iManage | DocsCorp

Data Loss Prevention: Protect information and reduce the risk of a data breach

Smart. Secure. Integrated.

> "There are two types of companies: those that have been hacked, and those who don't know they have been hacked."
>
> **CISCO CEO, John Chambers**

Companies are generating, collecting, and storing more information than ever. Today, the biggest challenge they face is securing and managing this information, so it doesn't end up part of a data breach.

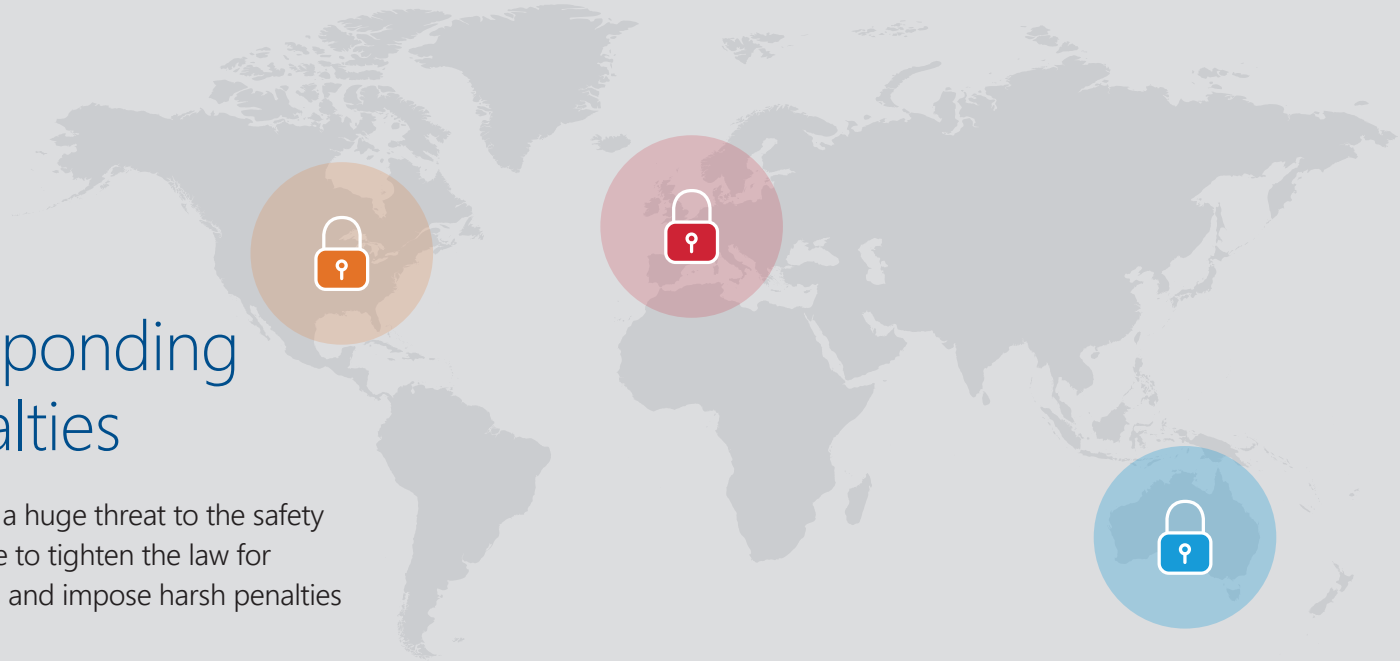
Unfortunately, not every data breach can be prevented. Many are the result of human error, like emailing the wrong person or sharing the wrong file. Phishing attacks are on the rise, and cybercrime is constantly evolving. What is possible, however, is reducing the likelihood of a breach while ensuring that, if one should happen, the damage is minimal.

Data breaches remain a significant problem in 2019

Who	**34%** involved internal actors
What	**24% of breaches involved human error***
Where	**53%** of breaches were network hacks
When	**59%** of breaches took months or longer to discover
Why	**71%** of breaches were financially motivated

Source: Verizon's 2019 Data Breach Investigations Report

*Source: IBM 2019 Cost of a Data Breach Report



Regulators are responding with tougher penalties

Governments understand cybersecurity is a huge threat to the safety and privacy of their citizens. They continue to tighten the law for businesses who hold valuable information and impose harsh penalties when it is not properly protected.

