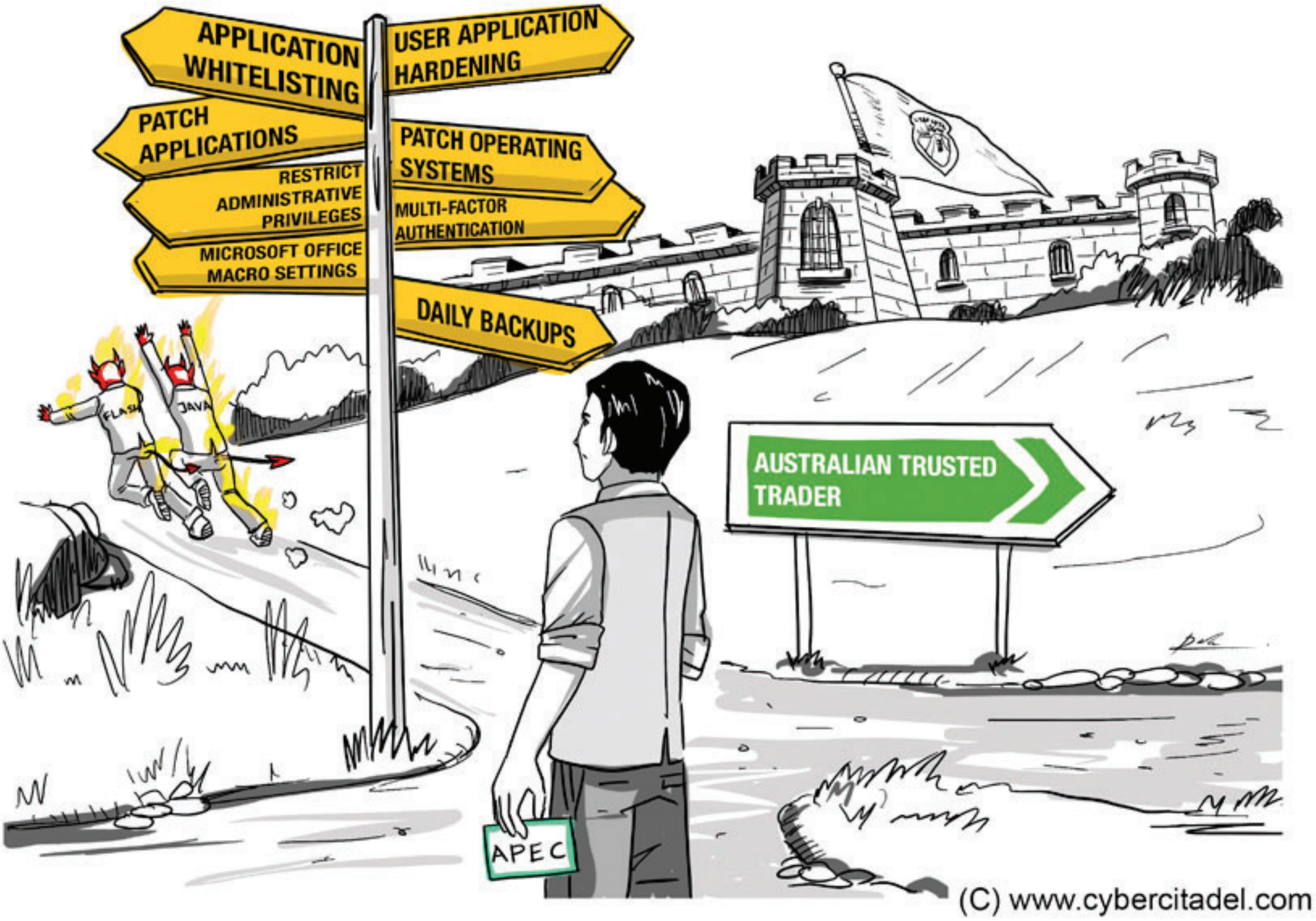

APPLICATION WHITELISTING
USER APPLICATION HARDENING
PATCH APPLICATIONS
PATCH OPERATING SYSTEMS
RESTRICT ADMINISTRATIVE PRIVILEGES
MULTI-FACTOR AUTHENTICATION
MICROSOFT OFFICE MACRO SETTINGS
DAILY BACKUPS
FLASH
JAVA
AUSTRALIAN TRUSTED TRADER
APEC

(C) www.cybercitadel.com

Australian Trusted Trader Cybersecurity Compliance

By JONATHAN SHARROCK, Director, Cyber Citadel

Businesses in Australia are being offered Australian Trusted Trader (ATT) status if they comply with a set of regulations. This status provides trading companies with a range of privileges and benefits that any trading company would be advantaged with.

