Deloitte.

Data Protection

Practical Strategies for Getting it Right

Jamie Ross

Data Security Day – June 8, 2016

Agenda

1) Data protection – key drivers and the need for an integrated approach
2) Common challenges – data protection in the public sector
3) Data protection programs – strategies for getting it right

Data protection

Key drivers and the need for an integrated approach

Data protection in BC

Increased focus on security, information management, privacy and access

Drivers

- **Increased awareness** – growing focus on information incidents, information management and information protection
- **Increased priority** - data security highlighted by the OCIO as a key priority across Government for 2016/2017
- **Updated regulatory requirements**- significant updates recently completed or under consideration for relevant legislation (e.g., *Information Management Act*)
- **Focus on performance** - Increased focus on improving performance related to security, records management, privacy and information access. Priorities include:
  - Training – ensuring the necessary training materials are available and that the right individuals receive regular training and awareness regarding records management, privacy and access
  - Compliance monitoring and reporting - goal of establishing a performance baseline across government and enabling improvement over time

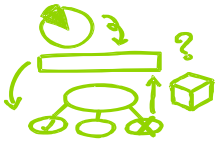
Common challenges

Data protection in the public sector

Data protection in the public sector

The current state

Trends



Complexity
Increasing volume and complexity of data flows, uses and systems

Threats
Increasing sophistication and capabilities of threat actors

Data
Increasing use of data and analytics to drive program delivery and improvement

Expectations
Increasing expectations regarding data protection and compliance

Technology
Rapid increase in the pace of technological change

Requirements/Guidance

Policies & Regulation
Extensive requirements in place

Standards & guidance
Standards, guidance and tools have been developed

Observations

Implementation is a challenge

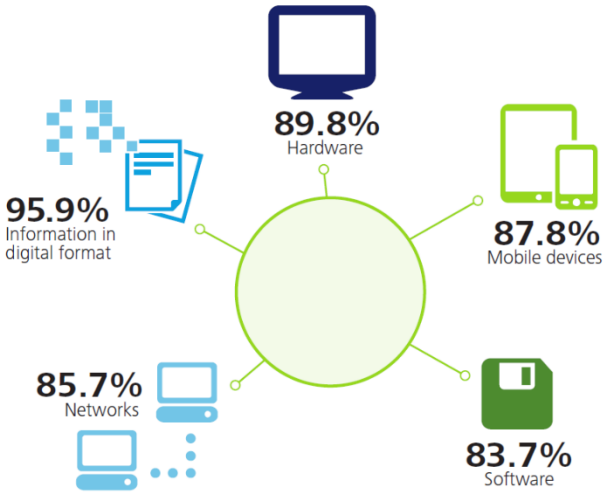
- Accountability
- Data flows & inventories
- Data classification
- Consistency in approach
- Working in the “grey” zone

Lack of clarity regarding accountability

Roles and responsibilities with respect to data protection are not always clearly understood

- Recognition that data protection is a shared responsibility but lack of clarity regarding specific accountabilities
- Data governance programs are increasingly common and define accountability across all types of data users within an organization (users, custodians, stewards, etc.)
- Responsibilities are becoming more formal, and are being incorporated into job descriptions

