51% conduct system-wide data backups that are tested regularly

39% do not use standardized data classification

31% have a disaster recovery program

28% do not have asset management policies and conduct asset discovery manually

25% have ineffective controls for removing or changing access when employees leave or are reassigned

23% have immature security policies

23% cannot prevent a power outage from affecting their organization

Security trends in **healthcare**

Key findings and recommendations

Microsoft

Trustworthy Computing

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.

Security trends in healthcare

The worldwide need for quick access to meaningful medical information is an increasing challenge for healthcare organizations. Almost 50% of hospitals and 40% of ambulatory practices are implementing self-service portals,[1] and a 75% increase in medical cybercrime over the course of two years[2] has increased concerns about security—because more self-service capabilities may increase opportunities for criminals to find new ways of stealing sensitive medical information through drive-by download and phishing attacks.

Cloud computing can help improve the security profiles of healthcare organizations by shifting to cloud service providers (CSPs) the burden of assuring safe, secure computing practices. CSPs strive to maintain secure operations and will work with healthcare providers to help minimize security threats. In addition, CSPs that work with electronic health records (EHRs) must abide by stringent regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the US, to ensure data is securely maintained. In short, cloud-based solutions could address the needs of medical practitioners while reducing or mitigating risk.

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 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.

[1] Terry, K. (2013, 12 23). *5 Trends For Health CIOs In 2014* - www.informationweek.com/healthcare/mobile-and-wireless/5-trends-for-health-cios-in-2014/d/d-id/1113133

[2] D., Gary R. Gordon Ed (2013, 07). *The Growing Threat of Medical Identity Fraud: A Call to Action* (PDF) - http://medidfraud.org/wp-content/uploads/2013/07/MIFA-Growing-Threat-07232013.pdf

Key Findings

23% of surveyed healthcare organizations have immature security policies

This condition may result in major breaches of regulatory requirements and may hinder an organization’s ability to enforce procedures.

34% of all industries surveyed worldwide do not have effective security policies, which suggests that healthcare organizations (at 23%) are more mature in this regard.

Recommendation

Healthcare organizations should have centrally managed information security policies that conform to industry best practices with regard to security, privacy, and risk management.

CSPs will typically implement such policies and will help ensure that they are integrated with asset management, physical security, and access control policies. Regular audits help ensure effectiveness and compliance.

26% of surveyed healthcare organizations have ineffective controls for removing or changing access when employees leave or are reassigned

Without management accountability, terminated or reassigned employees can maintain unauthorized access.

31% of all industries surveyed worldwide have ineffective controls for changing access when employees leave or are reassigned, which suggests that healthcare organizations (at 26%) are more mature in this regard.

In addition, 26% of healthcare organizations do not centrally manage, log, and audit physical access to facilities. Even with role-based key cards, without logging and auditing access, healthcare organizations may risk unauthorized entry into sensitive areas.

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. 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.

39% of surveyed healthcare organizations do not use standardized data classification

Some organizations have policies for personally identifiable information (PII) but lack procedures or standard terminology that adequately protect patient information while allowing providers the ability to get their jobs done.

42% of all industries surveyed worldwide do not use standardized data classification, which suggests that healthcare organizations (at 39%) are more mature in this regard.

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 confidential 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.

52% of surveyed healthcare organizations conduct system-wide data backups that are tested regularly

Also, almost 27% of healthcare organizations expect individuals to be responsible for ensuring the correct means of disposal of sensitive data.

49% of all industries surveyed worldwide conduct system-wide data backups that are tested regularly, which suggests that healthcare organizations (at 52%) are more mature in this regard.

A data backup and recovery plan defines the approach an organization takes to back up and to recover data in case of need.

Recommendation

Organizations should have a data backup and recovery plan that 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. 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.

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

28% **of surveyed healthcare organizations do not have asset management policies and conduct asset discovery manually**

34% of all industries surveyed worldwide do not have effective asset management policies, which suggests that healthcare organizations (at 28%) are more mature in this regard.

In addition, only 42% of healthcare organizations self-identified themselves as mature in their use of asset management policies to protect assets such as equipment, pharmaceuticals, and patient records.

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.

31% of surveyed healthcare organizations have a disaster recovery program

Also, only 24% regularly test their disaster recovery site, which puts them at potential risk for untimely interruptions.

35% of all industries surveyed worldwide do not have disaster recovery programs, which suggests that healthcare organizations (at 31%) are more 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.

23% of surveyed healthcare organizations cannot prevent a power outage from affecting their organization

Redundant systems provide continuity of operations if a disruption occurs.

26% of all industries surveyed worldwide cannot prevent a power outage from affecting their organization, which suggests that healthcare organizations (at 23%) are more mature in this regard

Without redundancy, a data center can become a single point of failure that threatens the routine operations of an organization.

Recommendation

Power systems should use dedicated 24x7 uninterruptible power supply (UPS) equipment and backup generators, and all critical electrical components should be constantly monitored. Power systems include all critical electrical components, including transfer switches, main switchgear, and power management modules.

CSPs typically have dedicated operations center facilities that monitor critical support systems like power.

References for additional reading

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

Secure Software Trends in Healthcare (PDF)
http://aka.ms/SDLHealthcare