Data Protection for Shared Services

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 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:

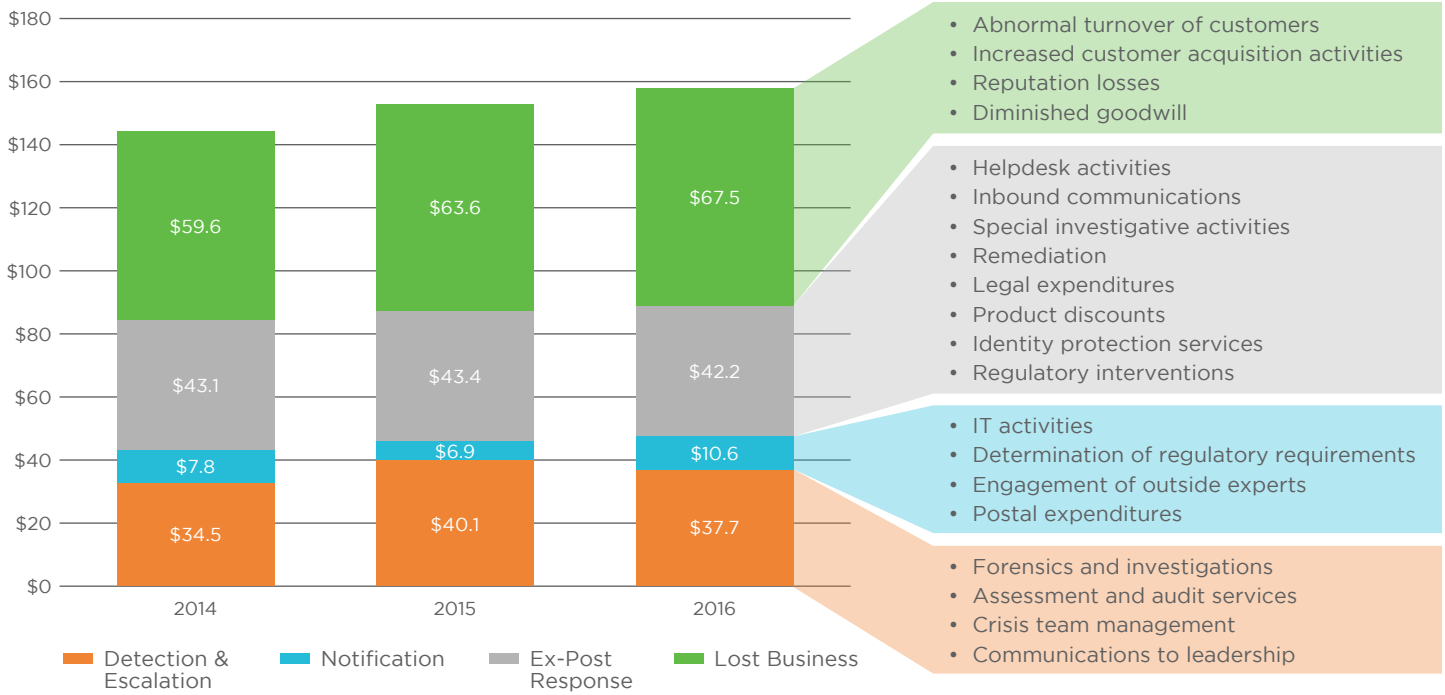
- *Data Integrations* – SSOs transmit sensitive data across many secured and unsecured channels. This can expose data to malicious activity. An example of this is the interface for communicating with an external payroll provider
- *Communication Practices* – Email, chat, and service tickets are common 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.

