GRC PROFESSIONAL
GOVERNANCE • RISK • COMPLIANCE

CONFERENCE EDITION
THE OFFICIAL MAGAZINE
OF THE GRC INSTITUTE

The State of Compliance

BOOK REVIEW

A Cautionary Tale

A review the of Adele Fergusons' *Bad Banks*

Governance, Compliance and Enforcement Reconsidered

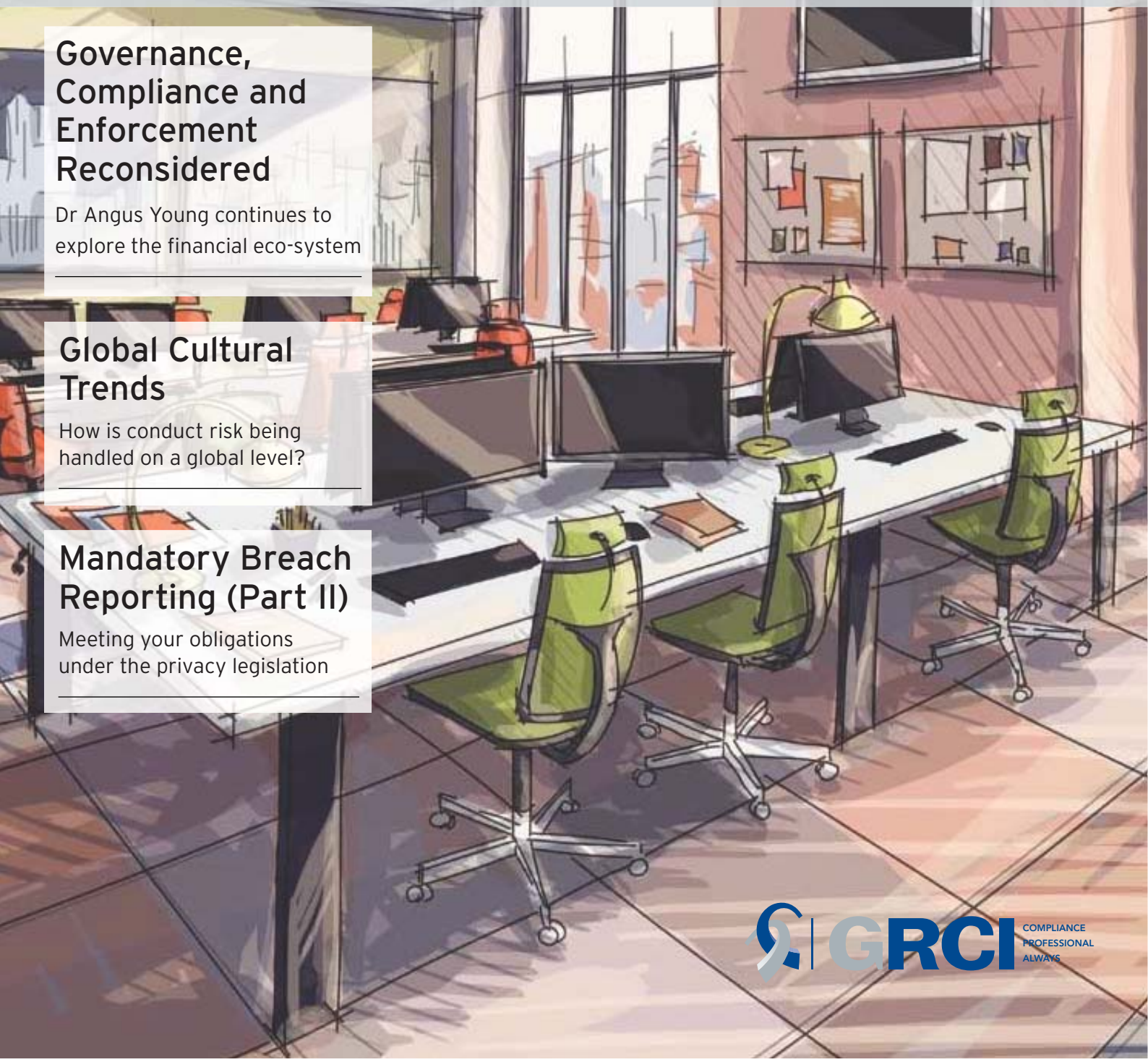
Dr Angus Young continues to explore the financial eco-system

Global Cultural Trends

How is conduct risk being handled on a global level?

