scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.®

Cybersecurity in Shared Services Organizations

June 2016

Contents

- Introduction to Shared Services Cybersecurity
- What’s at Risk?
- Cyber Attack Trends
- Key Shared Services Organization (SSO) Risk Factors
- Building Blocks of an SSO Cybersecurity Program
    - Data Security
    - Education and Awareness
    - Governance and Compliance
- SSO Cybersecurity Leading Practices
- How ScottMadden Can Help

Introduction to Shared Services Cybersecurity

Shared Service Organizations (SSOs) control much of an organization's confidential and restricted personal information. While handling and using this data is routine for SSOs, it is exactly the kind of information that is highly prized by cyber criminals. A robust cybersecurity program is imperative to protect the organization, employees, and customers.

Cyber threats can materialize in a number of ways but can be broken down into two main types:

Type	Description	Examples
External	▪ Cyber criminals use offensive maneuvers with the intent of stealing, altering, or destroying data, networks, infrastructure assets, and/or personal devices	▪ Denial of service attacks designed to make network resources unavailable to its users ▪ Unauthorized users gaining physical access to a computer and downloading sensitive data ▪ Attempts to acquire usernames, passwords, and credit card details directly from users (e.g., phishing)
Internal	▪ Employees unintentionally compromise sensitive data or systems, potentially exposing the organization to cyber attacks ▪ Employees maliciously circumvent data security protocols and/or willingly aid cyber criminals	▪ Sending documents containing sensitive information via standard email rather than through secure email programs ▪ Purposefully opening email attachments from external senders known to contain malicious code

Many organizations have dedicated Information Security (InfoSec) groups that manage security programs enterprise wide. However, accountability for protecting sensitive shared services and employee information ultimately falls to the SSO.

What’s At Risk?

Confidential Information refers to data/information for which unauthorized access or disclosure could result in an adverse effect on the organization, an individual, or both. This information could either be personally identifiable information (PII) or confidential business information. Restricted Information includes the most sensitive Confidential Information and is typically protected by law or policy.

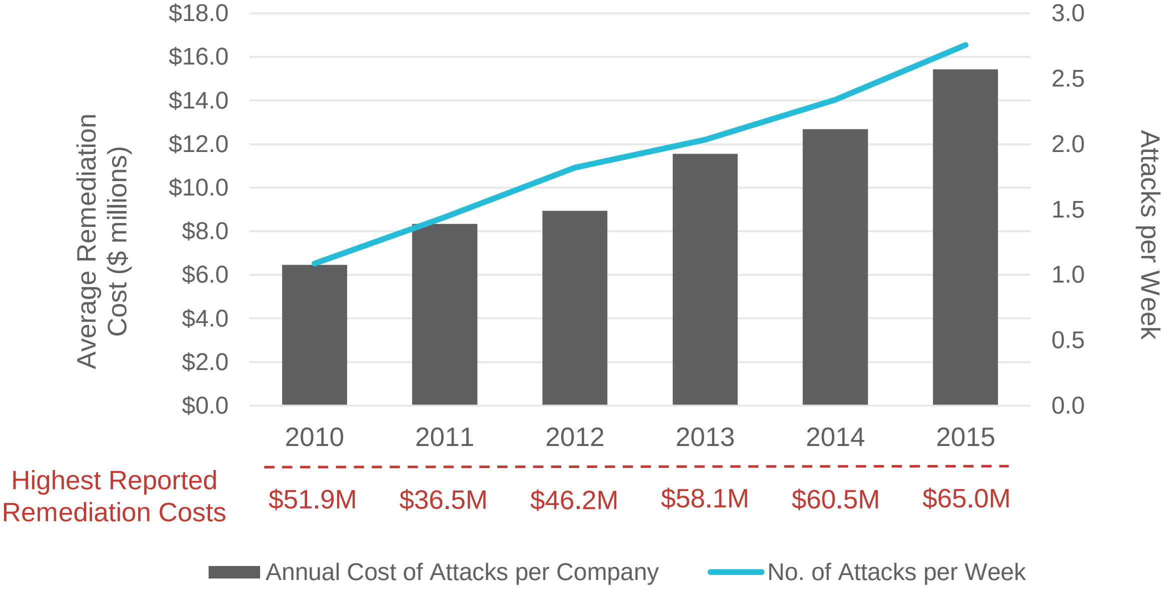
	Personal Data/PII		Business/Organization	
Examples of Confidential Information	- Name - Email address - Physical address - Phone number - Job title	- Work experience - Evaluations - Gender - Marital status - Age	- M&A or transactional activity - Ongoing lawsuits - Internal investigations - Proprietary content	- Advance SEC filings - Press releases - Emails - Internal memos - Company presentations
Examples of Restricted Information	- SSN - Passport - Driver’s license - Ethnicity - Nationality - Sexual orientation	- Medical history - Salary/compensation - Bank account information - Background checks - Credit reports - Criminal history	- Strategic plans - Budgets - Reports - Legal materials - Audits and assessments - P-card numbers	