Figure 1: Cost of Data Breach 2016



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

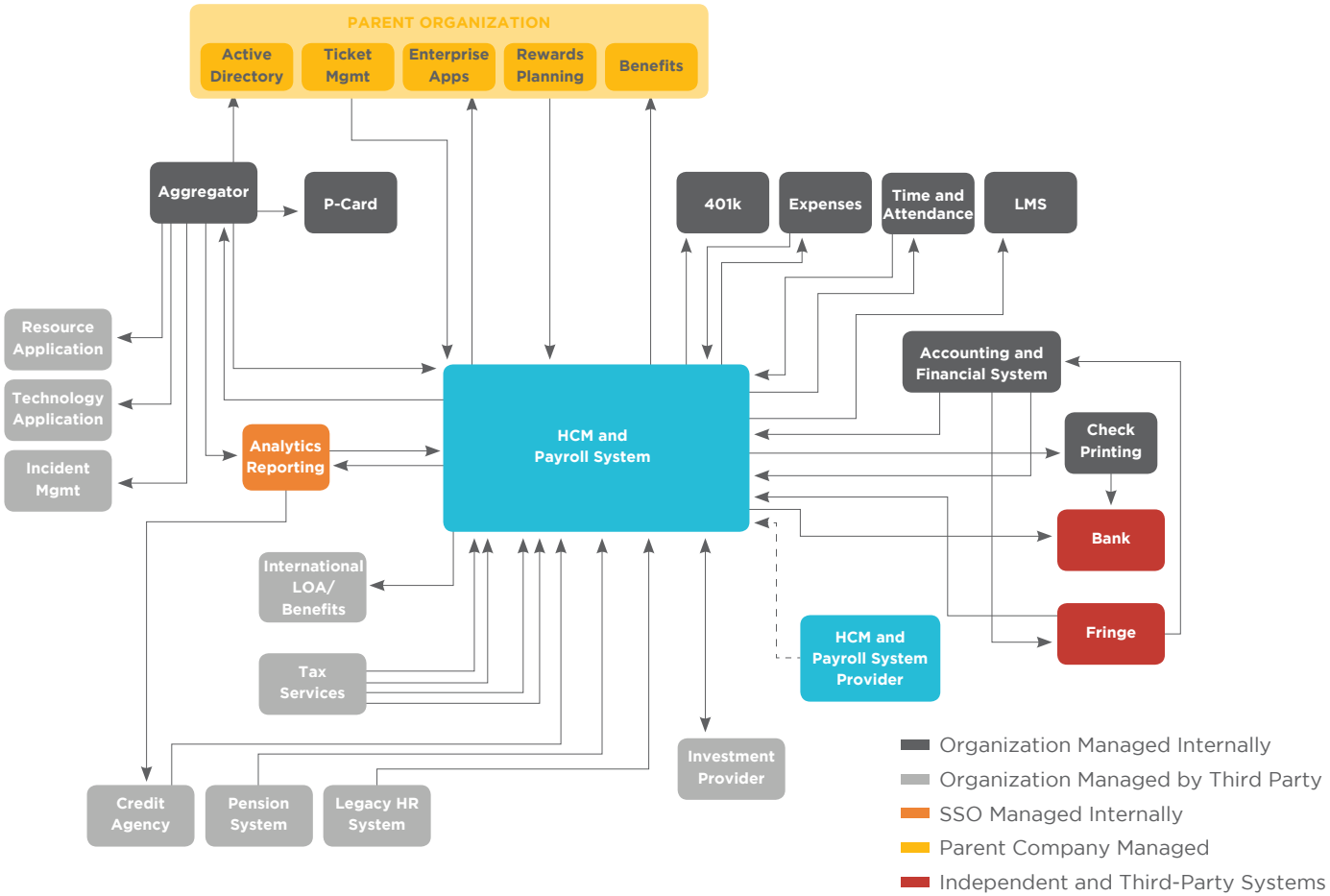
Building the Foundation for Your Shared Services Data-Protection Program

As an SSO owner, it is your responsibility to protect your data and mitigate the risk of a data breach. Establishing a data-protection program can help you accomplish this. A comprehensive data-protection program establishes policies, procedures, and controls that monitor, detect, and even block data transmissions. Technology solutions can prevent distribution or leakage of sensitive data, regardless of whether the leak was intentional or inadvertent.

SSOs are data-breach targets; data protection is an essential SSO program that needs to be prioritized in order to protect sensitive data.

To effectively build and implement a suitable shared services data-protection program, you need an in-depth understanding of the data you need to protect. A comprehensive understanding of your data ensures your program adequately mitigates all relevant risks. First, you will need to define the objectives and scope of your program.

Figure 2: Complexity of HR SSO Information Ecosystem



Define the Data-Protection Program

Data-protection programs are enabled by technology; however, implementing technology is not enough. An effective data-protection program starts with carefully defining the program objectives, securing buy-in from all stakeholders, establishing key performance indicators (KPIs), and establishing a change management plan:

- *Defining Program Objectives* – The objectives for implementing a data-protection program are driven by your business's unique data-protection needs. When establishing these objectives, ensure that your program defines expected outcomes for data that is important and must be protected
- *Securing Stakeholder Buy-in* – A data-protection program cannot be a success without the combined efforts and support of key stakeholders. They should be engaged in the identification of data-breach risks. Ensure that there is no disconnect across the stakeholders on the purpose and scope of your program
- *Establishing KPIs* – The right KPIs are essential to measure the success of your data-protection program. These KPIs may include the number of data leakage incidents, the extent of process coverage, and the level of application coverage. Establish KPIs early in the planning process to baseline where you stand right now and where you want to be
- *Establishing a Change Management Plan* – A comprehensive data-protection program brings significant changes to your SSO operations, employee behavior, and culture. Employees could perceive that the data-protection program is intrusive and unproductive; therefore, part of your data-protection strategy must be to establish a change management plan to build awareness for the need for your program