Mandatory Breach Reporting (Part II)

Meeting your obligations under the privacy legislation



GRCI COMPLIANCE PROFESSIONAL ALWAYS

Annelies Moens,
Managing Director, Privcore

Mandatory data breach reporting: outcomes since reporting began

Part 2

By Annelies Moens

This article discusses mandatory data breach reporting since its commencement on 22 February 2018 and provides simple and effective steps to mitigate cyber and privacy risks.

It is Part 2 of a two-part series, first published by Legalwise. Part 1 appears in the Winter Edition of the *GRC Professional Magazine*.

The mandatory data breach reporting scheme has been in effect since 22 February 2018. In its first year, approximately 1,000 data breach incidents were reported to the Office of the Australian Information Commissioner (OAIC). Between 1 April 2018 and 31 March 2019, 964 data breaches have been notified to the OAIC, averaging almost 20 notified data breaches per week. The OAIC intends to report on a six-monthly basis going forward, with the next report due for release towards the end of the year.

Generally, two-thirds of notified data breaches are due to malicious or criminal attacks and one-third due to human error. In the malicious or criminal attack category, cyber incidents dominate. It is elucidating to break down the cyber incident category as, contrary to common beliefs, hacking only represents 8% of the problem.

For the period 1 April 2018 – 31 March 2019, the largest cause of cyber incidents were phishing attacks (39%), with a further 28% also due to compromised or stolen credentials, which may include phishing, bringing this category to a total of 67%. These statistics have been similar each reporting quarter, which suggests that targeted sectors are doing little to minimise this risk. This risk can be mitigated through the adoption

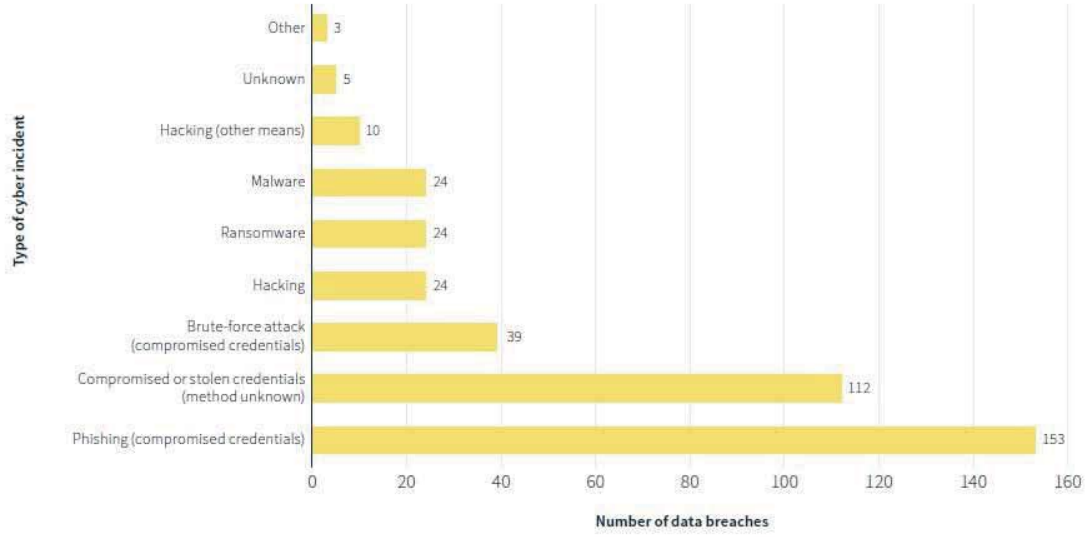


Figure 5 — Cyber incident breaches—all sectors, from 1 April 2018 to 31 March 2019

of two-factor or multi-factor authentication. With multi-factor authentication enabled, should a phishing attack cause user names and passwords to be compromised, the attacker is going to find their attempt significantly thwarted if a further step is required before gaining access to the account. In an earlier article, I discussed the differences between the types of two-factor authentication methods, with hardware tokens and software tokens being the most secure and SMS two-factor authentication being the least secure (though SMS is a little better than not having two-factor authentication implemented).

"With multi-factor authentication enabled, should a phishing attack cause user names and passwords to be compromised, the attacker is going to find their attempt significantly thwarted if a further step is required before gaining access to the account."