- **US** – Nearly all US states are strengthening their data breach notification laws. The California Consumer Privacy Act (CCPA) will go into effect on January 1, 2020. It includes limits on the collection and sale of personal information by businesses, as well as increased rights and protections for consumers. Different industries have their own regulations - the Health Insurance Portability and Accountability Act (HIPAA), for example, covers medical data.

- **Canada** – Organisations subject to Canada's notifiable data breach law, the Personal Information Protection and Electronic Documents Act (PIPEDA), are obligated to report certain types of privacy breaches.

- **Europe and the UK** – The General Data Protection Regulation (GDPR) completely changed how businesses collect, store and process the personal data of EU citizens. The GDPR obliges data processors and controllers to follow strict security and protection guidelines to ensure personal data is not leaked or disclosed – even accidental exposure is defined as a breach under the new law. Under the GDPR a company can be fined €20 million or 4% of global revenues, whichever is higher.

- **Australia** – The Notifiable Data Breach (NDB) scheme requires all businesses in Australia that experience a data breach to report it to the regulatory body that oversees enforcement within 30 days.

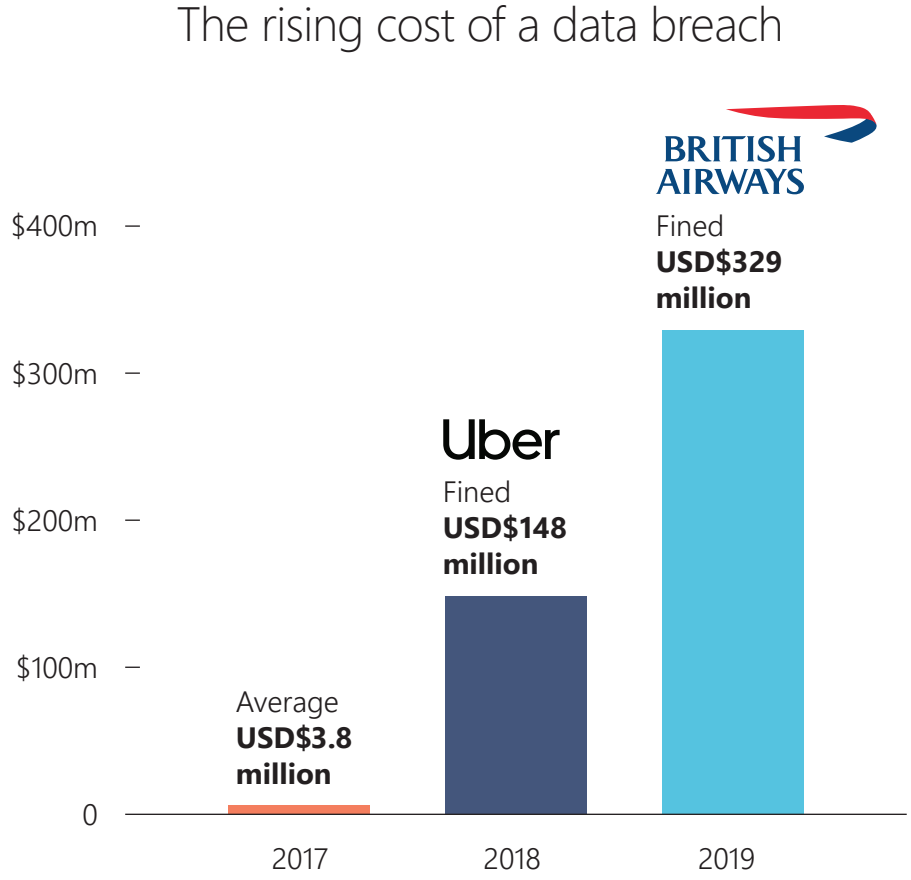
The costs of a data breach have increased dramatically

Companies including Equifax, Facebook, and Yahoo have been fined hundreds of millions of dollars after serious data breaches affected millions of users. In the past, the risk of regulators imposing fines was low. Now, we are witnessing regulators issuing massive fines and wielding increased power over businesses that experience a breach.

Brand reputation – a data breach could seriously impact a brand's reputation, leading to a loss of existing and future clients. Other effects could be unwanted media attention as well as legal action for professional negligence and other lawsuits.

Loss of confidence – clients expect firms to implement measures and policies to protect their data. If a client learns the firm has suffered a data breach, it could lead to an irreversible loss of confidence, resulting in the client taking their business elsewhere.

Regulatory penalties – a growing body of government and industry regulations are establishing rules and standards for the protection of client data. Failure to comply can result in severe financial penalties. The USD$329 million fine issued by the GDPR regulator to British Airways proves these penalties aren't just idle threats.



