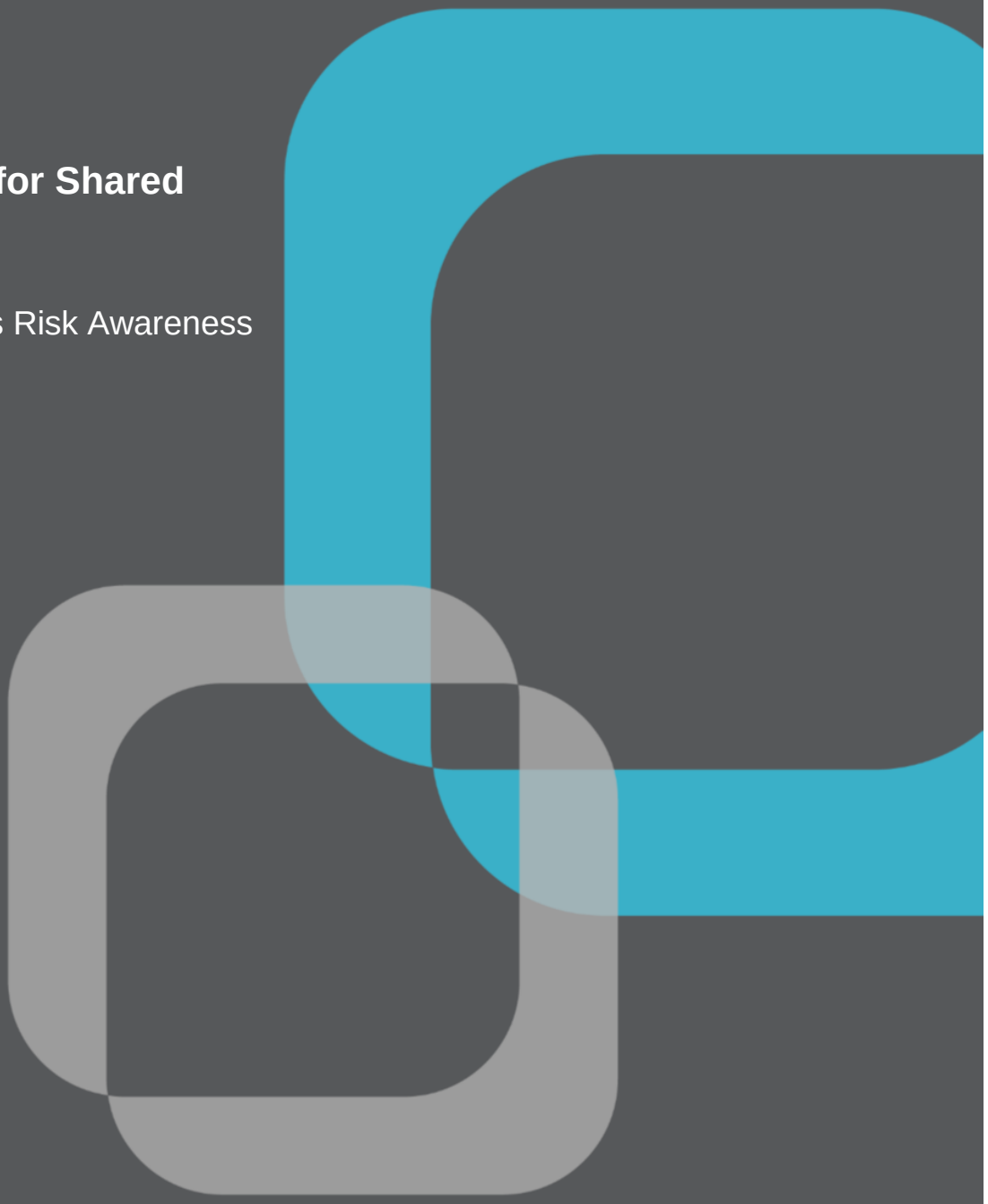
Data Protection for Shared Services

Part One: Data Loss Risk Awareness

May 2017



Smart. Focused. Done Right.®

scottmadden
MANAGEMENT CONSULTANTS

INTRODUCTION

Due to their transactional nature, Shared Services Organizations (SSOs) often control much of an organization's confidential and restricted personal information. This is exactly the kind of information prized by cyber criminals. Because SSO employees must access this data to perform their jobs, there is additional risk of this sensitive data being compromised, either maliciously or unintentionally. While most organizations have enterprise security programs, this may not be enough. The sensitive nature of these operations merits additional measures, and it often falls to SSO leadership to implement them.

Data breaches are pervasive, hard to detect, and expensive:

- **Pervasive.** There were 2,260 data security incidents with confirmed data loss in 2015
- **Hard to Detect.** Detected data breaches have an average time of 201 days (almost 29 weeks) before discovery
- **Expensive.** The cost of a data breach is increasing—the average 2016 total per capita cost of a data breach cost was $221 per record

Data ownership and protection require a proactive approach to mitigate the risk of data loss and its consequences.

Key SSO Data Breach Risk Factors

SSOs operations include several risk factors:

- **Data Integrations.** SSOs transmit sensitive data across many secured and unsecured channels. This can expose data to malicious activity. An example of this is the interface for communicating with an external payroll provider
- **Communication Practices.** Email, chat, and service tickets are common modes of sending messages into and out of SSOs. These regularly include sensitive information that can inadvertently fall into the wrong hands. For example, your case management system might automatically send updates via email to end users with their personal information attached
- **Information Storage.** SSOs often use historical information to support employees and provide reporting. This may lead to large amounts of sensitive information being stored on unsecured shared drives. Many shared drives date back to inception and may contain staffing spreadsheets that include social security numbers and salary data
- **Employee Engagement and Turnover.** SSOs with low employee engagement struggle to implement effective security practices. High turnover can increase the chance of malicious

insider activity. Research indicates that the higher the employee satisfaction score, the better the data security culture

