Document management before & after a data breach

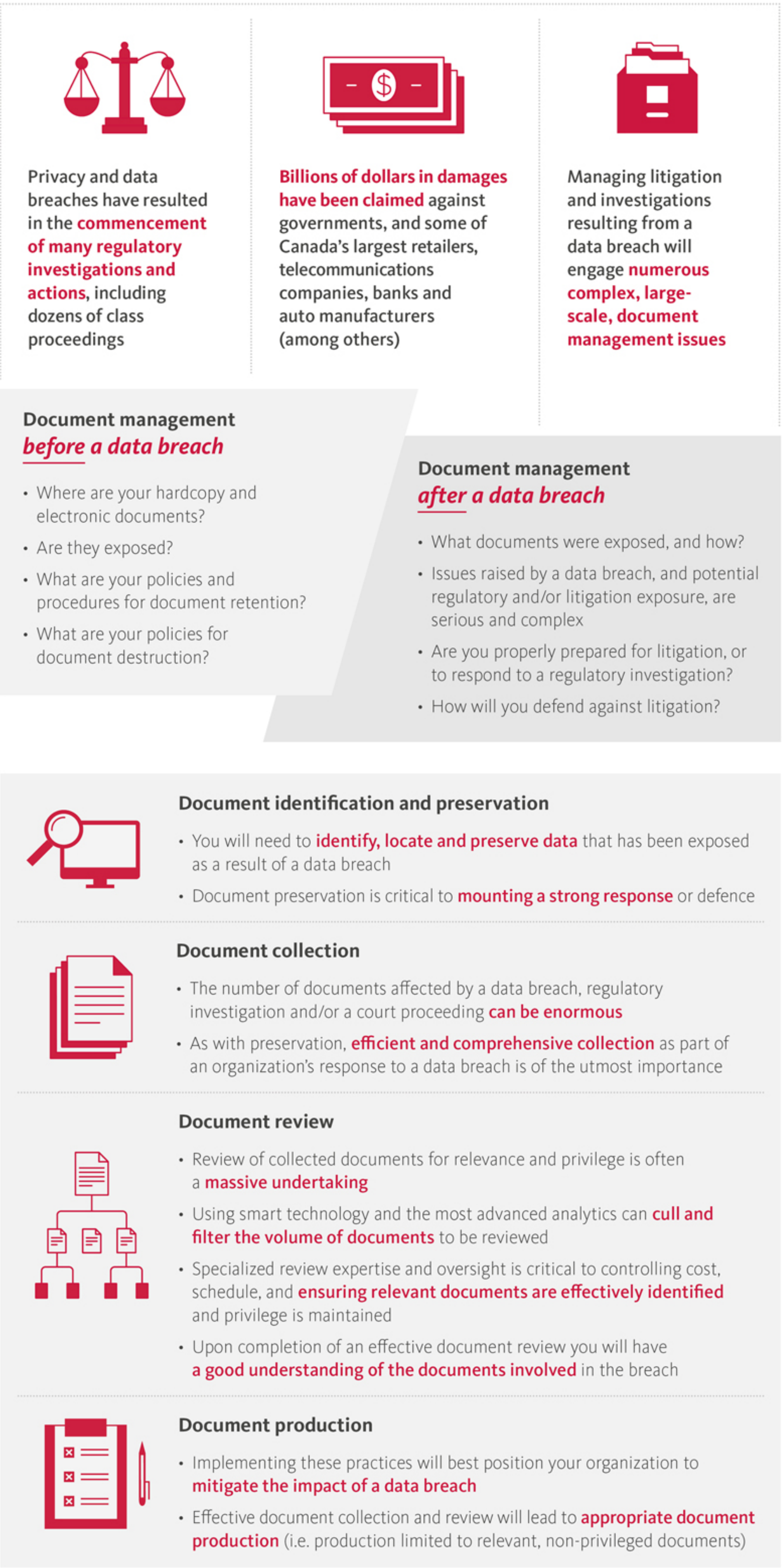
MAY 17, 2017 1 MIN READ

Related Expertise

- Privacy and Data Management
- Professional Services
- Regulatory Investigations

Authors: Geoffrey Hunnisett, Shelby Austin (Deloitte), Sarah Millar

The number of documents involved in a data breach investigation or litigation can be immense; proper preparation and response is critical. The below infographic highlights what is essential to document management when dealing with a data break investigation or subsequent litigation.



Privacy and data breaches have resulted in the **commencement of many regulatory investigations and actions**, including dozens of class proceedings

Billions of dollars in damages have been claimed against governments, and some of Canada's largest retailers, telecommunications companies, banks and auto manufacturers (among others)

Managing litigation and investigations resulting from a data breach will engage **numerous complex, large-scale, document management issues**

Document management *before a data breach*

- Where are your hardcopy and electronic documents?
- Are they exposed?
- What are your policies and procedures for document retention?
- What are your policies for document destruction?

Document management *after a data breach*

- What documents were exposed, and how?
- Issues raised by a data breach, and potential regulatory and/or litigation exposure, are serious and complex
- Are you properly prepared for litigation, or to respond to a regulatory investigation?
- How will you defend against litigation?

Document identification and preservation

- You will need to **identify, locate and preserve data** that has been exposed as a result of a data breach
- Document preservation is critical to **mounting a strong response** or defence

Document collection

- The number of documents affected by a data breach, regulatory investigation and/or a court proceeding **can be enormous**
- As with preservation, **efficient and comprehensive collection** as part of an organization's response to a data breach is of the utmost importance

Document review

- Review of collected documents for relevance and privilege is often a **massive undertaking**
- Using smart technology and the most advanced analytics can **cull and filter the volume of documents** to be reviewed
- Specialized review expertise and oversight is critical to controlling cost, schedule, and **ensuring relevant documents are effectively identified** and privilege is maintained
- Upon completion of an effective document review you will have **a good understanding of the documents involved** in the breach

Document production

- Implementing these practices will best position your organization to **mitigate the impact of a data breach**
- Effective document collection and review will lead to **appropriate document production** (i.e. production limited to relevant, non-privileged documents)

<> Add this infographic to your website

Download infographic

Add this infographic to your website using the following HTML

```
<a href='https://develop.osler.com/en/resources/governance/2017/document-management-before-after-a-data-breach' rel='nofollow'><img src='https://develop.osler.com/osler/media/Osler/infographics/privacy-data-management/document-management-before-and-after-a-data-breach.jpg' width='780'></a><br/><a
```