Cyber Attack Trends

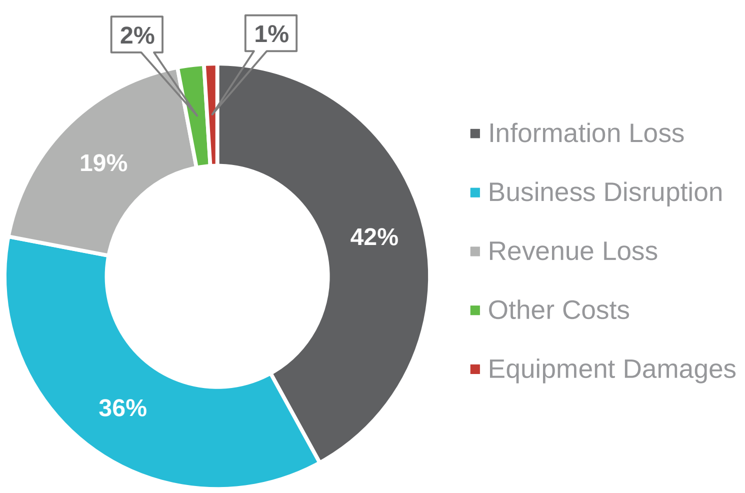
The number of cyber attacks against organizations continues to grow in complexity, frequency, and severity. Significant data breaches in 2015 included[1]:

- VTech (children's technology maker) – personal data compromised for 5 million parents and 6 million children
- Kaspersky Lab (security vendor) – 13 million account records exposed
- Experian (credit service provider) – personal data compromised for 15 million customers
- US Office of Personnel Management (federal government) – PII and restricted data exposed for 21.5 million federal employees
- Anthem Blue Cross Blue Shield (health insurer) – PII and restricted data exposed for 80 million patients and employees

2015 Cyber Attack Trends[2]



2015 Cyber Attack Cost Breakdown[2]



In 2015, the average organization spent more than $15 million remediating the effects of cyber attacks. To mitigate potential costs, SSOs must take action to understand and protect the flow of their sensitive information.

[1] CRN, 10 Biggest Data Breaches of 2015

[2] Source: 2015 Cost of Cyber Crime Study, Ponemon Institute

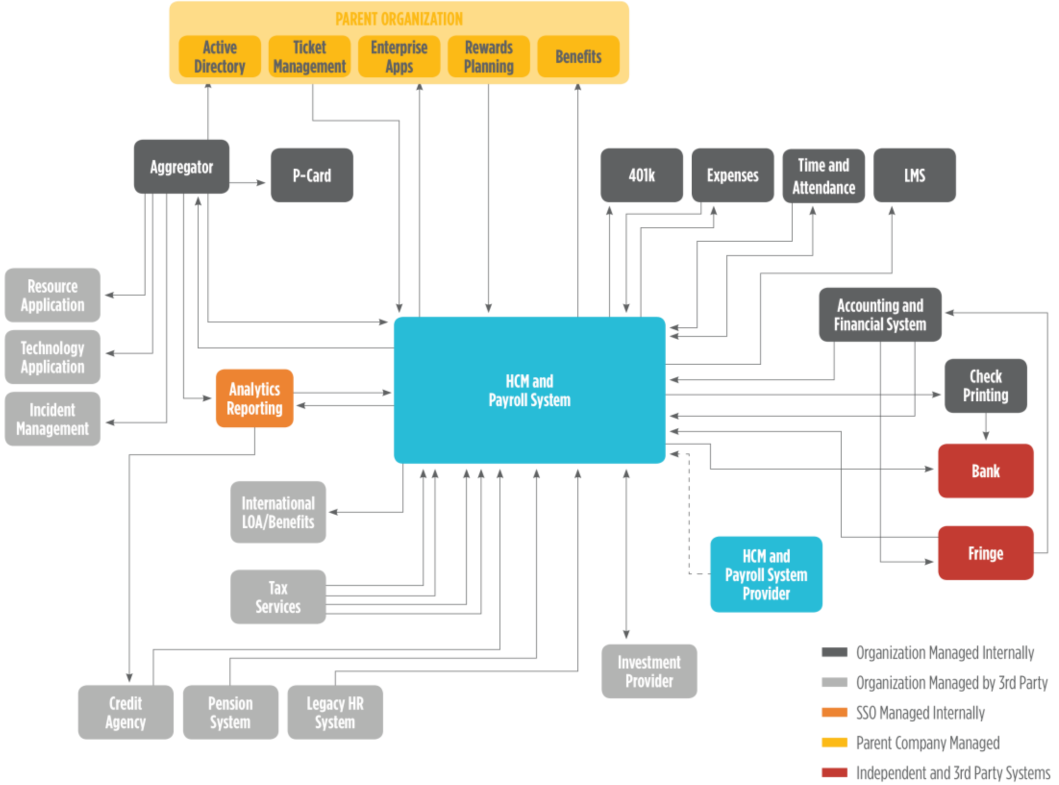
Key SSO Risk Factors

The volume of sensitive data makes SSOs a target. While a high volume of data tends to correlate to increased operational efficiency, it also increases the risk that this data may be compromised. Despite this, data security is often overlooked in favor of gains in operational efficiency and customer service.

