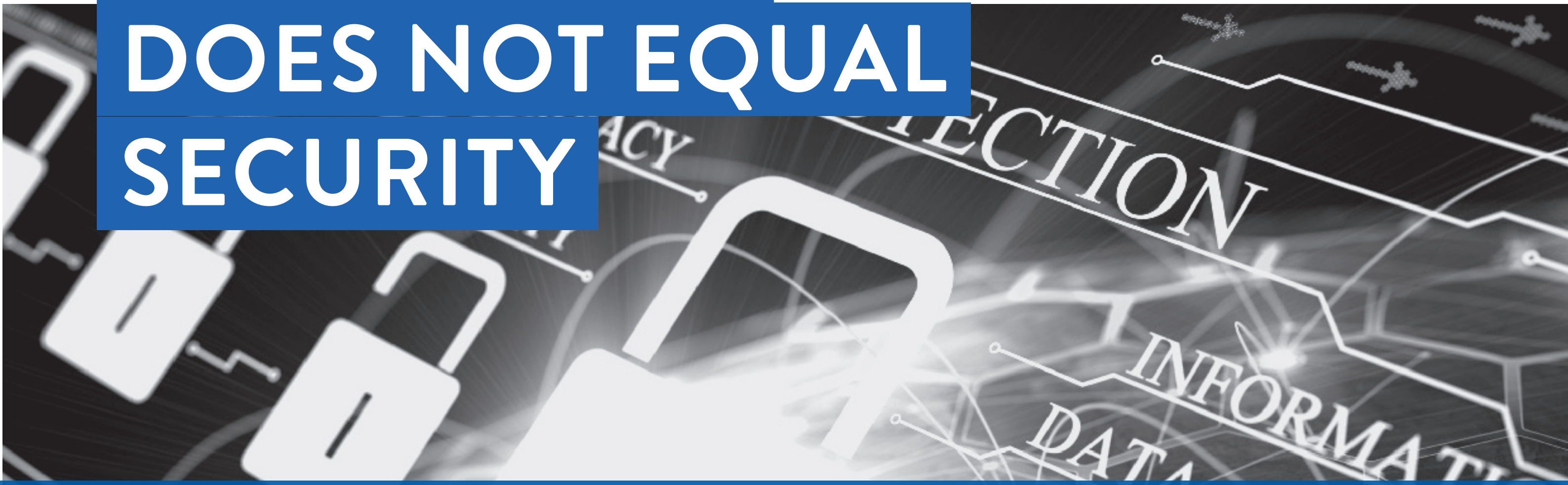
GILBERT + TOBIN

COMPLIANCE DOES NOT EQUAL SECURITY



WRITTEN BY BERNADETTE JEW

Data is fast becoming one of our most valuable corporate assets. Cybersecurity best practice is all about protecting that corporate data – protecting it not just against loss or theft, but also against unauthorised access that could lead to data manipulation or corporate sabotage.

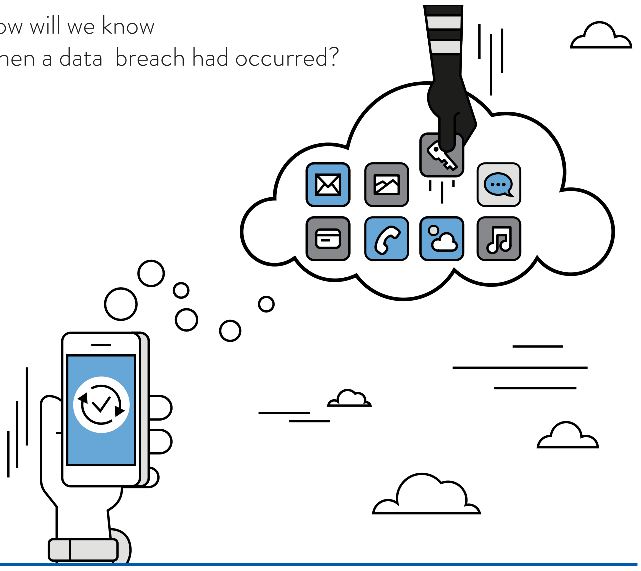
MARCH 2016

Unfortunately, corporations sometimes assume that data security is about meeting their legal and regulatory obligations – and this can lead to a very narrow focus. It results in corporate compliance and risk teams placing a heavy focus on privacy and the protection of personal information - while the security of commercial and strategic data can be at risk of falling between the gaps.

This narrow focus misses the bigger picture - compliance with laws and regulations is no guarantee as to data security. Having said that, not all data security risks are created equal – the focus needs to be on the corporation's "sensitive" data. Data can be sensitive, not just because of the need to comply with laws and regulations – but because of its commercial or strategic value, or its impact on the corporate's reputation.

A best practice approach to cybersecurity requires corporations to put their sensitive data front and centre. Cybersecurity is no longer just a compliance responsibility or a technology responsibility – it requires a much broader "data awareness" across the entire corporation around:

- which data is sensitive data?
- who has access to that data?
- how is access to that data structured, controlled, logged and monitored?
- how will we know when a data breach had occurred?



By way of example, this "data awareness" needs to be an integral component of corporate procurement processes. Procuring a new technology solution is no longer just about buying technology and delivering business outcomes. It also requires a clear focus on the underlying data that will be created or controlled or accessed by the new technology solution. Is it sensitive data? What are the access rights and controls around that data? What role will the vendor need to play in relation to the security of that data? What information does the corporation need to obtain about the vendor's approach to cybersecurity? Does the corporation need to impose any cybersecurity service levels on the vendor?

Cybersecurity is no longer just a compliance responsibility or a technology responsibility. Data awareness and cybersecurity best practice need to be embedded across the business processes of every corporation – and they also need to be embedded in the commercial arrangements with the corporation's suppliers.

Going forward, it is not going to be possible for corporations to just keep on working in the same old way – and hoping that cybersecurity will look after itself. Best practice cybersecurity requires a fresh approach to management and day-to-day business processes – with a focus on requiring every person in the corporation to play an active role in relation to cybersecurity.

Cybersecurity is less about discharging compliance or regulatory obligations – and more about the essential steps that need to be implemented across the corporation on a day-to-day basis to protect and maximize the ongoing value of the corporation's sensitive data.