72% do not have budgeted disaster recovery plans

51% do not have a plan for responding to security breaches

35% still use paper-based inventory or asset management solutions

32% are not effective at managing access

31% do not use role-based access control

29% increase capacity ONLY after there is a capacity shortage

Security trends in **retail organizations**

Key findings and recommendations

Microsoft

Trustworthy Computing

Security trends in retail organizations

In the last year, the security challenges that retailers face have become increasingly apparent. Regulations such as Payment Card Industry Data Security Standards (PCI DSS) identify the need to protect customer data, which mature retail organizations are well aware of. And yet worldwide security trends indicate that many retail organizations fall short in the area of safe, secure computing practices.

With 72% of shoppers expecting a seamless in-store to web experience,[1] it's not surprising that retailers are focusing on how to use new technologies to improve the shopping experience. Rapid adoption of supply chain management, web services, self-service portals, and customer relationship management (CRM) solutions have all contributed the kinds of key benefits that retailers are seeking. However, the rush to bring web experiences in line with the in-store experience can encounter issues when IT departments overlook key security concerns.

Cloud computing can help improve the security profiles of retail organizations by shifting the burden of assuring safe, secure computing practices to cloud service providers (CSPs). It's not a matter of retail organizations shirking responsibility, but of embracing it and doing the right thing for their customers.

Although the cloud offers considerable benefits, retail organizations that plan to adopt cloud-based solutions can benefit from having an understanding of the relative maturity of their own security practices and trends in their industry. The security trends 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 sample.

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

[1] Accenture. (2014, 1). *Top Trends in Retail: U.S. Seamless Retail Survey Results 2014.* www.accenture.com/us-en/Pages/insight-accenture-seamless-retail-survey-2014.aspx

Key Findings

31% of surveyed retail organizations do not use role-based access control

Retail organizations that do not use employee roles to manage user access may allow inappropriate access to resources and create vulnerabilities.

In addition, only 25% of retailers indicated they are logging and auditing access to secure areas based on policy and practice.

Also, more than 30% of retail organizations do not have the ability to revoke or change employee access when they are terminated or reassigned.

26% of all industries surveyed worldwide do not use role-based access control, which suggests that retail organizations (at 31%) are less mature in this regard.

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

Restrict access by role. 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.

Major CSPs typically conduct regular pre-hire and post-hire background checks on their employees.

32% of surveyed retail organizations are not effective at managing physical access

Failure to manage physical access could leave files or secure areas vulnerable, with no accountability.

30% of all industries surveyed worldwide do not effectively manage physical access, which suggests that retail organizations (at 32%) are less mature in this regard.

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

Recommendation

Only authorized personnel should have access to data center environments. 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.

CSPs typically conduct operations in high-security facilities that are protected by a range of mechanisms that control access to sensitive areas.

35% of surveyed retail organizations still use paper-based inventory or asset management solutions

In addition, only 5% have a formal policy to classify and manage assets that is regularly audited and that verifies inventory.

35% of all industries surveyed worldwide still use paper-based inventory or asset management solutions, which is about the same as retail organizations.

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.

Recommendation

Asset owners need to classify and protect their assets and maintain up-to-date information about asset management, location, and security.

CSPs typically use formal asset management policies that require all assets to be accounted for and have designated asset owners. A typical CSP maintains an inventory of major hardware assets used in their cloud infrastructure environment, and conducts regular audits to verify the inventory.

51% of surveyed retail organizations do not have a plan for responding to security breaches

This finding may indicate that the organizations have never conducted a worst-case scenario analysis, and that they only take action when it's absolutely necessary.

40% of all industries surveyed worldwide do not have a plan for responding to security breaches, which suggests that retail organizations (at 51%) are less mature in this regard.

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.

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

72% of surveyed retail organizations do not have budgeted disaster recovery plans

This finding indicates that retail organizations have a basic understanding of the need for disaster recovery plans but don't fully appreciate how disastrous occurrences could affect the ability of the organization to function.

35% of all industries surveyed worldwide do not have budgeted disaster recovery plans, which suggests that retail organizations (at 72%) are less mature in this regard.

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.

CSPs typically maintain disaster recovery frameworks that are consistent with industry practices.

29% of surveyed retail organizations increase capacity ONLY after there is a capacity shortage

This condition may result in significant downtime because of unexpected capacity needs during times of increased retail activity (for example, during the holidays, special promotion or an advertising push).

31% of all industries surveyed worldwide are not effective at capacity planning, which suggests that retail organizations (at 29%) are more mature in this regard.

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.

Recommendation

Organizations need to be responsible for monitoring and planning the capacity needs of their own applications and virtual resources.

CSPs 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. Service health dashboard can provide customers and prospective customers with quick web-based access to information about the availability of different cloud resources.

References for additional reading

TwC Trusted Cloud
http://www.microsoft.com/twcloud

Aligning the Microsoft SDL with PCI DSS/PCI PA-DSS Compliance Activity
www.microsoft.com/en-us/download/details.aspx?id=16853