SSO Risk Factors

- SSOs enhance their efficacy by integrating their primary systems with third-party systems for benefits management, time and attendance, etc. Each of these integrations typically transmits sensitive data over myriad secured and unsecured channels
- Business process complexities, policies, and exceptions increase along with the amount of sensitive data flowing through the SSO
- Email, chat, and open service tickets are common modes of sending communications in and out of SSOs. These regularly include sensitive information that can inadvertently fall into the wrong hands
- Some SSO departments (e.g., workforce administration, call centers) can experience low employee engagement, especially for data security initiatives
- These departments can also experience high turnover, opening the SSO up further to potential malicious insider activity

Complexity of an HR SSO Information Ecosystem



SSO data is constantly moving through countless systems, applications, and individuals. Only a robust cybersecurity program can mitigate the complexities of the information ecosystem.

Building Blocks of SSO Cybersecurity

Tiered SSO delivery models often include payroll and leave-of-absence specialists, AP clerks, and HRIS teams that have elevated privileges to sensitive data. SSOs need to provide employees the tools, awareness, and direction to properly handle, communicate, and use confidential and restricted data.

Building Block	Key Questions	Potential Vulnerabilities
Data Security	▪ Do you know where your confidential and restricted data is stored and for how long? ▪ What controls are in place to ensure data safely reaches its intended destination? ▪ Do you have secure methods for handling and collaborating with restricted data? ▪ Who has access to confidential and restricted data?	▪ It is not clear how many systems, applications, servers, etc. house PII ▪ Old databases and files are left on shared drives "as is" after they are no longer needed ▪ Some employees save files containing PII to their local drives ▪ Third-party support vendors have access to applications that process/contain PII
Education and Awareness	▪ What information security training do SSO employees receive? ▪ How often is the material refreshed and presented?	▪ Employees receive minimal, ineffective training ▪ Training documentation is not up to date with current trends and leading practices
Security Governance and Compliance	▪ Are there clear roles and responsibilities between the SSO, IT, and InfoSec? ▪ Are you in compliance with enterprise data security standards and policies?	▪ Lack of an overall governance structure that clearly outlines roles and accountabilities ▪ Enterprise data retention policies require file deletion before statutory paystub regulations

SSO Data Security

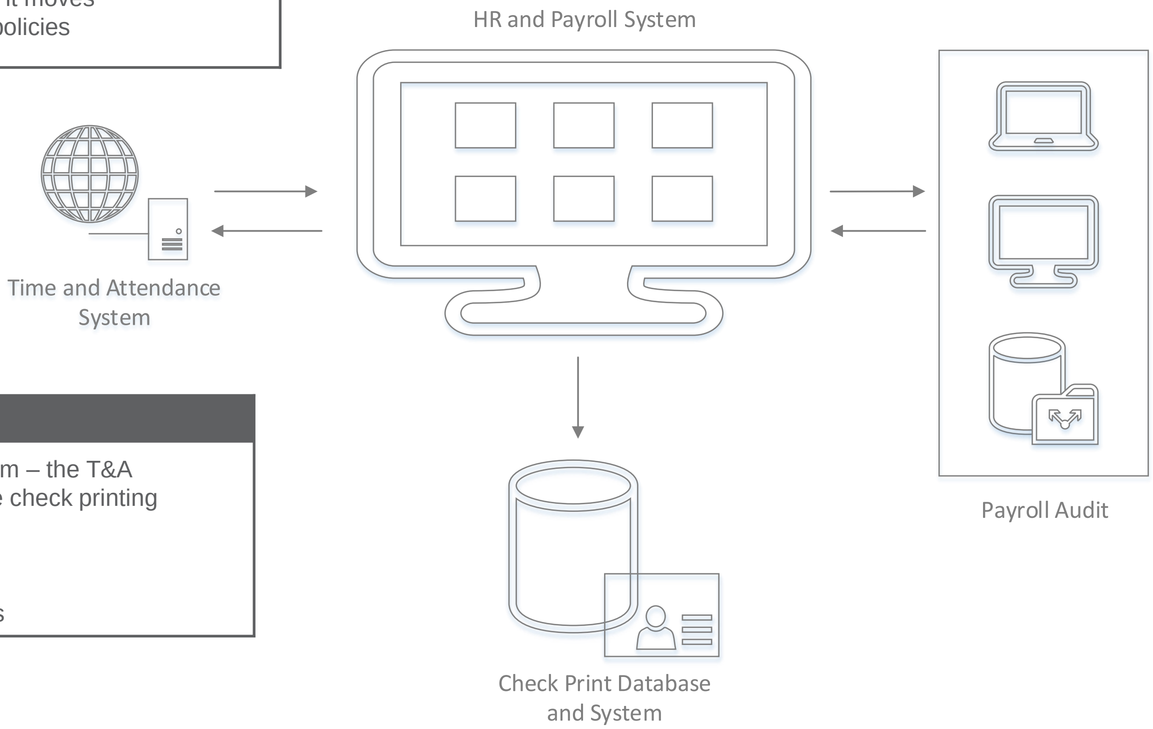
SSO data is stored in and moves through countless on-premises and cloud applications and systems. Understanding where sensitive data is stored and how it is used and shared are essential to developing and implementing effective security controls. Data can be classified in three categories:

