not have a plan for responding to security breaches

34% do not have budgeted disaster recovery plans

33% do not have uniformly enforced security policies

24% have adequate policies and practices for secure data disposal

20% do not use roles to manage access

Security trends in public sector

Key findings and recommendations

Microsoft

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 Web site references, may change without notice. You bear the risk of using it.

Security trends in public sector

Public sector organizations today are learning that data and asset protection is becoming more complex because of regulations with which they must comply, such as the European Union Data Protection Directive (EUDPD), and the increasing demand for self-service solutions. Additional resources are needed, but there are consistent and constants pressures to reduce budgets. As a result, public sector organizations worldwide are considering additional cloud-based solutions to achieve cost savings while actually increasing services.

As for the need to comply with an increasing number of regulations, cloud computing can help improve the security profiles of public sector organizations by shifting the burden of assuring safe, secure computing practices to cloud service providers.

Although the cloud offers considerable benefits, organizations that plan to adopt cloud-based solutions can also benefit from having an understanding of the relative maturity of their own security practices. The security trends that are identified in this report result from anonymized data that was collected from 12,000 respondents to a survey that was conducted during the period of from November 2012 to February 2014. The trends are representative of a worldwide audience.

For more information, including worldwide results and tables from which the findings were created, see www.microsoft.com/trustedcloud.

Key Findings

33% of public sector organizations do not have uniformly enforced security policies

This condition may hinder these organizations' ability to enforce federal standards or guidelines effectively.

Recommendation

Public sector organizations should have centrally managed information security plans that conform to industry best practices regarding security, privacy, and risk.

Cloud service providers will typically implement centrally managed information security plans and will help ensure that they are integrated with asset management, physical security, and access control policies. Regular audits help ensure effectiveness and conformance.

40% of public sector organizations still use paper nondisclosure agreements (NDAs) and use them inconsistently

In addition, some organizations may not even require employees and vendors to sign NDAs. 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.

Recommendation

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 typically 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.

20% of public sector organizations do not use roles to manage access

Also, more than 26% of public sector organizations have only a generally accepted method of user access but no official procedure for terminated or reassigned employees.

Only 20% of public sector organizations have a written process that includes management accountability and verification of user access revocation when employees are terminated or reassigned.

Public sector organizations that do not use employee roles to manage user access to physical sites may allow inappropriate access to resources and create vulnerabilities.

Recommendation

Restrict access by role and also by need to know. Limit the number of people who can grant authorizations to a relatively small set of trusted staff members, and track authorizations using a ticketing/access system. Review and regularly update a list of authorized personnel.

45% **of public sector organizations do not use standardized data classification**

Also, only 12% of public sector respondents stated that they used standardized policies and that they proactively verify and enforce those policies.

These findings mean that secret and sensitive information may be misclassified or not classified at all. 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.

Recommendation

Organizations need to ensure that stores that contain confidential data are classified as sensitive assets that require an elevated level of security. Typically, organizations retain responsibility for classifying their own data internally.

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.

24% **of public sector organizations have adequate policies and practices for secure data disposal**

Also, only 16% of public sector organizations have written policies that require destruction records to be actually collected, practiced, and audited.

Recommendation

Public sector organizations should have strong policies that govern the proper disposal of electronic and paper records to 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 cloud providers is typically subject to strong data disposal policies that are derived from data classification programs and that require disposed media to be destroyed or sanitized as outlined by a data retention and recovery program.

36% **of public sector organizations do not have a plan for responding to security breaches**

Also, only 10% of public sector organizations operate using the "Black Swan" theory, which means that they test for the worst-case scenario, when reporting security incidents.

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.

Recommendation

For effective response, it's important to communicate that information security events need to be 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.

34% **of public sector organizations do not have budgeted disaster recovery plans**

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

Recommendation

A disaster recovery plan should be created that assigns clear responsibilities to specific personnel; defines objectives for recovery; delineates standards for notification, escalation, and deceleration; and provides for training all appropriate parties.

Cloud providers typically maintain a disaster recovery framework that is consistent with industry practices.

References for additional reading

http://microsoft.com/trustedcloud