- **Size and Complexity of Data.** SSOs work with a large amount of data on a daily basis. One financial process might include multiple data sources and complicated interactions with different applications. The sheer volume of transactions and source systems creates a difficult environment to track and manage

Even with these risk factors, SSOs struggle to implement data loss prevention measures due to uncertainty of security responsibilities and competing priorities. But SSOs are data breach targets; data protection is an essential SSO program that needs to be prioritized in order to protect sensitive data.

Data Protection

Data protection is a strategy for preventing sensitive or critical information from leaving the corporate network. A shared services data protection program identifies the appropriate policies, procedures, and controls to prevent loss of important, personally identifiable information or other confidential data that may have negative legal, financial, or reputational ramifications.

The program may include supporting technologies with data protection capabilities:

- Data monitoring
- Network detection
- Data access blocking

These prevent distribution or leakage of sensitive data (either intentionally or not) and are a necessary component to a holistic, robust data protection program.

TAKEAWAYS

- SSOs are an attractive target for cyber criminals, given both the sensitive nature and volume of the information handled every day
- Data breaches are only becoming more common, harder to detect, and more expensive. Cost estimates can conservatively reach hundreds of thousands, if not millions, per breach
- A shared services data protection program, in addition to your corporate cybersecurity program, provides the additional protections necessary to mitigate SSO-specific risk factors

NEXT STEPS

To begin building your program, you will need to determine the specific data risks your program must cover and identify the key stakeholders that must be engaged. Part Two of this series, Building the Foundation of Your Data Protection Program, provides a step-by-step guide.

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.

SOURCES

- ScottMadden Research and Expertise
- *2016 Data Breach Investigations Report*, Verizon, 2016 – http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
- *2016 Cost of Data Breach Study: Global Analysis*, Ponemon Institute LLC, June 2016

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 leader, 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.