

Data leakage protection services

Fostering trust, building eminence, and avoiding headlines

The security of confidential information is key to stakeholders' trust

The security of confidential information is key to stakeholders' trust. Economic and competitive pressures have transformed the business landscape – and in the process, created profound new challenges. Outsourcing, offshoring, partnerships, mobile employees and customers have blurred organizational boundaries and complicated information management. Sharing information is a strategic need for organizations seeking innovation and collaboration. At the same time, protecting an organization's intellectual property is vital to its long-term survival.

Privacy and corporate regulations set ground rules for how organizations may collect, use or disclose personal and confidential information in the course of their business activities. Regulations give individuals the right to know about security breaches and correct their personal information.

The challenge

Organizations have always had to deal with personal and confidential information. However, the volume and speed of electronic information passing through the organization and its boundaries today make data leakage and theft a considerable challenge. Some of these challenges are:

- Knowledge workers are increasingly open, tech savvy and willing to share information. This willingness combined with the nature of our interconnected world exposes organizations to an extraordinarily high risk of damage to reputation. Creating and delivering a consistent awareness and training program can be an enormous challenge.
- Organizational boundaries are beginning to blur. Many organizations are growing through acquisition and integration to serve their global communities. This results in the processing, disseminating and

storage of sensitive customer information and intellectual property in a wide range of systems. This highly fluid and complex environment makes it challenging to know who has what information, how it is being managed and how it is made accessible.

- Outsourcing and off-shoring enhance operational efficiencies but often result in moving client and other confidential information into less known environments that may not have adequate controls.
- Organized crime has shifted its focus towards corporations and governments. Breaches and attacks are increasing both in magnitude and sophistication. This demands an adaptive approach to information security that can detect and respond to evolving attacks.
- Increasing reliance on the internet, electronic communication and social networking tools promises new possibilities, as well as, fatal vulnerabilities when they are not proactively managed.

The solution

The solution must begin with a few key ingredients. The first ingredient is a multi-disciplinary team equipped with knowledge in risk management, business processes, information technology, security and privacy.

Next, you will need the support of the business executives to experience true success.

Finally, a clear and well-defined approach including the right tools and experience will provide a solid support structure for any of your data protection initiatives.

Once your key ingredients have been established, you can then begin to understand your current operating environment, implement controls and acquire the right capabilities to protect your information assets. The rest is performed through the following five step process:



I. Know your data

Primary to protecting your information assets is to understand what information you have, where it is, its business value and who has access to it. It is also important to know how information flows in and out of your organization to your business partners, government agencies, employees, customers and competitors.

Many organizations are unaware of the information they possess and their critical importance to their ongoing business activities. As such, identifying sources and copies of information inside and outside of the organization boundaries is critical. These sources can be structured or unstructured data in various forms, including endpoint devices, servers, archives, backups and prints.

By using business processes, software applications, customers and business partner information, auto-discovery tools, interviews and workshops, it is possible to obtain an inventory of the organization's information assets.

Once the inventory is established, you must then classify the data. Data classification is the process of classifying information based on its operational and regulatory value. This exercise can produce instant and powerful results that provide a demonstrable improvement in the way that client data is protected.

II. Know your data lifecycle

Once data is discovered it is important to understand its lifecycle from point of origin through processing, maintenance, storage and disposal. Gaining a good understanding of the lifecycle of the data and its related controls at each stage clarifies many of the threats and vulnerabilities your organization may face.

III. Know your channels

Data is seldom stagnant. It continuously flows throughout the organization and beyond. Identifying the channels used by the organization to collect, process and

distribute information is a necessary step in understanding the threats, vulnerabilities and risks.

The first three steps provide a clear understanding of the current state of data protection in the organization.

IV. Implement & Monitor Controls

Armed with knowledge of the existing vulnerabilities, threats and risks, it is time to implement the necessary controls. These controls fall into three main categories of preventive, detective and corrective controls that protect:

- Endpoints such as desktops, laptops, mobile devices, software applications, fax machines, printers and other systems
- Channels such as internet, network, phone and email
- Data lifecycle such as creation/caption, organization, processing, storage and disposal

Constant monitoring and measurement of controls is necessary for continuous improvement. As a result, an adaptive approach is needed to evolve with changing threats and risks.

V. Acquire Capabilities

To keep up with shifting threats, it is necessary to acquire the requisite capabilities. These capabilities allow your information security to evolve with the challenges and prevent undesirable incidents proactively. The primary and requisite capabilities are:

- Information governance
- Information management
- Access and identity management
- Enterprise application security management
- Communication and messaging security management
- Risk management
- Privacy management
- Fraud management
- Security training and awareness

Why Deloitte?

Our multi-disciplinary data protection team has in-depth knowledge and experience in business, regulatory and operational risks and a proven track record in solution implementations that can make the best use of limited resources.

Managing risk from the boardroom to the network

To learn more about how our security professionals can help your business succeed in information protection, please contact

Global Leader
Adel Melek
(416) 601-6524
amelek@deloitte.ca

Andreas Faruki
(416) 601-4693
afaruki@deloitte.ca

Nick Galletto
(416) 601-6734
ngalletto@deloitte.ca

Reza Kopae
(416) 601-5938
rkopae@deloitte.ca

www.deloitte.ca

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 7,600 people in 56 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. The firm is dedicated to helping its clients and its people excel. Deloitte is the Canadian member firm of Deloitte Touche Tohmatsu.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms have any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.