

 **38%** do not have budgeted disaster recovery plans

 **37%** do not use standardized data classification

 **29%** do not have a plan for responding to security breaches

 **23%** have adequate policies and practices for secure data disposal

 **22%** have not established a formal risk management program

 **21%** are not effective at managing physical access

 **20%** do not use roles to manage access

# Security trends in **financial services**

## Key findings and recommendations

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.

Microsoft is a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Copyright © 2014 Microsoft Corporation. All rights reserved.

# Security trends in financial services

Information technology (IT) landscapes in worldwide enterprise banking and financial organizations are changing rapidly, in part because of the finding that more than 75% of customers are willing to switch to another financial institution if it offers better technology.<sup>1</sup> As a result, banking and financial organizations are working to provide increasingly tech-savvy users with solutions that use newer technologies. In addition, banking and financial organizations are using the cutting-edge capabilities of social media to help increase their market share. These factors require close attention to developing IT capabilities and a good understanding of key financial regulations, such as Sarbanes-Oxley (SOX); one study suggests that between 30% and 50% of financial organizations are spending their discretionary IT budgets on regulatory compliance.<sup>2</sup>

Cloud computing can help improve the security profiles of financial organizations by shifting the burden of assuring regulatory compliance and minimizing risk to cloud service providers (CSPs). Although the cloud offers considerable benefits, organizations that 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 sample.

For more information, including worldwide results and tables from which the findings were created, see [www.microsoft.com/trustedcloud](http://www.microsoft.com/trustedcloud).

---

<sup>1</sup> 2014 Forecast: Tech Trends in Commercial Banking - [www.channelpronetwork.com/article/Top-Cloud-Trends-in-the-SMB](http://www.channelpronetwork.com/article/Top-Cloud-Trends-in-the-SMB)

<sup>2</sup> Market Trends: Banking, Worldwide 2014 (PDF) [www.luxoft.com/upload/iblock/36c/market\\_trends\\_banking\\_worldw\\_gartner.pdf](http://www.luxoft.com/upload/iblock/36c/market_trends_banking_worldw_gartner.pdf)

# Key Findings

## 20% of surveyed financial organizations do not use role-based access control

Financial organizations that do not use employee roles (such as administrator, user, and guest) to manage access may allow unlawful access to resources and create vulnerabilities.

26% of all industries surveyed worldwide do not use role-based access control, which suggests that financial organizations (at 20%) are more mature in this regard.

In addition, 38% of responses indicate that financial organizations are logging and auditing user access based on proper policy and practice.

Almost 20% of financial organizations do not have the mechanisms, policies, or procedures to revoke or change employee access when they are terminated or reassigned, which is the same percentage as the worldwide industry average.

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 and also by need to know. Restrict 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.

## 21% of surveyed financial organizations are not effective at managing physical access

This lack of ability to manage physical access may leave secure files and rooms vulnerable, with no accountability.

30% of all industries surveyed worldwide are not effective at managing physical access, which suggests that financial organizations (at 21%) are more mature in this regard.

Maintaining up-to-date physical access control 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 and 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 protected by a range of mechanisms that control access to sensitive areas. Using such a CSP might help reduce the cost of managing on-premises data centers.

**37%** of surveyed financial organizations do not use standardized data classification

This finding suggests that secret and sensitive information may be misclassified or not classified at all.

42% of all industries surveyed worldwide do not use standardized data classification, which suggests that financial organizations (at 37%) are more mature in using data classification.

Standardized 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 data stores that contain customer data are classified as sensitive assets that require an elevated level of security.

CSPs typically classify data and other assets according to well-defined policies, which dictate a standard set of security and privacy attributes among others.

**23%** of surveyed financial organizations have adequate policies and practices for secure data disposal

Also, in more than 14% of banking organizations, individual employees are expected to perform their own document retention and backup functions, without a formal policy or procedure, which could potentially lead to data retention violations.

31% of all industries surveyed worldwide have adequate policies and practices for secure data disposal, which suggests that financial organizations (at 23%) are less mature in this regard.

An effective data disposal policy provides guidance on how and where to dispose of data safely and securely, and helps to provide users with the necessary tools for complying with the policy.

### **Recommendation**

Organizations should have a data backup and recovery plan that defines an approach to back up and to recover data in case of need. A typical data backup and recovery plan assigns clear responsibilities to specific personnel and defines objectives for backup and recovery. Also, strong policies that govern the proper disposal of electronic and paper records help prevent sensitive data from unauthorized disclosure.

CSPs typically maintain a data backup and recovery framework that is consistent with industry practices. In addition, 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.

**22%** of surveyed financial organizations have not established a formal risk management program

Also, the same 22% most likely only conduct risk assessment when an incident occurs.

27% of all industries surveyed worldwide have not established a formal risk management program, which suggests that financial organizations (at 22%) are more mature in this regard.

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

### **Recommendation**

Organizations should have an information security plan. Such plans are most effective when they are integrated with a larger information risk management framework.

CSPs typically conduct regular risk assessments that evaluate threats to the confidentiality, integrity, and availability of data and other assets under their control; they typically use centrally managed information risk management frameworks.

**29%** of surveyed financial organizations do not have a plan for responding to security breaches

This finding may imply that the same 29% of organizations have never conducted a worst-case scenario test, and that they only take action when it's mandated that they do so.

40% of all industries surveyed worldwide do not have a plan for responding to security breaches, which suggests that financial organizations (at 29%) are more 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 incident 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.

**38%** of surveyed financial 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.

35% of all industries surveyed worldwide do not have budgeted disaster recovery plans, which suggests that financial organizations (at 38%) are less mature in this regard.

### **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.

## References for additional reading

### **TwC Trusted Cloud**

<http://www.microsoft.com/twcloud>

### **Aligning the Microsoft SDL with PCI DSS/PCI PA-DSS Compliance Activity**

<http://go.microsoft.com/?linkid=9762341>

### **Microsoft Security Development Lifecycle Adoption: Why and How (PDF)**

<http://aka.ms/D5akge>