secRMM

Security Removable Media Manager

Whitepaper- Finance

OVERVIEW. Financial Institutions and creditors who are subject to administrative enforcement by the Federal Trade Commission ("FTC") have the duty to detect, prevent, and mitigate identify theft.[1] Included in this requirement is to establish an identity theft prevention program that is appropriate to the size, complexity, nature and scope of the financial institution or creditor. [2] The passing of the Gramm-Leach-Bliley Act, set forth additional standards for developing, implementing, and maintaining reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information by all financial institutions over which the FTC has jurisdiction.[3] The additional standards include the design and implementation of controls over risks of disclosure and regular tests monitoring the effectiveness of the controls, systems, and procedures.[4]

It is within the nature of financial institutions business to keep large internal networks of personal and sensitive information. Employee mismanagement of this information through writing it to unauthorized removable media not only could cause legal liability, but also a potential loss of "good-will" and future business. secRMM allows organizations to evaluate and adjust their removable media information security program to their specific security needs. The event log and the exact source file will show who and what an individual is writing to removable media. By secRMM providing the source file, organizations will have the capability of determining what exact files are being pulled from your network. This allows organizations to adjust their security program in light of monitoring to ensure that there is no material impact on sensitive information located on their network.

---

[1] Duties regarding detection, prevention and mitigation of Identity theft, 16 C.F.R. §681.1.

[2] *Id*.

[3] See 16 C.F.R. 314.1

[4] 16 C.F.R. 314.4(c)

secRMM BENEFITS TO FINANCIAL INSTITUTIONS…

SecRMM HELPS SATISFY REQUIRED SECURITY GUIDELINES. The following is a list of procedures that secRMM satisfies with respect to the Interagency Guidelines Establishing Information Security Standards to protect data (as to removable media):[5]

1) Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;
2) Detection of unauthorized individuals gaining access to customer information systems;
3) Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;
4) Intrusion detection system to alert of possible attacks on computer systems that store customer information;
5) Rapid and accurate determination of possible intrusion of private information.

ADDING secRMM TO FINANICAL INSTITUTIONS SECURITY RESPONSE PROGRAM. The FTC recommends a financial institution to develop and implement a response program as part of its information security program. The response program should address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. secRMM addresses the following key components of an effective response program (with respect to removable media);

1) Assesses the nature and scope of a potential incident and identifies what customer information has been accessed or misused; AND
2) Allows for effective measures to contain and control an incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence.

Risk assessment is an ongoing process requiring the continued review of policies and procedures to make certain adequate safeguards of customer information has taken place. secRMM's log of attempted and actual write activity provides solid factual information for financial institutions to determine where current sensitive data is being held, what work stations are writing the information, and if there needs to be further authorization considerations due to unauthorized access.

SIMPLE AUTHORIZATION MODULES. secRMM provides simple authorization modules for organizations to control the who/what/where/when/how of data being written from their network to removable media. Unlike other competing solutions, secRMM lets organizations control what files the end-user can copy from both the local computer and the network. Additional functions allow for the control of removable media write activity based on userid, removable media serial number, removable media internal IDs (i.e. VIDs and/or PIDs) and the program that is being used to perform the write operations. The solution can also prevent unauthorized devices from mounting to the Windows Operating System. When an individual try's to perform an unauthorized copy or mount secRMM logs the event. This enables organizations to further investigate why the user was attempting to perform that activity and helps stop future potential breaches.

CONTINUED USE OF "BRING YOUR OWN DEVICES" ("BYODs") WITH SECURITY. With the increasing use of BYODs organizational networks cannot be adequately secure without procedures in place to limit/prevent write activity or monitor the who/what/where/when/how of files being written. secRMM is the only solution capable of providing source file names for write operations to virtually all removable media- smart phones (iPhone, Blackberry, Windows, Android, etc.), tablets, USBs, and CD/DVDs. This allows organizations to easily and centrally evaluate activity being performed on endpoint terminals. secRMM provides for effective assessment of potential risks by monitoring and collecting detailed forensic data about removable media write activity or even attempted write activity.

ADDED PROTECTION TO ENCRYPTION TECHNOLOGY. secRMM works seamlessly with hardware/software encryption technologies to generate security events which informs a system administrator when an encrypted device has been mounted, and whether authorization was granted.

INTEGRATED WITH MICROSOFT SYSTEM CENTER SUITE OF PRODUCTS. secRMM is tightly integrated with the Microsoft System Center suite of products; including System Center Configuration Manager ("SCCM"), System Center

[5] ¶III.C.1.a-h of the Security Guidelines.

Operations Manager (“SCOM”), SCOM Audit and Collection Services (“ACS”), and System Center Orchestrator. This allows the system administrator to set up alerts, notifications, tasks, reports, and can optionally generate SNMP traps, among other desirable capabilities.

COMPLETE SOURCE PATH. secRMM is the only Data Loss Prevention (“DLP”) software capable of capturing the complete source path of a file being copied to a removable media storage device.

secRMM DOES NOT REQUIRE ITS’ OWN FRAMEWORK. secRMM easily integrates into the enterprise management framework organizations are currently using. This makes secRMM particularly cost effective compared to other solutions. secRMM accomplishes this by utilizing the base Windows Operating System components. Furthermore, secRMM is completely functional within the Windows Event Log and the base Microsoft Management Console (“MMC”). Given these efficiencies Squadra is able to provide the software at *affordable pricing*.

Squadra Technologies
7575 West Washington Ave.
Suite 127-252
Las Vegas, NV 89128
+1 (760) 846-6844

For More Information Contact:
info@squadratechnologies.com

Free Trial Download Visit:
www.squadratechnologies.com