

Consumer Insights

Digital Fraud



THE CONSUMER'S
RIGHT TO CHOOSE

Digital data breaches affect thousands and cost millions every year in Australia. The solution to digital fraud could be as simple as pen and paper.

Data breaches have gained widespread attention as businesses of all sizes become reliant on digital data and cloud computing. In 2015, there were 110 data breaches notified to the Office of the Australian Information Commissioner. Some of the major companies attacked include:

Aussie Travel Cover had 870,000 customer information records exposed with sensitive customer information such as names, addresses and partial credit card details.

.....

Websphere, a commerce software used by retailers, saw Kmart and David Jones' customers data - names, email addresses and home addresses - stolen.

.....

In July 2016, more than 22,000 people have received fake Telstra bills via email offering a refund as part of a phishing scam.

IBM and the Ponemon Institute report that in 2015, the average total cost of a data breach for Australian companies participating in their research was \$2.82 million (or \$144 for each lost or stolen record or file). With the average number of breached records being 19,788. A majority of company information breaches are due to malicious or criminal attacks and these types are the most expensive to remedy.

Although the financial, services, industrial and energy companies tend to be hit harder and incur higher remediate costs, companies in the public sector, transportation and retail sectors are still affected by the issue.

According to Stu Sjouwerman, founder and CEO of cybersecurity firm KnowBe4, such attacks have been happening with increasing frequency around the world but are often not made public for PR reasons.³

Globally the digital fraud issue has been coming to the attention of corporations who are opting for paper records. As Glenn Reynolds, University of Tennessee Law Professor points out, paper records are inherently more secure from attack than electronic records. "To steal, or hold for ransom, 10 million electronic user records... all you might need is a cracked password and a thumb drive. To steal that many records on paper, you'd need a fleet of trucks and an uninterrupted month."



“Paper has become our lingua franca, our fallback and standby. In our new digital universe, we have peculiarly seen a retro explosion of paper.”

Dr Abigail Zuger, M.D.

“From intelligence agencies to hospitals, paper records are the killer app for stopping hackers.”

Moving from paper to electronic records and trying to keep one step ahead of digital data breaches is not only a continuous and costly exercise but one that causes frustration and errors among its users - who often resort back to using paper.

The Health sector is under pressure to go digital, however errors are occurring. A study of electronic health recording (EHR) implementation on surgical residents work load showed that even after 6 months, the time to complete patient documentation was significantly longer with digital solutions than with paper records. In addition, most residents felt their risk of making medical error was higher using electronic documentation.

The drive to expensive electronic bookkeeping (\$29 billion over 10 years for the US health sector) is not stacking up when reviewing time and accuracy measures.

Reputed medical professional, Dr. Zuger has covered the issues and points out, the drive within the medical community to compile and rely on electronic information whilst prompted with honourable intentions to improve patient care, reduce administrative costs and lower medical errors has failed. As she and her colleagues struggle daily to accomplish these goals, they succeed through the simple expedient of paper.

Sometimes the most innovative measures are using the best tool to do the best job.

Sources

1. Financial Review, 2016.
2. itnews, 2015.
3. CBC, February 2016.
4. USA Today, February 2016.
5. Wormer et al, 2015.
6. HealthcareIT News, July 2014.
7. New York Times, December 2015.