Major benefits include increased administrative efficiency through severely reducing bureaucracy, especially with regards to customs and the handling of goods at the border, as well as improving cash flow as a result of the ability to defer duty to a specified date to be singularly processed. In addition, businesses receive recognition as a trusted trader both at home and abroad with the opportunity to apply for a business travel card (for Asia-Pacific participating nations) and fast-tracked temporary skills shortage (TSS) visas which would normally take 12 months to process. The status also entitles you to personalised logistics support provided by border force, which can significantly improve the continuity and consistency of service at customs. The support even includes a data collection service which tracks your goods and can be used not only to improve logistics but also detect and reduce fraudulent transactions.

There really are no apparent reasons not to apply for this status.

To do so however, requires your company to comply with a set of regulations, amongst which protecting your data against theft, loss, and misuse is essential. The base level requirement from the Australian Cyber Security Centre (ACSC) is summarised by a set of guidelines known as The Essential 8.

While no single mitigation strategy is guaranteed to prevent cyber security incidents, implementing the Essential 8 makes it much harder for adversaries to compromise systems. Furthermore, implementing pro-actively can be more cost-effective – in terms of time, money and effort – than having to respond to a large-scale cyber security incident.

Organisations can meet different compliance tiers, called maturity levels, ranging from 1 to 4. The ACSC stipulates that most companies should aim for the 3rd level, unless they are particularly prone to cyberattack due to the sensitive nature of their data.

A security assessment is three-fold: identification of a hazard (such as a third party); establishment of the risk (an example being the privileges the third party has); and determination of a mitigation strategy (for instance: third parties should meet the same standard of security as your own company and be restricted in their access to your network).

Identification as an initial preliminary to security should not be underestimated in value.

It is recommended that before implementing any of the Essential 8 mitigation strategies, organisations should perform the following activities:

1. Identify which systems require protection (i.e. which systems store, process, or communicate sensitive information, or information with a high availability requirement);

2. Identify which adversaries are most likely to target their systems (e.g. nation-states, cyber criminals, or malicious insiders); and

3. Identify what level of protection is required (i.e. selecting mitigation strategies to implement based on the risks to business activities from specific adversaries).

In particular, well-established companies should keep in mind the risks associated with legacy systems which they have brought onto new, wider networks. These systems may not have the necessary security features required to deal with threats in the modern technology age, especially if they were designed prior to a globally accessible internet. In addition, companies bringing physical machines online to streamline processing and provide better data collection should also be aware of the risk of doing so and should consider isolating these on a separate network which can be quarantined in the event of a security breach.

In addition, third-party providers are often the limiting factor for logistics company security. All companies, including third party vendors, should follow the principle of least privilege: the idea that at any user, program, or process should have only the bare minimum privileges necessary to perform its function. For example, a user account created for pulling records from a database doesn't need admin rights, while a programmer whose main function is updating lines of legacy code doesn't need access to financial records.

Furthermore, any third parties should meet the same security requirements as your own organisation. Company data is only ever protected as much as the path of least resistance: you can have a moat around your castle, but if your food suppliers use bridges the moat makes no difference under an assault.

Once identification has been conducted, the Essential 8 tackle three key areas of data security: preventing malware delivery and execution, limiting the extent of cybersecurity incidents, and recovering data and system availability. The Essential 8 are conveyed in the below schematic.