- Data at rest: Anything that holds data in a static state, such as file shares, databases, servers, etc.
- Data in motion: Data in transit ("on a wire") between applications, systems, individuals, etc. via email, web, or other Internet protocols
- Data in use: Data that resides on the end-user workstation and needs to be protected from being leaked through removable media devices like USBs, DVDs, CDs etc.

The graphic below depicts a sample flow of data through an SSO's payroll process:

Data in Motion

Key concerns:
- Level of encryption on data as it moves
- Encryption key management/policies



Data in Use

The payroll audit team uses computers and shared drives to audit payroll files prior to releasing for final printing. Key concerns include:
- Frequency that drives and computers are wiped for sensitive information
- Access restrictions to shared drives
- Standards for sharing sensitive data

Data at Rest

Data is stored in multiple locations in this diagram – the T&A database, the cloud HR/payroll solution, and the check printing software database. Key concerns include:
- Level of encryption (e.g., full disk, file level)
- Consistent use of encryption
- Access restrictions to databases and servers

Mitigating Common SSO Data Security Challenges

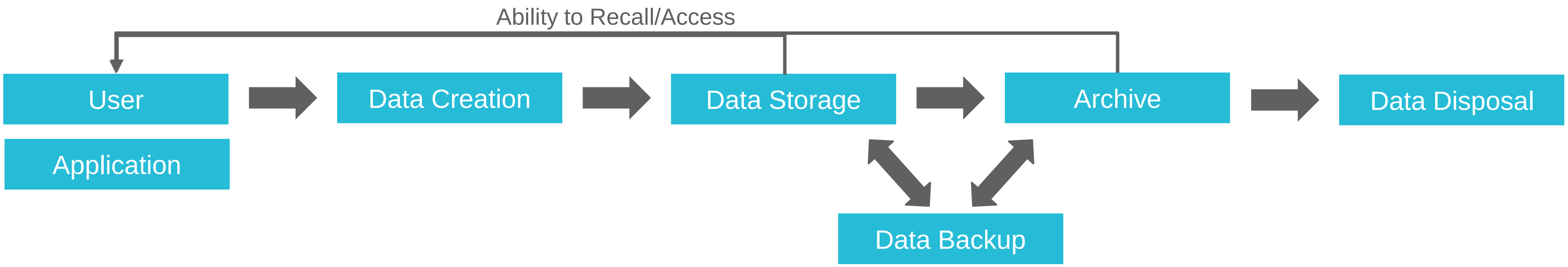
Many SSOs face similar data security challenges and risk points they must address:

- Stale or outdated data maintained on servers and databases
- Numerous locations and mechanisms for storing data
- Necessity of cross-functional collaboration using sensitive data
- Inconsistent use of encryption and secure file transfer protocols
- Lack of clarity with regards to retention standards

Formal data security standards can help mitigate these risks throughout the data life cycle. Key considerations include:

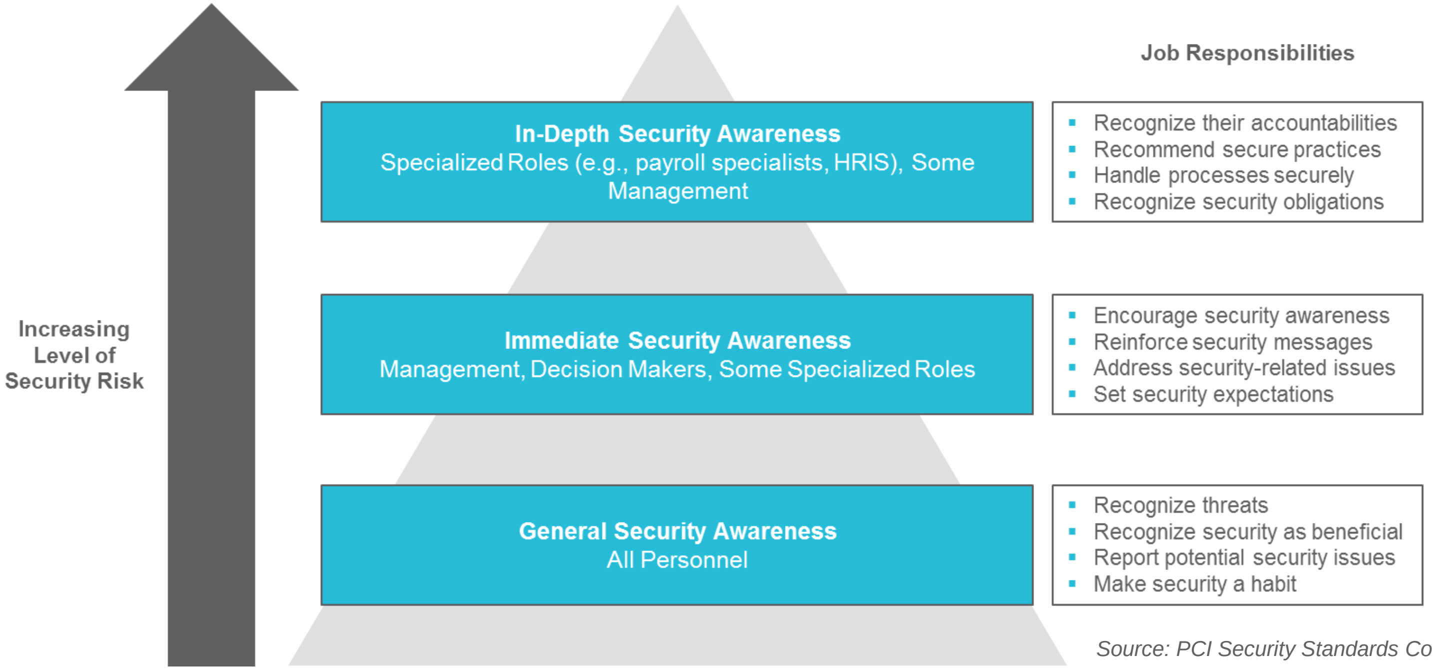
- What data will be stored, and for how long
- Where data will be stored, both physically and electronically
- Who can access data, including both applications and users
- How often and where data should be backed up
- When and how to destroy data

Life Cycle of SSO Data



Education and Awareness

Cyber crimes are not the only sources of risk for SSOs—the action or inaction of employees can also lead to security incidents. It is vital SSOs maintain a security awareness program to ensure employees understand the importance of protecting sensitive information, how to handle it securely, and the risks of mishandling such information.



In-Depth Security Awareness
Specialized Roles (e.g., payroll specialists, HRIS), Some Management

- Recognize their accountabilities
- Recommend secure practices
- Handle processes securely
- Recognize security obligations

Immediate Security Awareness
Management, Decision Makers, Some Specialized Roles

- Encourage security awareness
- Reinforce security messages
- Address security-related issues
- Set security expectations

General Security Awareness
All Personnel

- Recognize threats
- Recognize security as beneficial
- Report potential security issues
- Make security a habit

Source: PCI Security Standards Council

Qualities of an effective and sustainable awareness program include:

- Information is provided in a way that relates to the SSO culture (i.e., how employees think and behave)
- Information is delivered in different formats to affect change and is consistently reinforced and repeated
- Management is on-board and understands the holistic security risks (e.g., financial, reputational, legal)
- Presentations are personal – “bring the message home,” “security is everyone’s job”
- Information is relevant to current events and trends and is consistently updated with lessons learned