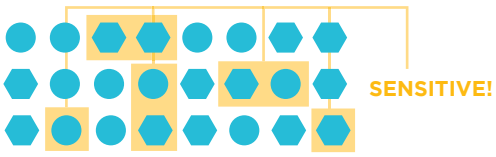
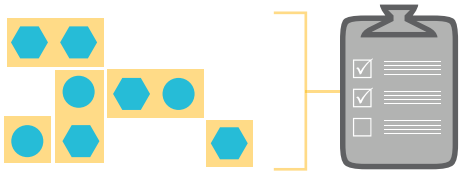
Know Your Data

Identification and classification of data is the most important part of the SSO data-protection program. As shown in Figure 2, SSO data is constantly moving through systems, applications, and individuals, resulting in an extremely complex SSO information ecosystem. The volume of sensitive data makes SSOs a target. While a high volume of data tends to correlate with increased operational efficiency, it also increases the risk that this data may be compromised. Despite this risk, data security is often overlooked in favor of gains in operational efficiency and customer service.

Due to the sheer volume and diversity of SSO data, it's important to carefully analyze your data to set the policies needed to detect and respond to incidents. As shown in Figure 3, ScottMadden recommends four steps:

- **Step 1:** Understand Data Access and Flow. A key step in planning for an effective data-protection program is understanding how the data is accessed and how it flows in and out of your organization
  - *Access:* Most users access data within applications, such as case management, HR information systems, or accounts payable systems. Shared drives, end-user devices, and third-party tools, like cloud storage services, are also used for data storage
  - *Transmission:* SSO application integrations are the

Figure 3: Know Your Data

PROCESS	EXAMPLE	EXPLANATION
Step 1 Understand Data (Access and Flow)		Inventory integrations, applications, databases, and storage media
Step 2 Identify Sensitive Data		Identify which data include sensitive information
Step 3 Assess the Risk		Conduct thorough risk assessment of sensitive data measuring the impact of a potential data-leakage incident
Step 4 Assign Classifications		Categorize data to facilitate prioritization

primary data transmission media used by the end users. However, some data integrations occur over unsecured pathways (e.g., email) and need to be identified and secured

- **Step 2:** Identify Sensitive Data. Identification of data is a challenging step in designing an SSO data-protection program. At any given time, sensitive data is being used, shared, or stored across your servers, databases, workstations, laptops, and internal networks. Your organization's data can be divided into two broad categories: structured data and unstructured data
    - Structured data refers to any data that resides in relational databases and spreadsheets, including benefits information, employee payroll information, and personally identifiable information. The structured data has the advantage of being easily entered, stored, queried, and analyzed and is typically managed centrally
    - Unstructured data consists of all data that cannot be easily organized and includes PowerPoint presentations, word processing documents, PDF files, emails, and images. Unstructured data is managed by end users

Identify structured data by working with SSO centers of excellence to understand what sensitive data is stored in databases and other network locations, how it is managed, and how it is accessed. Identify unstructured data using a variety of discovery tools. This includes special data-loss-prevention products that come with a range of data identification technologies. These products consist of a discovery engine that crawls all the data in your SSO network, indexes it, and organizes it for risk assessment and classification.

- **Step 3:** Assess the Risk. Classify data by assessing the risk associated with it. You can then assign protection measures based on data risk classification. Assess risk using questions such as:
    - Is the data protected by regulations?
    - Is the data critical to business operations, and if so, can it cause financial loss?
    - Is the data important from a privacy perspective?
    - Is the data important to customers and business partners?

- **Step 4:** Assign Classifications. Based on the data risk assessment, assign classifications (high risk, moderate risk, low risk) to the data. These classification levels are often defined by enterprise information security

Takeaways

- Focus on understanding and protecting SSO data risks rather than implementing technical data-protection products. A thorough data inventory and assessment will help you develop accurate data-protection policies and procedures
- Establish KPIs to measure your data-protection program's success. KPIs will help you monitor progress and prove value to your stakeholders
- Spend time on stakeholder buy-in and proactive communication with employees. Implementing an SSO data-protection program is not an IT project, but an SSO business initiative that requires both process and employee behavior changes

Next Steps

Once you have defined your SSO data-protection program, obtained stakeholder buy-in, and undertaken the analysis of your data, it's time to consider the processes, policies, and procedures involved in a successful data-protection program. For more information, see Part Three: The Core Elements of Your Data-Protection Program.

A thorough data inventory and assessment will help you develop accurate data-protection policies and procedures.

The Core Elements of Your Shared Services Data-Protection Program

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 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

Given how often data breaches occur, and the cost associated with them, data loss-prevention programs are no longer optional.