CISO Responsibilities*



The Rise of the Privacy Officer*

	2012		2014
CISOs	92%	→	96%
CPOs	18%	→	29%

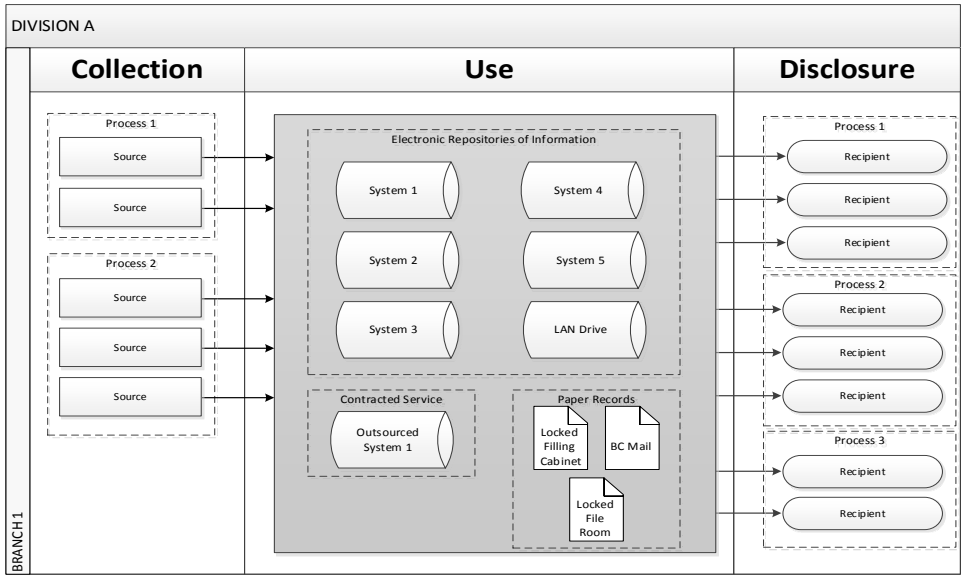
*Deloitte-NASCIO Cybersecurity Study (2014)

Inconsistent awareness of data flows and assets

Inventories support focus and prioritization

- Most organizations do not have an enterprise-wide inventory of key data flows and inventories
- Risk-based data protection requires an understanding of data throughout its lifecycle (collection, use, storage, access/disclosure and disposition)
- High-level data-flow diagrams and inventories, combined with classification, can be a critical tool in prioritization and resource allocation

Data flow diagram (example)

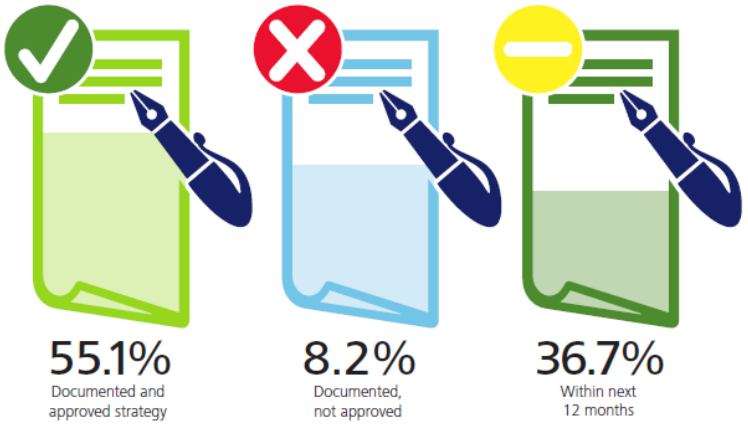


Lack of priority for data classification & protection

Data protection is poorly understood and not widely adopted

- Organizations are resource-constrained, making a coordinated, risk-based approach to data protection seem difficult to implement
- Focus is often on program management and/or major IT and business transformation program delivery
- Visibility across the organization is variable (strategy, monitoring, reporting, remediation, etc.)

US States with Approved Strategies*



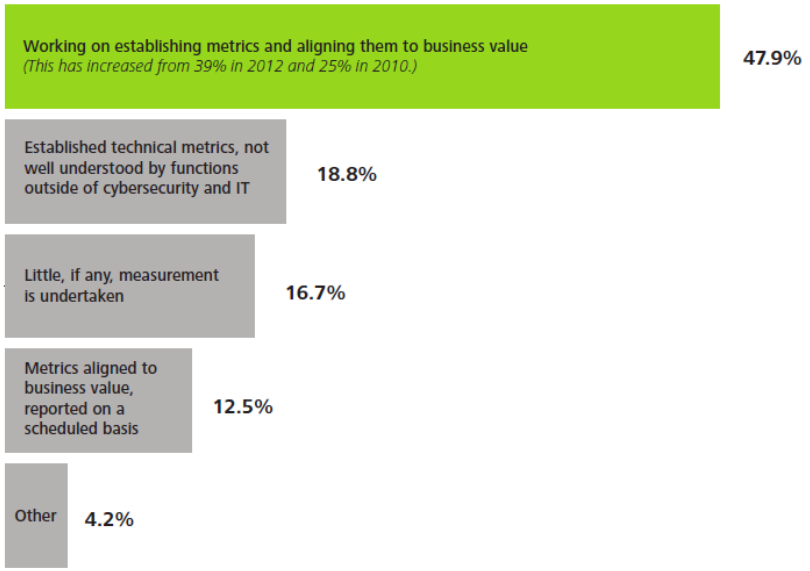
*Deloitte-NASCIO Cybersecurity Study (2014)