Governance and Compliance

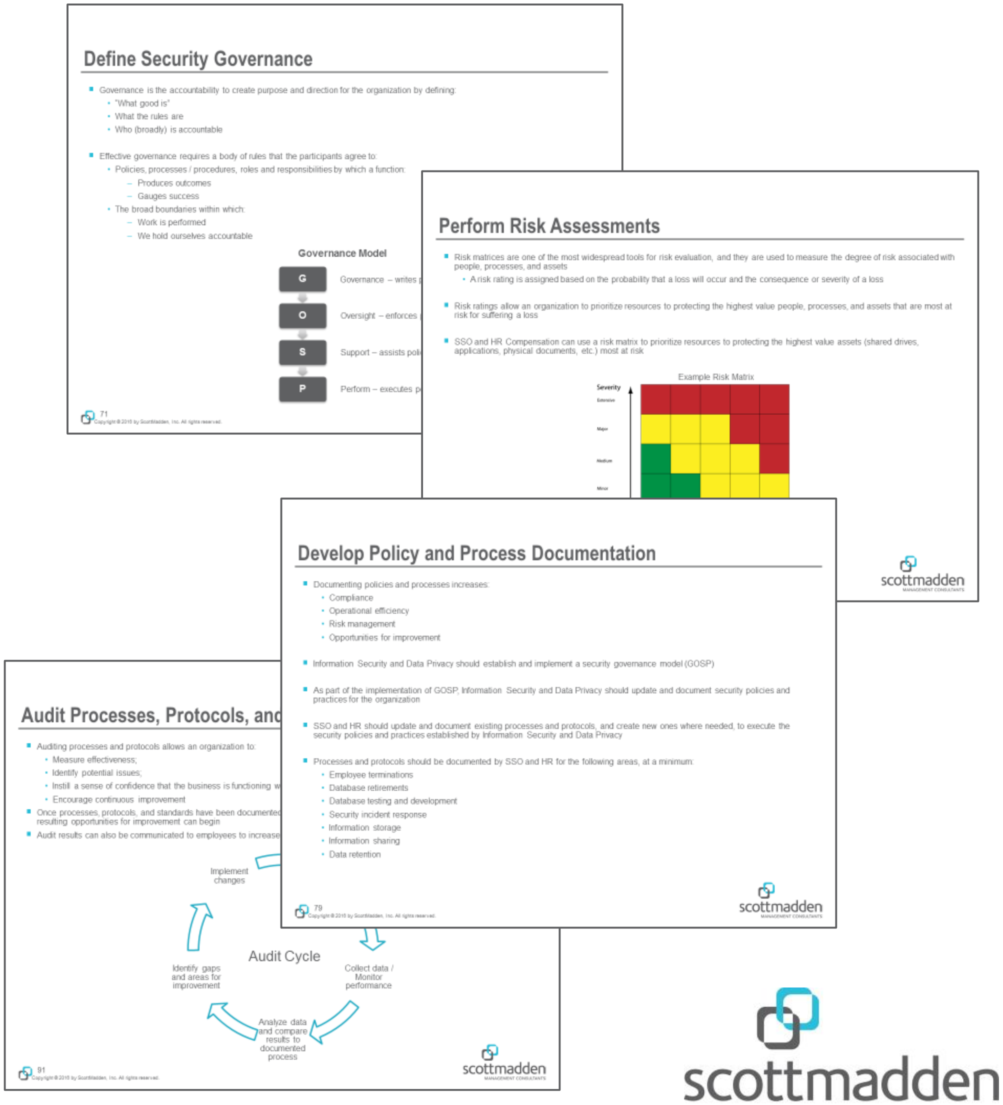
In addition to securing sensitive data and educating employees, SSOs must work with other parts of the organization to clearly define security roles and responsibilities. Establishing a governance model creates a structure that enables the SSO to operate with clear role definition, fosters appropriate accountabilities, and ensures compliance with corporate standards.

Foster Collaboration between the SSO, IT, Legal and InfoSec

- Identify a clear set of roles and responsibilities for which each group is accountable
- Leverage the insight of each group to determine risk points
- Ensure communication between all groups is timely, efficient, and ongoing
- Work together on policy creation to ensure the alignment on data security priorities and standards

Establish Enterprise Data Security Standards

- Conduct analysis to understand where the SSO is in relation to existing enterprise data security policies and identify highest priority gaps
- Collaborate to establish overall data security standards taking into account special SSO situations and laws/regulations
- Document policy and process documentation
- Establish a process and standards audit cycle



Define Security Governance

- Governance is the accountability to create purpose and direction for the organization by defining:
  - "What good is"
  - What the rules are
  - Who (broadly) is accountable
- Effective governance requires a body of rules that the participants agree to:
  - Policies, processes / procedures, roles and responsibilities by which a function:
    - Produces outcomes
    - Gauges success
  - The broad boundaries within which:
    - Work is performed
    - We hold ourselves accountable

Governance Model

71
Copyright © 2016 by ScottMadden, Inc. All rights reserved.

Perform Risk Assessments

- Risk matrices are one of the most widespread tools for risk evaluation, and they are used to measure the degree of risk associated with people, processes, and assets
  - A risk rating is assigned based on the probability that a loss will occur and the consequence or severity of a loss
- Risk ratings allow an organization to prioritize resources to protecting the highest value people, processes, and assets that are most at risk for suffering a loss
- SSO and HR Compensation can use a risk matrix to prioritize resources to protecting the highest value assets (shared drives, applications, physical documents, etc.) most at risk