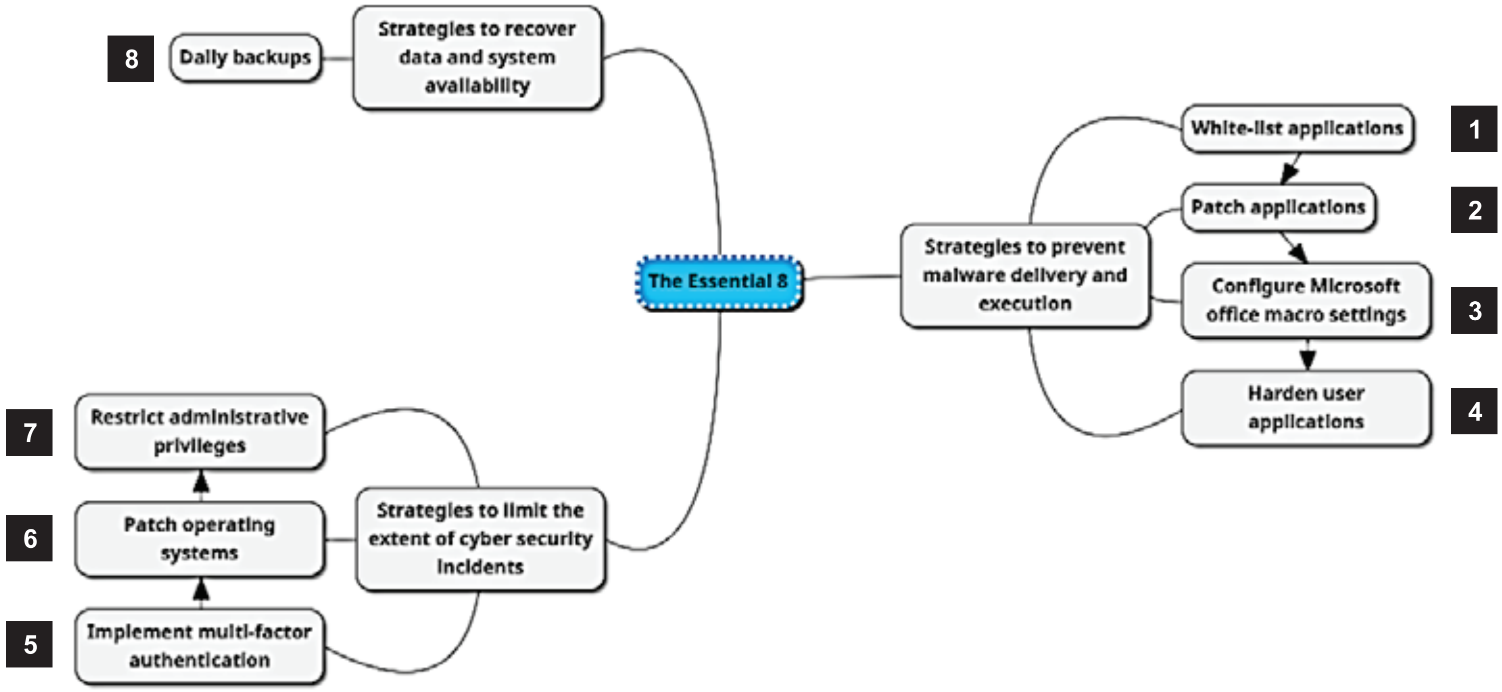
Implementation of the Essential 8 will ensure compliance with the requirements of the ATT application form questionnaire, but it is certainly a sensible way to conduct business security in the 21st century regardless of any application process.

Cyber Citadel can provide a comprehensive support service, ranging from advice on managing risk to a full implementation of any of the Essential 8.

Critically, assessment never stands still. Third parties change, employees change, police checks are irregular, and the security requirements themselves are constantly – often rapidly – evolving. This means that all companies should keep records, both in terms of a digital footprint (covering activity, access, sharing, data creation and loss) and in terms of changing business situations such as employees or policy.

This may all seem overwhelming, but the Essential 8 are really just that – essential. And implementing them can provide you with access to ATT membership. You don't need to do it alone: security firms such as Cyber Citadel are here to help you and your company every step of the way if need be. From updates on existing systems to full security rebuilds, as well as assessment of your company's greatest risks and mitigation solutions. The idea is simple – your company is your castle, and when goods move across your moat, the bridges should be drawn up afterwards.

CYBER CITADEL


8
Daily backups
Strategies to recover data and system availability
The Essential 8
Strategies to prevent malware delivery and execution
White-list applications
1
Patch applications
2
Configure Microsoft office macro settings
3
Harden user applications
4
Restrict administrative privileges
7
Patch operating systems
6
Strategies to limit the extent of cyber security incidents
Implement multi-factor authentication
5