Inconsistent data protection practices

Examples of good practice exist, but are often not consistent across the organization

- Within most organizations there are excellent examples of leading practice with respect to data security and privacy
- These practices are often not consistently deployed leading to significant variability in the level of risk across the organization
- Monitoring and reporting on data security metrics provides greater visibility to areas of good practice and can also support improved consistency

Effective measurement & reporting are works in progress*



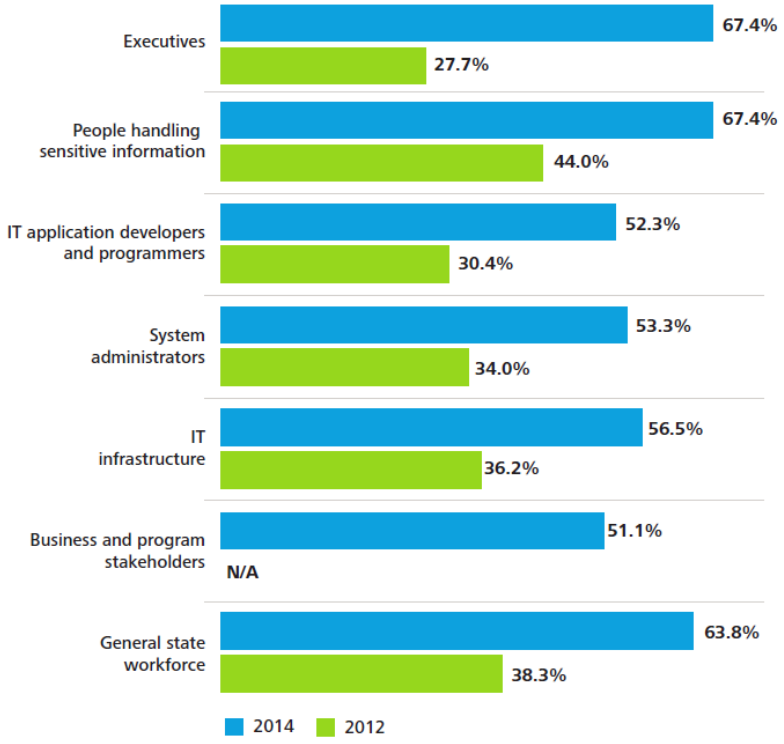
*Deloitte-NASCIO Cybersecurity Study (2014)

Working in the “grey zone”

Effective data protection is a result of numerous decisions made on a daily basis

- Clear policies and procedures are often in place with respect to open data and data that is understood to be highly sensitive
- With increased potential for data linkage, data integration, analytics and visualization, the challenge is often in understanding how new data products should be classified and managed
- Sensitivity of aggregated information can often be context-specific
- De-identification doesn’t eliminate the risk (however, the risk can be quantified)
- Training and awareness are critical in supporting risk-based decision-making

Focus on training at all levels is increasing significantly*



*Deloitte-NASCIO Cybersecurity Study (2014)

Data protection programs

Strategies for getting it right

A risk-based approach

Key considerations for data protection

1. Focus on Ministry-wide risk mitigation

Develop a Ministry-wide assessment of risk and avoid siloed solutions to data security and data protection. Central coordination can facilitate an enterprise view of risks and potential threats.

