

Does your current SuperStream & STP process properly protect your clients' and employees' data?



With the release of the Notifiable Data Breach scheme in February 2018, organisations regulated by the Privacy Act are responsible for ensuring their payments systems are secure – these organisations include any Government agencies, businesses and not-for-profit organisations with **annual turnover of \$3 million or more**.

Employers, payroll providers and super funds, as recipients, retainers and transmitters of a huge amount of personal information, must have strict measures in place to ensure the security of their data, particularly customers' and employees' personal and financial information, or **risk fines of up to \$2.1 million**, in addition to the loss of trust and damaged reputation with customers and suppliers.

Understanding the Risks

According to the Notifiable Data Breaches Quarterly Statistics Report: 1 October – 31 December 2018, the Office of the Australian Information Commissioner (OAIC) received 262 data breach notifications for the same period, compared to 242 from 1 April to 30 June 2018.¹

The type of personal information most commonly involved in data

breaches was contact information, followed by financial details and identity information. All these types of information are kept and transmitted by employers and super funds.

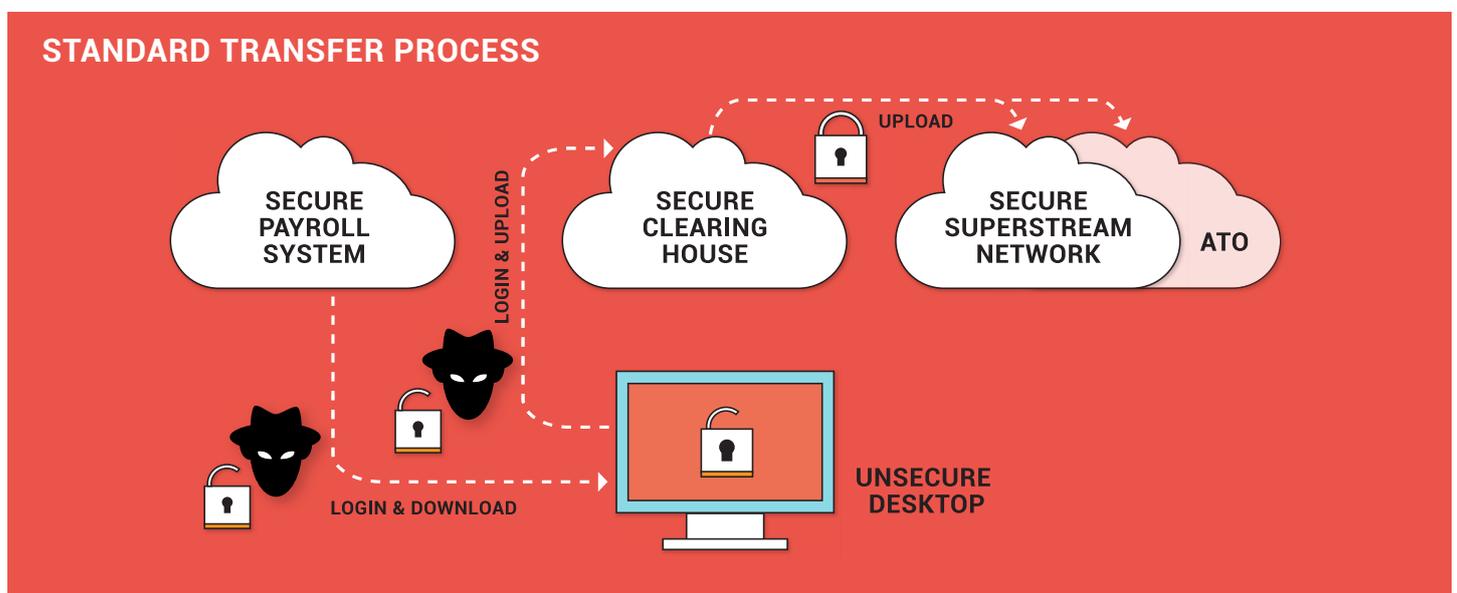
Overall, **malicious or criminal attacks** accounted for 168 data breaches in the last quarter of 2018, or **64% of the total**, while **human error** accounted for 85 data breaches, or **33%**. System faults accounted for just nine data breaches, or 3%.

How Personal and Private Data Could Be Exposed

Many employers today utilise a portal process to send single touch payroll (STP) data to the ATO and SuperStream data to the superannuation funds. **See diagram below.**

Data is downloaded from a secure payroll system and onto a desktop, or share drive, and then uploaded to a secure portal for transmission to the ATO and superannuation funds.

And herein lies the risk: with data being downloaded onto a desktop, it is potentially exposed to malicious or criminal attacks, or human error – the leading causes of data breaches in Australia.



