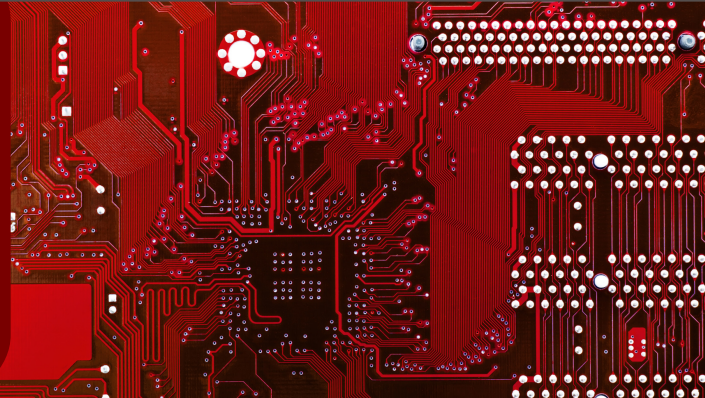


"We help to identify information security deficiencies, and develop an action plan to assist the mitigation of vulnerabilities and risks.



## Solution Overview

Alliance Business Technologies' 'IT Vulnerability Assessment' is a complete, comprehensive evaluation of your organisation's IT environment. We will identify any security vulnerabilities, relevant security risks, the impact of each vulnerability, and provide appropriate recommendations based on industry best practice to improve your overall security posture.

Your organisation will receive a documentation-based snapshot of your system's design. Developed through hands-on assessments from security-certified IT technicians, this solution's soul purpose is to uncover as many security vulnerabilities within your business systems and processes as possible.

### Benefits of your business getting an IT Vulnerability Assessment:



#### Identify & Respond

Potential and current weaknesses in your devices, applications, software, websites, and more.



#### Detect & Repair

Potential and current weaknesses in your network before they are exploited, or prevent further exploitation.



#### Understand & Enhance

Your organisation's current cyber security posture, providing recommendations to fortify security, and reduce risk levels.



#### Determine & Comply

Cyber security awareness and policy compliance regarding disaster recovery, employee training, and industry regulations.

To learn more about how our IT services can help drive your business, call **1300 705 062**, email us at [sales@abtechnologies.com.au](mailto:sales@abtechnologies.com.au), or visit our website at [www.abtechnologies.com.au](http://www.abtechnologies.com.au).

## ABT Corporate Snapshot

We are a member of the ASCS - Managed Service Provider Partner Program (MSP3), which is part of the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) that provides expert guidance to help entities mitigate cyber security incidents caused by various cyber threats. Our accreditations include ISO 9001:2008 Quality Assurance, GISC Accreditation Q-2645.



## Key Focus Areas



### Internal Assessment



Identify vulnerabilities of your network from the inside out.



### External Assessment



Identify vulnerabilities of your network from the outside in.



### Microsoft Vulnerability Report



Identify vulnerabilities within your Microsoft 365 and Microsoft Azure environments.



### Website Vulnerability Report



Unauthenticated or authenticated scan of public facing websites for known vulnerabilities and OWASP top 10.



### Email Threat Detection Scan



Authenticated scan of Exchange Online environment for dormant threats.



### Risk Detection Assessment



Leveraging dark web reporting to review accounts and credentials that are at risk of being used in an actual attack on your business email, website, internal network, desktops and laptop devices.

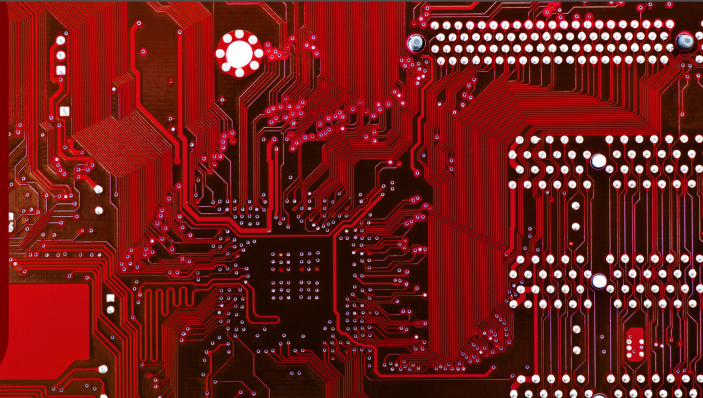


### Physical Security Assessment



Security review of your critical business data and hardware on site.

"We help to identify information security deficiencies, and develop an action plan to assist the mitigation of vulnerabilities and risks."



