Netsurion™ | EventTracker

Notifiable Data Breaches

Solution Brief

www.netsurion.com/eventtracker

NOTIFIABLE DATA BREACHES

About Netsurion

Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services.

Netsurion's SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion's SD-WAN edge appliance.

Netsurion's Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.

Notifiable Data Breaches Overview

In February 2017, the Notifiable Data Breaches (NDB) legislation was passed as an Amendment to the Australian Privacy Act (1988), with the new regime coming into effect on 22 February 2018. The data breach notification scheme aims to help people whose personal information has been breached, to regain some control sooner rather than later.

The NDB scheme requires businesses to notify both the Office of the Australian Information Commissioner (OAIC) and any affected individuals if the company experiences any unauthorized access, disclosure, or loss of personal information, if a reasonable person would conclude that this access, disclosure, or loss would be likely to result in serious harm.

Some businesses have expressed a concern that admitting to a security breach could make it easier for customers to launch a lawsuit, while most organizations agree that disclosing the breach is good business practice. The act makes it clear that serious harm isn't necessarily only related to financial losses, but could also include the public disclosure of private information such as a medical condition.

The Notifiable Data Breach Scheme under the Australian Privacy Act (1988) comes into effect in Australia on 22 February 2018. The scheme will impose an obligation on entities and agencies subject to the Act to notify individuals whose personal information is subject of a data breach that is likely to result in serious harm to those individuals. Entities must also notify the Australian Information Commissioner of eligible data breaches. Anticipating, identifying and responding to personal data breaches is an increasingly challenging responsibility for all businesses. Identifying ways to make this more manageable is key to operational and commercial success.

Summary of the new obligations

Organizations are expected to have policies and procedures in place that outline the steps that must be taken in response to a privacy breach including a Data Breach Response Plan and policies setting out expectations of staff when collecting, using, securing and disclosing customer information. When an organization identifies an eligible data breach it must assess the breach to ascertain if notification to the OAIC and impacted individuals is required.

Organizations are required to complete this assessment within 30 days but are also expected to complete a "reasonable and expeditious" assessment of the breach.

Eligible breaches and criteria for likely risk of serious harm:

A privacy/data breach will arise:

where there has been unauthorized access to, or unauthorized disclosure of, personal information about one or more individuals; or

where information has been lost and could be accessed or disclosed by unauthorized people or entities. An eligible data breach arises where a reasonable person would conclude that there is "a likely risk of serious harm" to any of the impacted individuals because of the unauthorized access or disclosure. Serious harm includes physical harm, financial/economic harm, emotional harm (e.g. embarrassment and humiliation), psychological harm and reputation harm. If there is a likely risk of serious harm will depend on the circumstances of the impacted individual which may or may not be known to the organization. Serious harm will be likely if such harm is more probable than not having regard to:

The security measures put in place by the organization (e.g. if the data is encrypted/password protected, anonymous, tokenized etc.);

The extent and sensitivity of the information;

The potential for exploitation or misuse of the information (e.g. credit card details, bank details, TFN's etc.) Serious harm will be likely if such harm is more probable than not having regard to all relevant matters. Organizations are expected to prepare a statement to give notice of an eligible data breach when notifying the OAIC.

The statement should be sent as soon as is practicable after identifying the breach and must include:

The identity and contact details of the entity

A description of the serious data breach that the Commissioner has reasonable grounds to believe has happened

The kinds of information concerned; and

Recommendations about the steps that individuals should take in response to the data breach that the Commissioner has reasonable grounds to believe has happened. An organization must:

If it is practicable to do so, take such steps as are reasonable in the circumstances to notify each of the individuals to whom the relevant information compromised in an eligible data breach relates; or

If it is practicable to do so, take such steps as are reasonable in the circumstances to notify those individuals who are 'at risk' from the eligible data breach; or

if it is not practicable to notify via either of the above two methods, make a statement by publishing the statement on the entity's website and taking reasonable steps to publicize the statement.

Organizations are expected to provide impacted individuals with general advice about steps they should take to mitigate the harm that may arise to them as a result e.g. checking transactions on their policies or bank/credit card accounts.

EventTracker offers preventative strategies to minimize the number of data breaches.

1. Protect against unauthorized and unlawful access, loss or damage

Description: Monitor the entire enterprise for activity and threat information across platforms, applications, networks, security controls and end points to protect the security of personal data and to alert on breach or misuse.

- EventTracker SIEM Monitor and alert on access to sensitive data sets, file shares and records. Monitor all print activity including Doc ID, printer, user, success or fail.
- EventTracker Continually monitor availability and integrity of firewalls, anti-malware and IPS. Alert on change and failure.
- EventTracker SIEM Audit and monitor all OS security groups and policy relevant to databases, apps and file share. Alert on additions to sensitive groups.
- EventTracker SIEM collects the logs from devices and application and Alert on email export of personal data to unknown recipients.

2. Ensure and demonstrate data protection

Description: Implement extensive and fully auditable monitoring to allow detailed querying and filtering of data, with drill-down, to enable issues to be rapidly investigated, corroborated and understood.

- EventTracker SIEM Alert on activity of new users and those subject to "managed risk". Visualization of personal data access. EventTracker SIEM Monitoring establishes How, Where and When access occurs.
- EventTracker SIEM Monitor application workflows, identifying backlogs and inappropriate processing

3. Implement security to prevent unlawful access, disclosure or loss

Description: Use security analytics to process data in real-time and identify activity or behavior indicating misuse or breach of personal data. Use dashboards to enable rapid demonstration of compliance.

- EventTracker SIEM Monitor and alert on Windows PnP events indicating connection of removable media & devices.
- EventTracker Real time dashboards showing Confidentiality, Integrity and Availability status of all sensitive data assets.
- EventTracker SIEM Correlate privilege user network authentication with critical business service change likely to lead to failure. Automatically analyses, alert and remediate.
- EventTracker SIEM Monitor corporate mobile devices and alert on attempted connection to data services when "out of country

4. Take steps to protect against insider data abuse

Description: Monitor use of applications and access to data across the enterprise but also monitor users, privileges and behaviors to spot unauthorized use by insiders or compromised users.

- EventTracker SIEM Monitor and alert on Windows PnP events indicating connection of removable media & devices.
- EventTracker SIEM Monitor the connection of USB device to the network, correlated with current user, terminal and data. Alert on non-compliance with policy.
- EventTracker SIEM Monitor and correlate network terminals, devices and users to identify and alert on unusual access e.g. an account authenticates from external IP at non-business hour.
- EventTracker SIEM Monitor database workflow to identify irregular patterns of activity indicating potential user negligence or mistake.