Example Risk Matrix

Severity					
Extensive	🟥	🟥	🟥	🟥	🟥
Major	🟨	🟨	🟨	🟥	🟥
Medium	🟩	🟨	🟨	🟨	🟥
Minor	🟩	🟩	🟨	🟨	🟨

scottmadden MANAGEMENT CONSULTANTS

Develop Policy and Process Documentation

- Documenting policies and processes increases:
  - Compliance
  - Operational efficiency
  - Risk management
  - Opportunities for improvement
- Information Security and Data Privacy should establish and implement a security governance model (GOSP)
- As part of the implementation of GOSP, Information Security and Data Privacy should update and document security policies and practices for the organization
- SSO and HR should update and document existing processes and protocols, and create new ones where needed, to execute the security policies and practices established by Information Security and Data Privacy
- Processes and protocols should be documented by SSO and HR for the following areas, at a minimum:
  - Employee terminations
  - Database retirements
  - Database testing and development
  - Security incident response
  - Information storage
  - Information sharing
  - Data retention

79
Copyright © 2016 by ScottMadden, Inc. All rights reserved.

scottmadden MANAGEMENT CONSULTANTS

Audit Processes, Protocols, and

- Auditing processes and protocols allows an organization to:
  - Measure effectiveness;
  - Identify potential issues;
  - Instill a sense of confidence that the business is functioning w
  - Encourage continuous improvement
- Once processes, protocols, and standards have been documented resulting opportunities for improvement can begin
- Audit results can also be communicated to employees to increase

Audit Cycle
Implement changes
Collect data / Monitor performance
Analyze data and compare results to documented process
Identify gaps and areas for improvement

91
Copyright © 2016 by ScottMadden, Inc. All rights reserved.

scottmadden MANAGEMENT CONSULTANTS

scottmadden
MANAGEMENT CONSULTANTS

SSO Cybersecurity Leading Practices

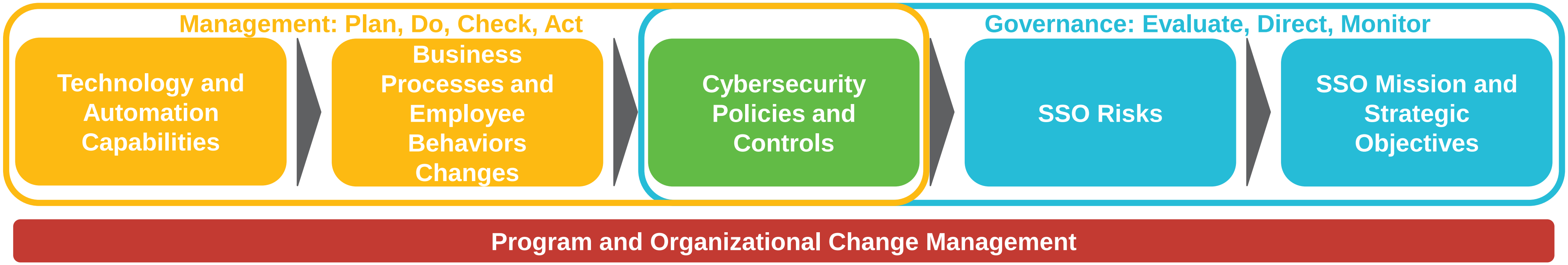
Building Block	Leading Practice	Benefit Description	Impact	Implementation Level
Data Security	Secure sensitive information that is not encrypted	▪ Reduces the likelihood of a successful breach ▪ Enhances the defense in depth through multiple avenues of layered security ▪ Supports secure business processes	High	Enterprise/SSO
	Enhance physical security practices	▪ Protects employees, hardware, programs, network, data, and other assets from physical intrusions and events that could cause loss or damage to an organization or individual	High	SSO
	Develop information sharing standards	▪ Provides clarity of expectations, increases accountability, and ensures the most effective tools at the organization's disposal are being used ▪ Ensures the applications and tools used to share information meet organizational security and business requirements	High	Enterprise/SSO
	Develop information storage standards	▪ Determines how SSOs will comply with the organization's data retention policy	High	SSO
	Inventory information at rest, in motion, and in use	▪ Allows an organization to: • Create policies and standards aligned with business needs • Secure data via encryption or other appropriate methods • Develop an effective defense in depth strategy	High	Enterprise/SSO
	Isolate restricted information and confidential information	▪ Creates and designates repositories for the storage of sensitive information ▪ Allows the organization to better understand where its data resides ▪ Ensures security solutions and resources are prioritized and aligned with protecting the organization's most valuable information	High	Enterprise/SSO
Education and Awareness	Develop a security awareness program	▪ Regularly reminds and reinforces the need to keep sensitive information secure ▪ Continuously promotes awareness	High	Enterprise/SSO

SSO Cybersecurity Leading Practices (Cont’d)