2. Build and maintain a comprehensive inventory of "crown jewels"

Allocate resources to the identification, classification and protection of key data assets.

3. Focus on defining threat scenarios and implementing solutions to secure information

Understand internal and external threat scenarios to support the identification and implementation of solutions to secure data in transit, at rest, in use.

4. Establish an information protection program

Develop an information protection program that includes governance, people, policy/process, technology, risk assessment, communication, training/awareness and measurement and reporting to secure critical information

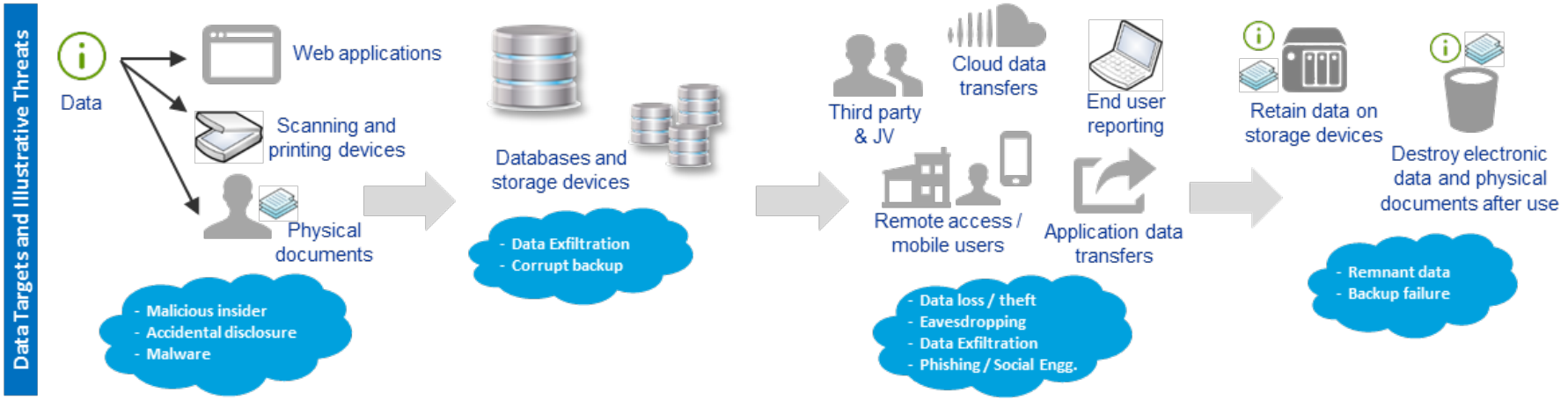
5. Consistently execute security fundamentals

Organizations need to consistently execute security capabilities (e.g., patching, access management, security monitoring, incident response). A lack of a focus on the fundamentals reduces the ability to protect critical data.

