EXECUTIVE BRIEF

MITIGATING SECURITY THREATS OF INSIDERS LEAKING DATA

- Insights for busy professionals
- Read in less than 10 mins
- Knowledge without the fluff

Underwritten by:

insight brief
RESEARCH. DISCOVERY. INSIGHTS.

quocirca

This Executive Brief is a summary of the white paper: What keeps your CEO up at night? The insider threat: solved with DRM

IMPORTANT DATA

- IT security is changing as more and more data leaks are instigated by legitimate users.
- Most data leaks incidents by insiders are accidental. Purposeful data breaches are most frequent by employees changing employers, employees seeking financial gain, internal spying and vengeful employees.
- Data sharing controls are becoming more and more necessary as online tools increase in number.
- Security systems including firewalls, data loss prevention and identity and access management have gaps and none are designed to secure data from internal threats.
- Data security with a digital rights management system (DRM) mitigates internal threats, is scalable and readily accepted by employees.
- A digital rights management system monitors and tracks document and data creation, access and document changes.
- Areas of IT security causing the greatest concern and keeping CEOs awake at night are viruses, data loss and hacking but insider threats are reported to be one of greatest concerns by over 20% respondents to a survey.
- Measuring actual data breach incidents as opposed to perceptions, research indicates over 40% involve insiders. More than half of actual data loss is due to insiders.
- Carelessness and ignorance of insiders leading to data breaches can be controlled by training, discipline and technological safeguards.
- 70% of malicious thefts of intellectual property - commonly customer and financial data - are committed within 30 days of an employee leaving a job.
- A survey revealed that 1 in 8 IT security professionals retained credentials to access a former employer's system.
- The increase in channels used to share documents including cloud based services means there is more likelihood that documents and data will end up in the wrong hands.
- The most common way employees steal documents is via Email. A growing danger is content sharing via social media.
- On-line document storage services such as Apple iCloud, Dropbox, Amazon Cloud Drive and Google Drive are often used by employees to back up and access confidential material.
- A study of security breaches indicates that 6% of insider thefts involve copying on a USB device and 26% are carried out via print.

IMPORTANT DATA (CONTINUED)

- A recent survey revealed that the vast majority of insider data threats come from non-technical employees, contractors, IT administrators, IT service providers and partners, customers and suppliers with legitimate access.
- Data access and usage policies are reported to have been implemented in only half of organizations responding to a survey. If a policy is in place it must be policed to prevent misuse of data.
- According to one survey only 47% of organizations have staff training programs dealing with security.
- Research indicates that about 40% of organizations have digital right management systems (DRM) of one sort or another. Commonly a DRM system is used only for the most sensitive data but as it is scaleable it should be used across a business to encompass all users of classified documents.
- The range of file types supported by the latest digital rights management systems is growing and now includes all popular office suites.
- Digital rights management is only intrusive for those breaching security for the remainder of employees the system is transparent when used with office suites.

TAKEAWAYS

- Identity and access management and user authentication do not prevent misuse of data. Theft of identification credentials is a common way for unauthorized access to data.
- Host based security does nothing to prevent misuse of data once it leaves the security perimeter. System level security does not adequately address insider threats.
- Network traffic inspection and data loss prevention only checks data when it is in motion not as it is used on a device or in storage.
- Encryption of data is only useful when data is stored. For data to be used it must be decrypted by insiders with right of access. Once decrypted, data can be shared in many ways from screenshots to printing.
- A digital rights management system is the only comprehensive technology that is designed to mitigate data misuse and theft by insiders.
- Security using a DRM system does not imply mistrust of employees. Many breaches in data security are inadvertent mistakes by insiders.
- A DRM system classifies every file and monitors it through its use creating an audit trail. It prevents simultaneous on-line activity on a device when a classified document is present. Offline activities are monitored when a classified document is present on the device.
- With a digital rights management system a pattern of data usage can be established for every user. Deviation can be investigated.
- DRM system audit trails for sensitive files include user identification, time stamps and actions carried out on the file.

SUMMARY TREND

- As more organizations come to recognize internal threats to data security the effectiveness of traditional security technologies are being questioned. There is a trend to turn to the superior protection provided by digital rights management systems.n.

DEFINITION

- Enterprise DRM (digital rights management) shares DRM's basic concept of controlling content use. However, it goes beyond unauthorized-copy protection to help stop sensitive information from being read, altered, or shared outside an origination -- while not interfering with users' work, including their ability to collaborate with colleagues.

CLICK TO ACCESS THE FULL WHITE PAPER

Share this document

Click or scan to access the full white paper

Click to access the full white paper

NOTE: *The original Quocirca white paper, 'What keeps your CEO up at night? The insider threat: solved with DRM' was sponsored by Fasoo, an EDRM (Enterprise Digital Rights Management) solutions provider, with industry leading solutions and services. However, all Quocirca content is written from an independent standpoint and addresses the issues with regard to the use of IT within the context of an organisation, rather than specific products.*

quocirca

Quocirca is a research and analysis company with a primary focus on the European market. Quocirca produces free to market content aimed at IT decision makers and those that influence them in business of all sizes and public sector organisations. Much of the content Quocirca produces is based on its own primary research.

ABOUT INSIGHTBRIEF

Our team produces short documents for busy professionals, summarising longer reports and research papers so that readers can swiftly become acquainted with a large body of knowledge and decide whether or not to read the full source document(s).

We vet and qualify reports for relevancy and value to its intended audience before creating an InsightBrief document. Our editorial team is independent from the originator of the report, ensuring that the insights exclude sales or vendor centric messaging, thereby creating real value for our time-poor readers.