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 an 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 life cycle 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 and 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

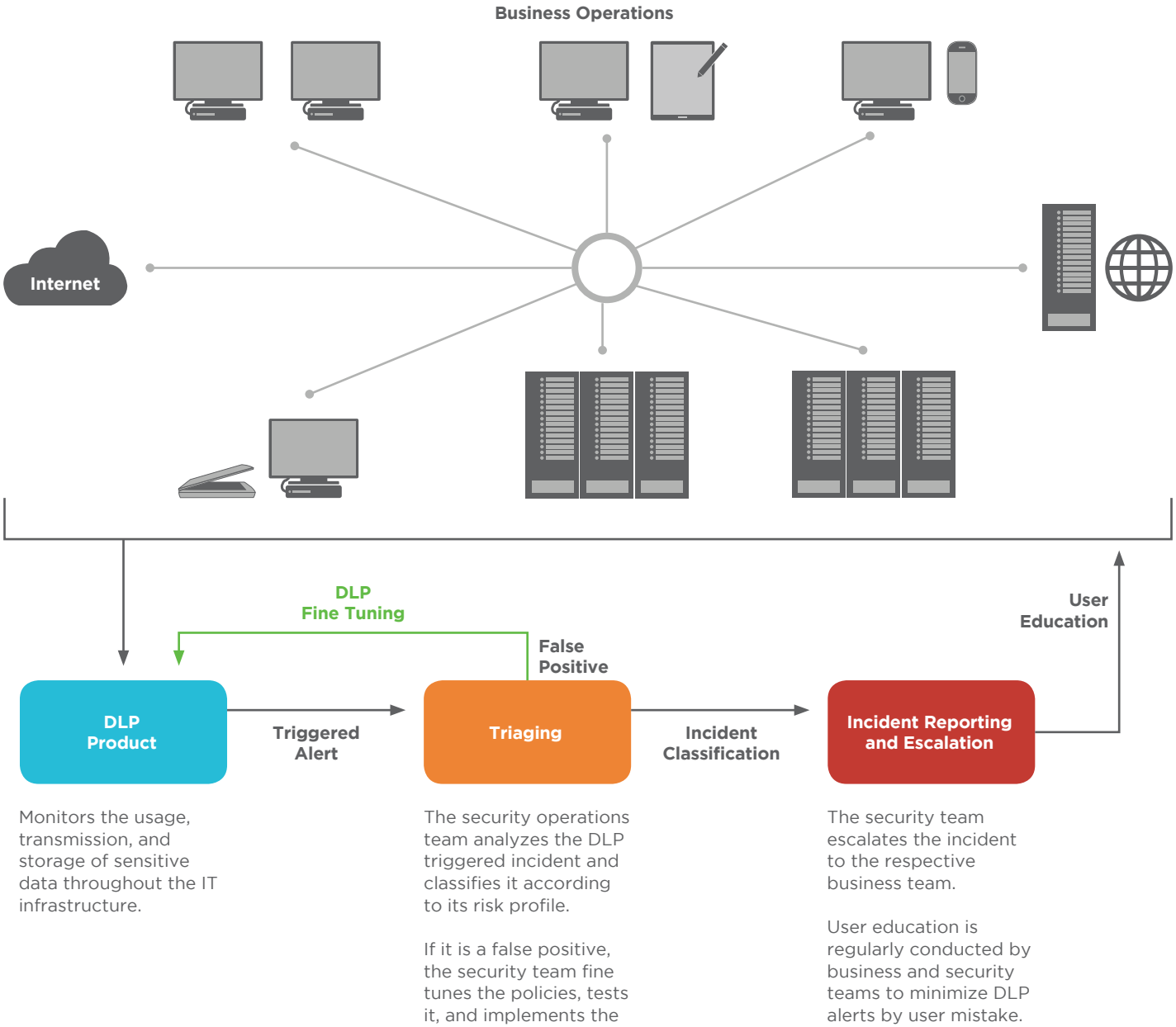
- Establish data protection policies and procedures that cover the life cycle of data throughout the complex SSO information ecosystem, including data in use, at rest, and in transit
- Conduct extensive user education and awareness on a regular basis to instill a security culture in your organization
- 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 an 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.

Figure 4: DLP Process



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

Smart. Focused. Done Right.®

scottmadden
MANAGEMENT CONSULTANTS

LOCATIONS

ATLANTA
3495 Piedmont Road, NE
Building 10, Suite 805
Atlanta, GA 30305
404.814.0020

RALEIGH
2626 Glenwood Avenue
Suite 480
Raleigh, NC 27608
919.781.4191

WESTBOROUGH
1900 West Park Drive
Suite 250
Westborough, MA 01581
508.202.7918