# Data Protection for Shared Services

## Part Three: The Core Elements of Your Shared Services Data Protection Program

May 2017

Smart. Focused. Done Right.®

scottmadden
MANAGEMENT CONSULTANTS

# The Core Elements of Your Shared Services Data Protection Program

## INTRODUCTION

A shared services data protection program can mitigate data security risks with policies, procedures, and controls that monitor, detect, and even block inadvertent or intentional data transmissions throughout the Shared Services Organization (SSO). These solutions can prevent distribution or leakage of sensitive data, saving your organization from the expense and reputational damage of a breach. Using the results of the data risk assessment described in Part Two of this series, you can identify and implement the security measures your organization needs to form the foundation of a shared services data protection program.

## Implement Program Controls

Establish data protection controls to provide the appropriate level of security for your sensitive data. These controls will also define the practices for responses to potential data leakage incidents.

### Establish Data Protection Requirements

Your data protection policies must cover data throughout the lifecycle—in use, in transit, and in storage. These policies must ensure the following:

- Data being used is secure
  - Users can only access and use sensitive data on encrypted or secured media
  - High-profile data is not permitted to be copied or moved to less-secure areas
  - Printing of sensitive data is restricted to designated users and to secure printers
  - Endpoint encryption is utilized on all computers regularly accessing sensitive data
  - Access to sensitive data is periodically monitored to ensure there are no unauthorized users
- Data being transferred is safe
  - Integrations within SSO applications are secured in a manner consistent with their assessed risk
  - Sensitive data should not be transmitted over email as it can be forwarded to individuals without appropriate permissions
  - Data transfers between users are carried out only through secure means and cannot be done via instant messaging, social media, cloud-based tools, personal emails, or USB drives
- Data being stored is protected
  - Shared drives are encrypted throughout the SSO infrastructure

- All devices storing sensitive data have robust security through password protections and remote access restrictions
- Access permissions are in place, defining user privilege levels and ensuring that sensitive data is accessed only by authorized individuals
- Storage and usage of personally identifiable information and other sensitive information is inventoried and reduced

### Develop Data Protection Practices

Your data protection program would be incomplete without practices related to incident response, incident reporting, and escalation. The practices must also include monitoring adherence and continuously improving your policies, as well as conducting extensive user education programs.

- **Monitoring.** Continuous improvement of policies and procedures relies on the ability of the SSO to monitor compliance with requirements. Monitoring is an intrinsic responsibility of every manager in a SSO. Some SSOs have even created a position dedicated to monitoring the security of the SSO information ecosystem and its established policies and procedures
- **Triaging.** The first step when an issue is identified is triaging the incident. The SSO leadership team analyzes the type of data leaked, who leaked it, and how it was leaked. If the incident is a genuine data loss threat, the SSO leadership notifies the enterprise information security team
- **Incident Reporting and Escalation.** The data loss incidents posing genuine threats are carefully investigated by the security team in collaboration with the SSO leadership. Based on the nature of the data breach, the security team will typically conduct a detailed analysis and provide a review and recommended actions to the leadership
- **User Education.** User education within the SSO needs to be an ongoing activity to constantly promote a security-savvy culture, while minimizing mistakes in data usage. User resistance and policy ignorance are the most difficult obstacle for data protection, as the procedures may be perceived as intrusive or inefficient

### Choose the Right Technology

Technology solutions can be used to augment the data protection policies and procedures. These technologies are commonly referred to as Data Loss Prevention (DLP) solutions. An appropriate DLP product can accurately detect your sensitive data within the complete data lifecycle and provide centralized management of the technical policies.

- **Data Detection Capability.** In a DLP system, detecting sensitive data accurately is vital—it helps detect potential data loss incidents with minimal false positives/negatives. To detect the data accurately, a DLP solution should have deep content analysis capabilities for both structured and unstructured data
- **Comprehensive Coverage.** The DLP product should cover the complete range of data leakage possibilities, including data moving through the network (data in motion), stored data on servers and workstations (data at rest), and data at the endpoint level (data in use). For example, for data at rest, these solutions typically include discovery tools that are designed to seek and find sensitive information on any storage medium, including laptops, desktops,

file servers, databases, email repositories, web content, or within applications. The DLP product capabilities should include disk encryption, access and permission control, and data wiping (when faced with potential data loss threats)

- **Central Policy Management.** DLP should include an easy-to-use central management server for administering enforcement and detection points, creating and administering policies, incident workflow, and reporting
- **Compatibility.** When choosing a DLP product, you should make sure that the DLP product can be integrated with your current technical environment and support the data formats used to store data in your business environment

## TAKEAWAYS

- Establish data protection policies and procedures that cover the lifecycle of data throughout the complex SSO information ecosystem, including data in use, at rest, and in transit
- Conduct extensive user education and awareness on a regular basis to instill a security culture in your organization
- Support the selection of an appropriate data protection solution to enhance the monitoring, detection, and even blocking of inadvertent or intentional data transmissions throughout the system

## SUMMARY

SSOs are both attractive and vulnerable to cyber criminals because of the sensitive and personal data they handle. Given how often data breaches occur, and the cost associated with them, data loss prevention programs are no longer optional.

Consider consulting with a SSO data protection expert, such as ScottMadden. While you can cover considerable groundwork on your own, a partner who knows both shared services and data protection can bring a different perspective and ensure nothing has been overlooked.

## HOW SCOTTMADDEN CAN HELP

ScottMadden can help you understand and resolve your shared services security issues by improving how you manage and govern cybersecurity. We provide a strategic, outcome-driven approach customized to your organization’s needs that entails four key actions: (i) identify the biggest security risks for your operation; (ii) assess the appropriate risk response; (iii) establish success measures for your security program; and (iv) determine how best to get you to the desired state.

ScottMadden is recognized as a shared services expert. We understand shared services operations, their risks, and the security practices that work best in these environments. Leveraging institutional knowledge and expertise, our experts can help you achieve your shared services security goals.

Please visit www.scottmadden.com to learn more about the services we offer.

## ABOUT SCOTTMADDEN'S CORPORATE & SHARED SERVICES PRACTICE

ScottMadden has been a pioneer in corporate and shared services since the practice began decades ago. Our Corporate & Shared Services practice has completed more than 1,500 projects since the early 90s, including hundreds of large, multi-year implementations. Our clients span a variety of industries from entertainment to energy to high tech. Examples of our projects include business case development, shared services design, and shared services build support and implementation.

## ABOUT THE AUTHORS

Jon Kerner (jkerner@scottmadden.com), partner and information technology practice area lead, Henry Bell (henrybell@scottmadden.com), director, Harold Lewis (hlewis@scottmadden.com), manager, and Jonathan Harb (jonathanharb@scottmadden.com), senior associate, are located in the Atlanta office. Talha Sheikh (tsheikh@scottmadden.com) is a senior associate in the Raleigh office.

## SOURCES

- ScottMadden Research and Expertise
- 2016 Data Breach Investigations Report, Verizon, 2016: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
- SNL Financial, SNL.com, March 2016
- *2016 Cost of Data Breach Study: Global Analysis*, Ponemon Institute LLC, June 2016
- *Data Loss Prevention*, SANS Institute, August 2008: https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883
- *Understanding and Selecting a DLP Solution*, SANS Institute, December 2007: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf