Fact Sheet

Cogito Group

PREVENT A PII DATA BREACH

SOMETIMES NOT ALL PRESS IS GOOD PRESS

As we know from recent experience, a data breach can negatively impact your organisations reputation for privacy protection, and as a result undercut an entity's commercial interests.

Privacy protection directly contributes to an individual's trust in an organisation. If your organisation is perceived to be handling personal information contrary to community expectations, individuals may seek out alternative products and services.

You can reduce the reputational impact of a data breach by effectively minimising the risk of harm to affected individuals, and by demonstrating accountability in your data breach response. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables and encourages individuals to take steps to reduce their risk of harm post breach. It also demonstrates that an entity takes their responsibility to protect personal information seriously, which is integral to building and maintaining trust in an entity's personal information handling capability.

More importantly, you can proactively manage service access to prevent a breach occurring in the first place.

What is a data breach?

A data breach is an unauthorised access or disclosure of personal information, or loss of personal information.

Data breaches can have serious consequences, so it is important that entities have robust systems and procedures in place to identify and respond effectively.

A data breach occurs when personal information that your organisation might hold is subject to unauthorised access or disclosure, or is lost.

Personal information is information about an identified individual, or an individual who is reasonably identifiable. You should be aware that information that is not about an individual on its own can also become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result. An example may be telephone numbers in a database, when combined with a telephone book allow who owns the telephone number to be identified.

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Prevent a PII Data Breach

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- compromise of a system or service containing personal information
- unauthorised access to personal information by an employee
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

Mitigation Strategies

Mitigation strategies can be implemented to protect from:

- targeted cyber intrusions and other external adversaries who steal data
- ransomware denying access to data for monetary gain, and external adversaries who destroy data and prevent computers/networks from functioning
- malicious insiders who steal data such as customer details or intellectual property
- malicious insiders who destroy data and prevent computers/networks from functioning.

We recommend any mitigation strategy should be first implemented to your high-risk users and computers such as those with access to important (sensitive or high-availability) data and exposed to untrustworthy internet content. Only then implement it for all other users and computers. Organisations should perform hands-on testing to verify the effectiveness of their implementation of mitigation strategies.

The Essential Eight

The mitigation strategies that constitute the Essential Eight are:

- Application control
- Patch applications
- Configure Microsoft Office macro settings.
- User application hardening restrict administrative privileges.
- Patch operating systems
- Multi-factor authentication
- Regular backups.

How Jellyfish can assist prevent a breach

Cogito's Jellyfish is a single pane of glass control panel for all your cyber tools. It provides your organisation with superior situational awareness, providing infrastructure monitoring logging, vulnerability protection, identity and access management, as well as token management, HSM Key management, mobile credential management and automation in other areas.

Prevent a PII Data Breach

Fact Sheet

A single pane of glass to increase security and cut costs with both active and automated capabilities built in.

How does Jellyfish Work?

Jellyfish combines multiple sensors and protection systems

Combines multiple sensors and applications to detect and respond

Allows a conversation between multiple protection platforms

Dynamically automates system responses

Jellyfish is an active approach to cyber security - rather than passive.

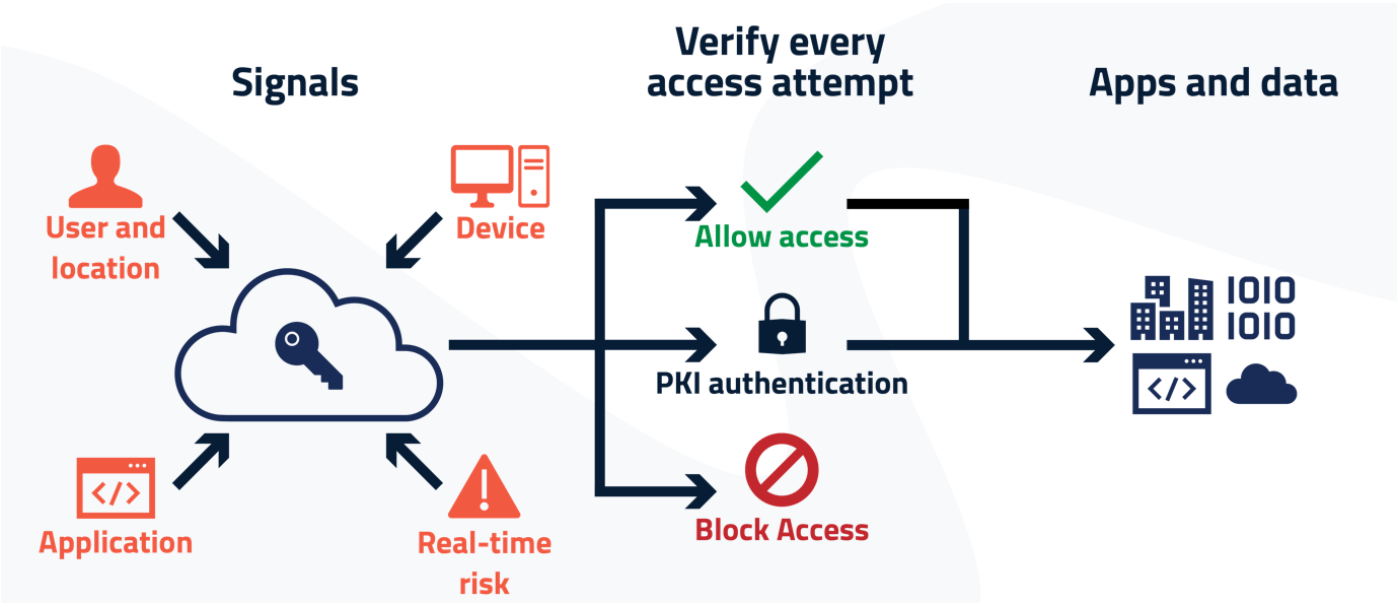
Most cyber products are passive

Jellyfish allows ACTIONS to be taken to stop breaches, as well as reporting them

Other solutions report on a BREACH – Jellyfish actively prevents it

A new approach to managing access and preventing a breach

The use of tokens and Hardware Security Modules in a Zero Trust environment ensures every attempt to access your data needs to be verified. Jellyfish PKI provides the credentials that allow for secure identification and stronger user and device authentication.



Prevent a PII Data Breach

Fact Sheet

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.