Loss Event

Commonwealth Bank of Australia
EL0202 - System Security External - Wilful Damage
AU - Australia

BL0301 - Retail Banking
AUD Not Identifiable LOSS | Australian Dollar
Asia / Pacific

Banking

Commonwealth Bank of Australia documents exposed in breach at printer company

Documents belonging to Commonwealth Bank of Australia (CBA) which contained the details of administrator credentials for two printer models used by the bank have been exposed in a data breach at printer company Ricoh Australia.

The printers involved are known as multi-function devices (MFDs). Along with printing, these devices include email functions, remote management features and built-in web browsers, potentially exposing them to malicious attacks.

The documents leaked, known as run-up guides, contained information for Ricoh technicians setting up new MFDs. They included technical details such as how the printer has been configured, how to encrypt the hard drive and how to update its firmware.

According to databreachtoday.com, although most guides did not contain usernames and passwords, a small number of the leaked guides contained Lightweight Directory Access Protocol and Active Directory credentials. These are used to configure who can use an MFD and the level of access for users.

CBA's documents date from January 2017. The documents contained simple mail transfer protocol (SMTP) credentials, which control access to the device's email inbox, for two Ricoh models used by CBA, the MPC6503 and the MP8003. The documents also contained two sets of administrator credentials and one supervisor account, databreachtoday.com reports.

A CBA spokesperson said that the bank had immediately changed the passwords and that none of its systems were compromised as a result of the breach.

According to security consultant Nick Ellsmore, the risk from the breach is low. An attacker would need to have network access to gain access to the MFDs, so the main risk is from internal employees. Potential attacks could include modifying the MFD so that it sends every document that is scanned to an external email address.

Over 20 organisations were affected by the breach, including the Australian Civil Aviation Authority and the Australian Federal Police. National Australia Bank (NAB) and insurer Arthur J Gallagher have also been affected, although it has not been reported that any of their credentials were exposed.

According to Ricoh, the breach took place between 25 May 2017 and 11 July 2017. As of 24 July 2017 it is unknown how the breach occurred, but Ricoh is investigating the incident and working with its customers to deploy corrective action plans. It has also taken down the domain where the documents were stored, although databreachtoday.com reported that cached versions were still available as of 20 July 2017.

Although CBA's systems were not compromised in this incident, ORX News has included this event in its database as an example of a third party data breach.

Author Margo Kane **Published Date** 24 July 2017 **Last Update** 24 July 2017

Source(s)

Related links

http://www.databreachtoday.com/ricoh-australia-scrambles-to-fix-document-leak-a...

,

https://www.crn.com.au/news/ricoh-australia-suffers-document-leak-468963

Event

Published In Media	Date of Occurrence - From	Date of Occurrence - To	Discovery Date	Date of Recognition/Settlement
20 July 2017	25 May 2017	11 July 2017		

Loss Amount USD	Loss Amount EURO	Provision	Boundary Risk
		No	Other Risk

Industry Event	Scenario	Product	Process
	SC0023 - Cyber-Related Data Breach	PD9900 - Not Product-Related	PC1303 - Management & Monitoring

Event Closed	ORX Member	Role of Firm
No	Yes	LS0305 - Outsourcer

Cause 1	Cause 2	Cause 3
CS0106 - Actions of External Staff		

Jurisdiction / Choice of Law	Counterparty	Environmental Volatility
LS0103 - Rest of the World	LS0212 - Not Identifiable	LS0406 - Not Identifiable