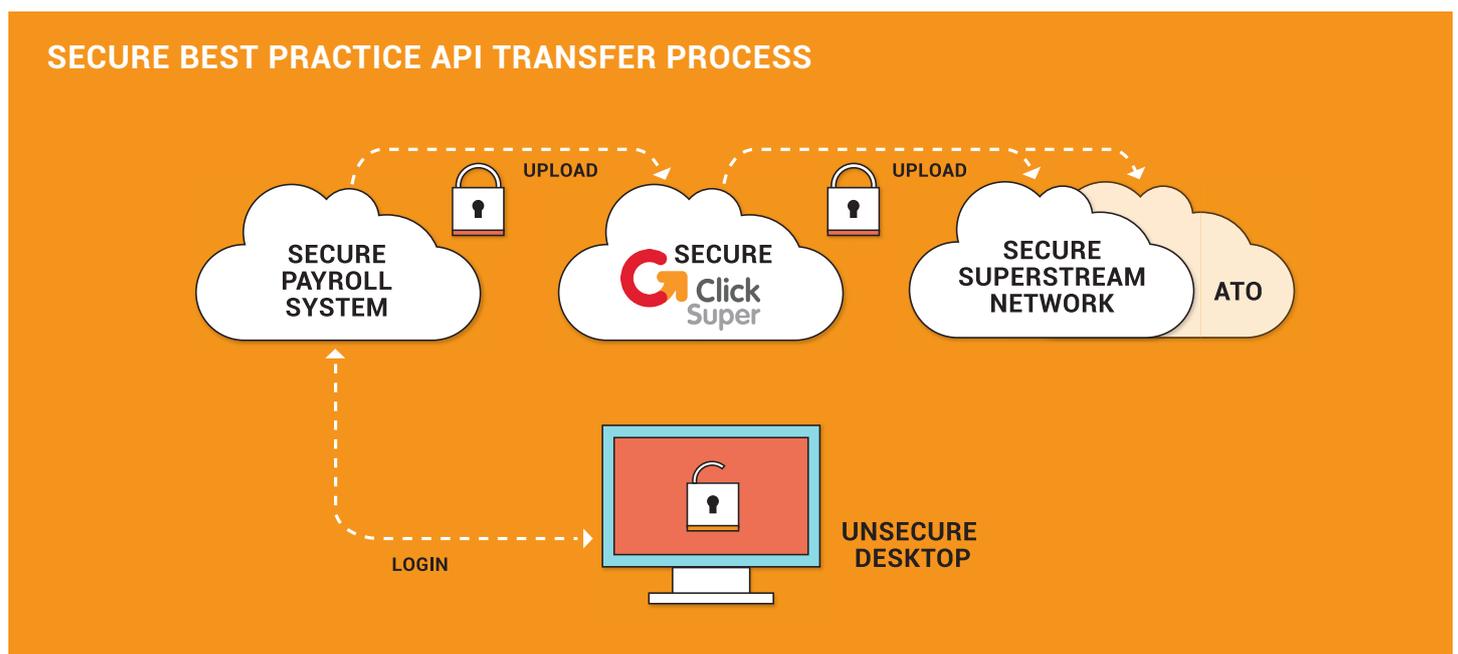
How to Protect Your Data

To help protect employees' data from cybersecurity risks, ClickSuper provides employers, payroll providers and superannuation funds with a **secure API** to prevent personal and private data from being exported outside of a secure business system.

A user logs in to the payroll system and data is sent to the ClickSuper platform through a secure connection. ClickSuper processes STP directly to the ATO and sends SuperStream data files to the superannuation funds via the SuperStream network. All personal and financial data is sent via ClickSuper's secure data centre. Data is never loaded onto a user's desktop outside of the password protected system.

The key benefit of ClickSuper is that data can never be hacked on an unsecured desktop or shared drive. This helps to defend against the number one source of notifiable data breaches: malicious and criminal attacks. It also helps to minimise human error, including the unauthorised disclosure of data, the loss of data stored on a desktop or mobile device, and the loss of data contained in paperwork.

The ClickSuper API solution therefore dramatically reduces the risk of data security breaches and identity theft. Identity crime is one of the most common crimes in Australia. The estimated direct and indirect cost of identity crime in Australia in 2015–16 totalled \$2.65 billion. This includes \$2.1 billion in losses suffered by Australian government agencies, businesses and individuals.²



¹ Notifiable Data Breaches Quarterly Statistics Report: 1 October – 31 December 2018 • ² Identity crime and misuse in Australia 2017

ClickSuper provides industry leading secure, simple and cost effective SuperStream and STP solutions for Superannuation funds, Payroll Providers and employers.

ClickSuper holds an Australian Financial Services Licence (No.337805) and is a signatory to the Superannuation Data and Gateway Service Standard and is one of only 9 active SuperStream Gateways.