Multi-factor authentication is essential under the Privacy Act

Australian Privacy Principle 11 outlines regulated entities' obligations in terms of securing personal information from misuse, interference, loss and unauthorised access, modification or disclosure. It requires that "such steps as are reasonable in the circumstances" must be taken. Multi-factor authentication is a reasonable step to take to secure personal information. If that reasonable step (multi-factor authentication) is not taken, then the regulated entity is in breach of the *Privacy Act*. An interesting dialogue the Australian Information and Privacy Commissioner had with Senators during Senate Estimates hearings on 22 October 2018 supports this interpretation. The relevant parts of that exchange have been reproduced below.

Australian Information and Privacy Commissioner – Angelene Falk:

The main issues that we're seeing in terms of cyber are around compromised credentials. An email might be sent or a text sent-phishing-purporting to be from a legitimate institution and luring an individual or tricking them into providing their password or log-in information. That's why some of the messaging that we're now able to do coming out of these reports is to look at the kinds of ways that could be prevented. One way is to have multi-factor authentication in place.

Senator Jim Molan:

Do you have the authority to impose that (multi-factor authentication) on organisations, or only to suggest?

Angelene Falk:

Under the *Privacy Act*, the test is that they must take reasonable steps to protect personal information. The kinds of measures I've outlined are reasonable steps. If they fail to have those in place, an individual could make a complaint or indeed I could investigate on my own initiative.

Type of breaches that need to be reported

The intent of the mandatory data breach reporting scheme is to help those affected by a data breach to minimise the harm they may experience, whether through identity theft, reuse of stolen passwords and other credentials to compromise other accounts, financial loss, embarrassment, reputation damage or other harms. The scheme applies to all entities regulated under the *Privacy Act*. This includes federal government agencies, ACT government agencies, private sector entities with an annual turnover greater than $3 million and some small businesses regardless of turnover, such as health service providers. It also applies to otherwise exempt small businesses, if they handle tax file numbers.

"The intent of the mandatory data breach reporting scheme is to help those affected by a data breach to minimise the harm they may experience, whether through identity theft, reuse of stolen passwords and other credentials to compromise other accounts, financial loss, embarrassment, reputation damage or other harms."

"The term 'serious harm' is undefined in the legislation."

An 'eligible data breach' as defined in Part 3C of the *Privacy Act* must be notified when:

> "(a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by the entity; and
>
> (b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates."

Entities have 30 days in which to undertake their assessment. Under the General Data Protection Regulation, similar data breach notification requirements require notification to occur within 72 hours of discovery.

The term 'serious harm' is undefined in the legislation. The explanatory memorandum accompanying the Bill, however, provides examples of serious harm. This includes unauthorised access to permanent information relating to an individual that cannot be changed, such as their date of birth. It is for this reason, alone, that entities that do not require the collection of this data point should never collect it, as it escalates risk enormously. Many organisations simply need to know that someone is over 18 or an age range, which presents much less privacy risk. Disclosure of address details may also cause serious harm, especially in circumstances where domestic violence is at play or restraining orders are in effect.

There are some exceptions to notification requirements, including where action is taken to remediate before the breach is likely to result in serious harm. This could, for example, occur when an email containing personal information is inadvertently sent to an incorrect recipient, and that recipient is contacted and advised of the mistake and asked to delete it, and the sender is confident that the incorrect recipient has deleted that information.

Another important exception relates to when multiple entities are involved in the same data breach, for example involving subcontractors or vendors. As long as one of those entities has undertaken the notification, then the law treats this as having been done for all entities. A real example of this was the PageUp data breach that occurred in mid 2018, for which the OAIC received over 50 notifications, when one would have been sufficient. Contracts between sub-contractors and contractors need to address which party will undertake the notification obligations when a data breach takes place.

Should notification be required after the relevant assessment has taken place, the notification itself must set out the following:

- The identity and contact details of the entity
- Description of the data breach
- The kind of information in the data breach
- Recommendations on what affected individuals should do in response to the breach

Unfortunately, data breaches are a commonplace occurrence and the lack of care organisations are demonstrating in their stewardship of the personal information of their customers must be addressed. However, there are simple steps to mitigate and manage these risks, as outlined in this article (Part 2) and Part 1.●

About the Author

Annelies Moens, CIPT, FAICD, CMgr FIML is a widely-recognised global privacy expert and thought leader, trusted by business executives, government and privacy professionals with close to 20 years' experience. She is Managing Director of Privcore and cofounder of the International Association of Privacy Professionals in Australia and New Zealand. Contact Annelies at: operations@privcore.com or visit: www.privcore.com.