Managing data risk across the lifecycle

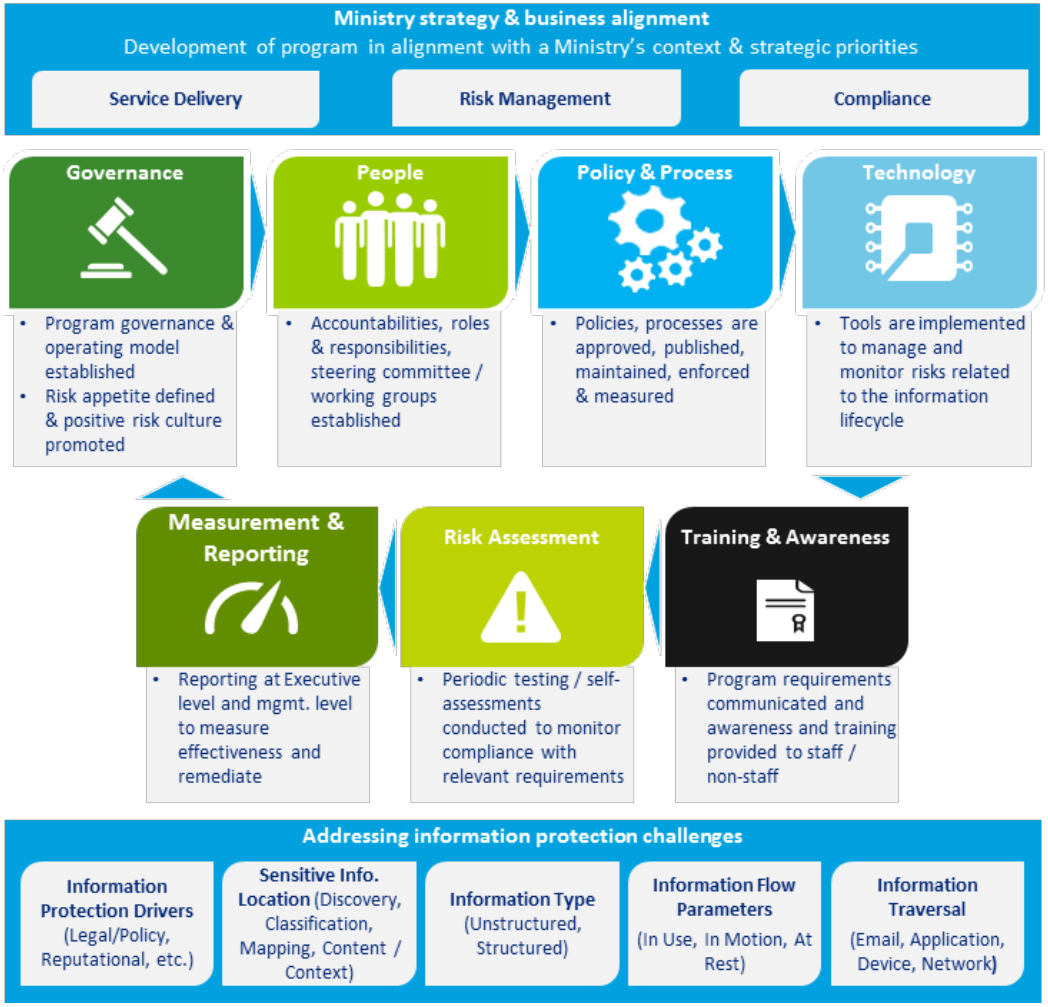
Identify risks and mitigation strategies at each stage

Information Collection	Information Storage	Information Usage and Sharing	Information Retention and Destruction
Critical information collected as part of organization's day-to-day operations via direct interaction, application forms, third parties, etc.	Collected information stored across multiple solutions such as databases, laptops, shared drives, backup locations, third party storage for further use by applications / users	Critical information is transmitted from storage solutions for processing on internal and external servers, applications, end-user devices & other devices within and outside the network	Critical information is retained or destroyed per regulatory, internal compliance or business requirements, using electronic or physical media for retention



Data protection programs

Formalize your approach and focus on the fundamentals



Accountability and governance

Ensure clarity with respect to roles & responsibilities (illustrative)

Information Protection Capabilities

Identify		Protect			Detect	Respond	Recover
Governance Risk & Compliance	Policy & Standards	Data Protection (in motion, at rest, in use)	Identity & Access Management	Vendor Management	Log Monitoring & Reporting	Incident Management & Response	Disaster Recovery
Asset / Info. Ownership & Inventory	Info. Classification / Data Mapping	Application Protection	Records Management	Human Resource Management		Records Discovery	
Training & Awareness		Infrastructure Protection	Physical Security	Threat Intelligence			

The journey from here
Concluding comments

- With increased focus on information management and protection, a right-sized data protection program is critical
- Utilize existing guidance and tools to establish clear objectives, governance, accountabilities and processes for data protection
- Start by understanding current maturity and take a risk-based approach to enhancements
- Build on existing capabilities, tools and successes where possible to maximize investments to date
- Communication, monitoring and reporting ensure appropriate visibility and priority are maintained

Deloitte.