With over 124 billion* business email sends on an average weekday, an email data breach is inevitable

Under global data protection regulations, these are the email data breaches that could cost your business millions.

Missent emails
Sending an email to the wrong person accidentally – usually because of a simple mistake like Outlook autofill suggesting the wrong 'John' or 'Jane.'

Wrong information
Unknowingly sending information in the email body or an attachment to the wrong person, or a person who is not authorised to receive it.

Spear phishing and phishing attacks
Clicking on a link or responding to an email that purports to be from a trusted contact (spear phishing) or a reputable company (phishing) and revealing personal information, including passwords and/or credit card numbers.

Metadata leaks
Metadata tells the reader more than what's on the page, like who created the document, how long was spent editing it, and where the document is saved. Certain types of metadata, like author properties, can contain personal information.

When careless is more costly than criminal
24% of data breaches are the result of human error.

Source: IBM 2019 Cost of a Data Breach Report

*Source: Radicati Group report on email traffic.

1. **Define policies:** In the cleanDocs panel inside Security Policy Manager, users can define the email addresses that can be communicated with for each client, matter, or project.
2. **Manage metadata:** In the cleanDocs panel inside Security Policy Manager, users can define the default metadata cleaning policy for each client, matter, or project.
3. **Monitor email:** cleanDocs checks each outgoing email - regardless of whether a document is attached - and confirms it meets the rules defined in Security Policy Manager.
4. **Immediate action:** The user is instantly notified if there is an issue, so incorrect or unauthorised recipients can be removed, allowing the email to be sent without delay.

iManage and DocsCorp have partnered to help reduce the risk of email data breaches

iManage Security Policy Manager enables an organisation to define, store, and implement regulatory or corporate information policies and ethical walls governing content security access. Security Policy Manager actively secures and protects content and communications based on centrally defined policies.

cleanDocs from DocsCorp checks all outgoing emails in Outlook to confirm that document metadata is removed and prompt the user to confirm they are emailing the right person. These checks support both desktop clients and mobile devices. Importantly, cleanDocs provides this security regardless of whether a document is attached, since sensitive information isn't always in a document. Often, it is in the email body itself.

How will the integration between iManage and DocsCorp benefit you?

iManage Security Policy Manager and **cleanDocs from DocsCorp** provide a unique and unparalleled security platform that extends internal document controls to all email communication, whether those emails are internal or external to your organisation.

Key benefits:

- Align your client data leak prevention policies to document and email access
- Add to your organisation's security capabilities in order to attract and retain more clients
- Sleep well knowing company emails are monitored for fraudulent activity or human error

iManage and DocsCorp offer a complete suite of security and governance solutions to protect your organisation and its data

iManage

iManage Security Policy Manager
Manage need-to-know security, ethical walls, and email security policies at scale.

iManage Threat Manager
Identify and neutralise active breaches on your networks using AI.

iManage Records Manager
Manage physical end electronic records and legal holds.

iManage Conflicts Manager
Identify conflicts of interest to then define ethical walls.

iManage Business Intake Manager
Manage new client onboarding including KYC and conflict checks.

LEARN MORE

DocsCorp

cleanDocs
Clean hidden metadata and prompt users to confirm what they are sending and who they are sending it to.

cleanDocs server
Extend email security to mobile devices, including smartphones, tablets, and browsers.

compareDocs
Compare versions of documents to isolate accidental or fraudulent document editing and confirm Microsoft Word Track Changes data is correct.

pdfDocs
Reliably redact sensitive information, apply document security, and convert to secure document binders.

LEARN MORE

Summary

The modern business must manage several security threats day in and day out – from savvy cybercriminals to employees who make innocent mistakes in the course of a busy day. Considering the average cost of a data breach to a company is USD$3.86 million, it pays to put the right protection in place.

A comprehensive and seamless approach to managing an array of risk factors is needed for true data protection. That's why iManage and DocsCorp security solutions are designed to work together, creating seamless lifecycle protection for data. Help protect your business from a breach by segregating information based on policy types and access, minimising the risk of human error, and sanitizing shared documents – in one simple, integrated approach.

DocsCorp

DocsCorp designs easy-to-use software and services for document professionals who use enterprise content management systems. We provide solutions for metadata removal, document processing, PDF manipulation, and document comparison.

iManage

iManage transforms how professionals in legal, accounting and financial services get work done by combining artificial intelligence, security and risk mitigation with market leading document and email management.