## Document Contents:



### Detailed 30+ Page Report

Detailed assessment providing a snapshot of current vulnerabilities internal and external, to provide remediation recommendations.



### Comprehensive Data Analysis

We design our reports so that your organisation and business executives can understand the technical data, without the complexity.

We provide both technical and visual data so not only are you able read about the progression and severity of security risks, but visually see what's happening with your security posture.



### Certified Security Experts

Data you can trust as our IT Vulnerability Assessments are completed by industry certified security and Microsoft experts.

## Contact Details:

**Alliance Business Technologies**  
 10A/121 Evans Road,  
 Salisbury, QLD, 4107

**P:** 1300705062

**E:** sales@abtechnologies.com.au

**W:** <https://www.abtechnologies.com.au>

High priority findings and poor significant target to the integrity and timeliness of the affected systems and applications. These risks often contain conditions that could lead to the compromise of one or several systems through techniques that may be less common or difficult to execute. The high priority ranking often includes vulnerabilities that are exploited through a combination of social engineering and technical exploits. These issues should be addressed in a timely manner, within 8 to 6 weeks.

**MEDIUM PRIORITY**  
 Medium Priority findings should be noted and addressed within 3-month timeframe. These risks may not pose an immediate threat to system security, but remediation is essential to increase overall security posture. Medium priority issues are often used in conjunction with various other high and low risk issues to enhance an attack. They often may require advanced tactics for exploitation.

**LOW PRIORITY**  
 Low Priority findings are often related to system configurations and/or technical processes that are operating at less than optimal status. These risks often provide unnecessary information to an attacker that could aid in planning an attack. These items are included to help the client improve technical processes and to assist in defining long term security strategy.

Alliance Business Technologies - SENSITIVE

14

## Identified Vulnerabilities

### Internal Network Assessment and Vulnerability Report

Audit Findings	Importance			
	CRITICAL	HIGH	MEDIUM	LOW
Automatic screen lock not turned on				
Screen lock time is > 15 minutes				
Suspected Brute Force Attack				
Potential Misconfiguration of network access to SQLServer03				
Update security stack to modern XDR Solution				
Account lockout not enabled				
Antivirus not up to date				
Unsupported Microsoft Office Version				
Security Patches missing on few computers				

Alliance Business Technologies - SENSITIVE

## Detected Vulnerabilities Detailed Report

### Internal Network Assessment and Vulnerability Report

Automatic screen lock not turned on  
 Enable automatic screen lock on the specified computers. Consider enabling screen lock to reduce the risk of unauthorized access to an interactive session.

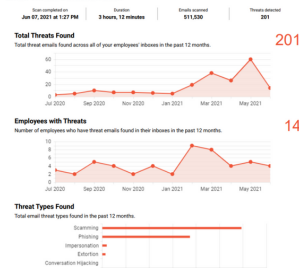
- ☐ MACHINE1
- ☐ MACHINE2
- ☐ MACHINE3
- ☐ MACHINE4
- ☐ MACHINE5
- ☐ MACHINE6
- ☐ MACHINE7
- ☐ MACHINE8
- ☐ MACHINE9
- ☐ MACHINE10
- ☐ MACHINE11
- ☐ MACHINE12
- ☐ MACHINE13
- ☐ MACHINE14
- ☐ MACHINE15
- ☐ MACHINE16

Screen lock time is > 15 minutes  
 Reduce screen lockout to 15 minutes or less on the specified computers. Even though screen lockout has been activated, extensive lockout times may lead to authorized access when users leave their computers.

- ☐ MACHINE1
- ☐ MACHINE2
- ☐ MACHINE3
- ☐ MACHINE4
- ☐ MACHINE5
- ☐ MACHINE6
- ☐ MACHINE7
- ☐ MACHINE8
- ☐ MACHINE9
- ☐ MACHINE10
- ☐ MACHINE11
- ☐ MACHINE12
- ☐ MACHINE13
- ☐ MACHINE14
- ☐ MACHINE15
- ☐ MACHINE16

- ☐ MACHINE1
- ☐ MACHINE2
- ☐ MACHINE3
- ☐ MACHINE4
- ☐ MACHINE5
- ☐ MACHINE6
- ☐ MACHINE7
- ☐ MACHINE8
- ☐ MACHINE9
- ☐ MACHINE10
- ☐ MACHINE11
- ☐ MACHINE12
- ☐ MACHINE13
- ☐ MACHINE14
- ☐ MACHINE15
- ☐ MACHINE16

### Email Threat Detection Scan



33