Building Block	Leading Practice	Benefit Description	Impact	Implementation Level
Governance and Compliance	Develop a data retention policy	▪ Helps organizations manage data, comply with laws and regulations, and prepare for business continuity in case of a disaster	**High**	Enterprise/SSO
	Define security governance	▪ Creates a structure that enables the organization to operate with clear role definition and accountabilities	**High**	Enterprise
	Develop policy and process documentation	▪ Allows senior leadership to communicate philosophies, strategy, and broad requirements to the organization ▪ Allows leadership to define and standardize how the requirements set forth in the policies will be accomplished	**High**	Enterprise/SSO
	Measure process effectiveness	▪ Allows an organization to assess the effectiveness of its security controls ▪ Facilitates decision making, improves performance, and increases accountability	**Medium**	Enterprise/SSO
	Audit processes, protocols, and standards	▪ Instills a sense of confidence that the business is functioning well and is prepared to meet potential challenges ▪ Encourages continuous improvement	**Medium**	Enterprise/SSO
	Perform risk assessments	▪ Highlights the cybersecurity risk to organizational operations, assets, and individuals ▪ Serves as a foundation for prioritizing improvement efforts and decision making	**Medium**	Enterprise
	Develop system requirements	▪ Describes functions which systems, applications, and other tools should fulfill to meet security and business requirements	**Low**	Enterprise
	Develop a formal data loss prevention program	▪ Improves data classification schemes ▪ Provides an understanding of the data life cycle ▪ Enhances controls over access to sensitive data	**Low**	Enterprise

Putting It All Together

A programmatic approach is required to secure SSOs. Attempts to build and improve cybersecurity capabilities through individual or disjointed projects are expensive and ineffective. SSOs must pursue a programmatic approach that mitigates SSO-wide risks.


Management: Plan, Do, Check, Act
Governance: Evaluate, Direct, Monitor
Technology and Automation Capabilities
Business Processes and Employee Behaviors Changes
Cybersecurity Policies and Controls
SSO Risks
SSO Mission and Strategic Objectives
Program and Organizational Change Management

In a formal cybersecurity program:

- A roadmap is created to identify critical risks, take immediate action, and achieve long-term capabilities. Many leading practices can be implemented quickly with significant impact on SSO cybersecurity
- Priorities are risk informed
- Project management and organizational change management enable a successful implementation
- Monitoring of indicators drives corrective actions and continuous improvement

Engaging SSO leadership and stakeholders in cybersecurity decision making is the single most important factor in creating a successful cybersecurity program—more than technology or funding.

scottmadden
MANAGEMENT CONSULTANTS

How ScottMadden Can Help

Cybersecurity Program Services

- Strategic planning support
- Security program management
- Design and implementation
- Security policy alignment
- Program assessments
- Sensitive data inventories
- Transformation

Cybersecurity Governance Design and Implementation

- Policy framework design
- Business policy and process assessments
- Data security standards creation
- Cybersecurity metric design and implementation
- Access management strategy development

Cybersecurity Organizational Change Management (OCM)

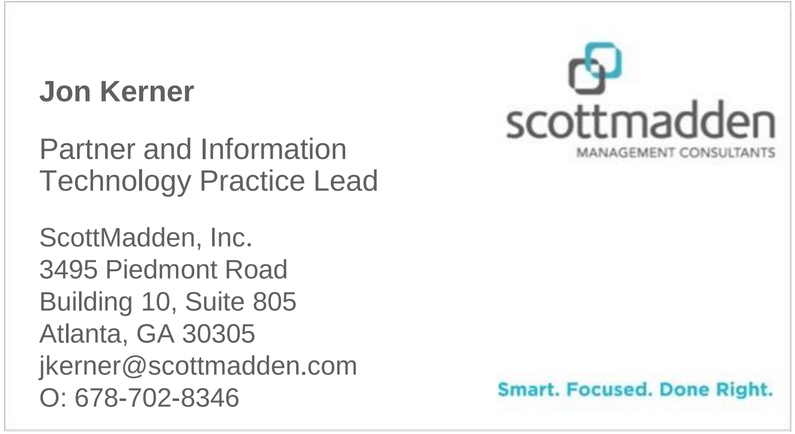
- OCM support of implementation efforts
- Cybersecurity awareness plan – design and implementation

Cybersecurity Capability Design and Implementation

- Process design
- Implementation project management
- Cybersecurity threat-based risk assessments
- Vendor selection

Contact Us

To learn more about SSO Cybersecurity, contact us.



Jon Kerner

Partner and Information
Technology Practice Lead

ScottMadden, Inc.
3495 Piedmont Road
Building 10, Suite 805
Atlanta, GA 30305
jkerner@scottmadden.com
O: 678-702-8346

scottmadden
MANAGEMENT CONSULTANTS
Smart. Focused. Done Right.