DARKTRACE

Australian Notifiable Data Breaches Scheme

WHITE PAPER

Overview

With the entry into force of the Privacy Amendment (Notifiable Data Breaches) Act 2017, the Australian legislature is introducing the Notifiable Data Breaches (NDB) scheme. Effective from 22 February 2018, this legislative framework introduces rigorous and mandatory data breach notification provisions for all entities regulated by the Privacy Act 1988.

Under the NDB scheme, organisations will be obliged to notify individuals whose personal information has been subject to a data breach that is "likely to result in serious harm", and must provide recommendations to said affected parties on how to mitigate the impact of the breach. Concurrently, in the event of an "eligible data breach", the targeted organisation is also required to inform the Office of the Australian Information Commissioner (OAIC) of the incident.

The Privacy Act 1988 defines a "data breach" as unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information which is likely to result in unauthorised access to or unauthorised disclosure of that personal information. For the purposes of the NDB scheme, an "eligible data breach" refers to a security incident where the data lost is "likely to result in serious harm to any of the individuals to whom the information relates".

The NDB scheme will apply to agencies and organisations subject to the Privacy Act 1988. This includes Australian Government agencies, businesses and not-for-profit organisations with an annual turnover of A$3 million or more, credit reporting bodies, health service providers, entities dealing in personal information and tax file number (TFN) recipients. Civil penalties of up to 2,000 penalty units (and up to five times that amount for body corporates) for serious or repeated breaches can be sought and any regulatory action taken will be publicised by the OAIC. Penalties for non-compliance are also significant.

Challenges

In the event of a suspected data breach, organisations are required to conduct an assessment within 30 days to determine whether the infiltration is likely to result in serious harm, and requires notification. If an eligible breach is confirmed, entities must notify individuals and the OAIC as soon as possible. Establishing the eligibility of a breach will represent a significant challenge for organisations that rely on traditional security tools.

As networks explode in digital complexity and span not just the physical, on-premise network, but also cloud and virtualised environments, non-traditional IT (IoT), and the supply chain, stealthy and sophisticated attacks can blend into the noise of the network and remain unseen for many months and years. This lack of visibility points to a clear inadequacy in organisations' ability to visualise what data has left their systems, or been compromised – and judge whether the loss of that data may cause serious harm. To comply with the NDB scheme, organisations need to gain a comprehensive and dynamic understanding of their digital estate.

> Darktrace's Enterprise Immune System can detect emerging threats without the need for rules. With its machine learning in action, we can defend our network 24/7 and address unfolding threats before they cause harm.
>
> **Asfar Sadewa, Head of IT,**
> **Jackson McDonald**

Darktrace and the NDB Scheme

The ability to detect the earliest signs of anomalous activity will be critical to ensure compliance with the NDB scheme.

Darktrace's core technology, the Enterprise Immune System, mimics the intelligence of the most powerful biological system, the human immune system, to catch and autonomously respond to emerging attacks, arming organisations with unprecedented network visibility.

Unlike traditional approaches which catalogue known examples of past compromise, Darktrace's AI does not require previous knowledge of threats in order to identify malicious activity. No rules or signatures are needed.

Instead, Darktrace leverages machine learning and AI algorithms to learn the 'pattern of life' of every user and device across the entire digital infrastructure. The technology then uses this evolving understanding of what is 'normal' to detect genuinely threatening anomalies, and takes autonomous action to stop or slow in-progress threats in their early stages, before they become data breaches. It can also understand if a threatening presence is already in operation on your network.

The Enterprise Immune System provides the real-time visibility required to make intelligent decisions in live situations, while enabling in-depth investigations into historical activity. Darktrace's unique user interface, the Threat Visualizer, not only provides a high-level graphical overview of anomalous network activity, but allows security personnel to dive deep into the granular details of particular events, such as specific device connections, or the volume of data transfers outside the organisation. The Threat Visualizer enables organisations to quickly determine if there is a data breach and conduct a thorough assessment.

Darktrace is ideally suited to detecting cyber-attacks in their earliest stages, before they escalate and cause harm. By identifying unexpected anomalies, security personnel are able to investigate compromises and insider risks as they emerge and throughout the stages of an attack's lifecycle.

- Catches the threats others miss
- Does not rely on any assumptions what 'bad' looks like
- Learns on the job, analysing live data in complex networks
- Autonomously responds to stop and neutralise in-progress attacks
- Arms security teams with powerful alerts and equips them with investigation tools to conduct an assessment of the chain of events leading up to the data breach.

> Before Darktrace, we lacked the power to detect if an authorised network-user had gone rogue, or if a novel threat had bypassed our legacy security systems. Armed with the Enterprise Immune System, our security team can now proactively defend against nascent threats in real time.
>
> **Graham Cray, Information Services Manager, Lockyer Valley Regional Council**

bsi. ISO/IEC 27001 Information Security Management

Darktrace has successfully been certified with ISO 27001:2013. This internationally-recognized, third-party validation demonstrates how seriously Darktrace takes its internal security and validates the information security management system that it has in place.

About Darktrace

Darktrace is the world's leading AI company for cyber security. Created by mathematicians, the Enterprise Immune System uses machine learning and AI algorithms to detect and respond to cyber-threats across diverse digital environments, including cloud and virtualized networks, IoT and industrial control systems. The technology is self-learning and requires no set-up, identifying threats in real time, including zero-days, insiders and stealthy, silent attackers. Darktrace is headquartered in San Francisco and Cambridge, UK, and has over 30 offices worldwide.

Contact Us

North America: +1 (415) 229 9100

Europe: +44 (0) 1223 394 100

Asia-Pacific: +65 6804 5010

info@darktrace.com

darktrace.com

@darktrace