

A photograph of a person in a server room, viewed from the side. The person is wearing a plaid shirt and glasses, looking at a server rack. The room is dimly lit with blue and orange lights. The image is framed by a large blue and grey geometric shape on the left side.

MANAGING THE INSIDER THREAT

AGILPERSEC001



COURSE OVERVIEW

COURSE OUTLINE

Insider threat has the potential to cause greater damage to an organisation than any other threat source. The statistics from several studies have found clear links between insider threats and exploitable weaknesses in organisation's security management procedures .

The result has been damages in excess of \$100,000 for 53% of companies, and over \$1 million for 12% of companies in 2017 alone and 74% of companies believe that they are still vulnerable.

This course will provide your organisation's executives, managers and human resources personnel with knowledge and skills they need to manage the risk associated with the insider threat.

BENEFITS

1. Understanding the threat from insiders through real world examples.
2. Identifying potential insider threats and creating plans to mitigate the risks they present.
3. Understanding how security vetting can reduce the likelihood of having insider threats.
4. Knowing why incident reporting is important for creating more robust risk and security planning.
5. Being aware of the importance and benefits of providing security training for all staff members.

PRE-REQUISITES

There are no pre-requisites for this course.

WHO SHOULD ATTEND

- Organisational executives
- Security management staff
- Human resources personnel
- Managers and supervisors at all levels

STUDENT LEARNING OUTCOMES

After this course, you will be able to:

1. Define insider threat and provide examples of "at risk individuals".
2. Understand how to reduce the prevalence of at risk individuals using appropriate onboarding and vetting procedures.
3. Understand the need for and implementing an annual security awareness training package and implementing an incident reporting and management system.
4. Create procedures that enable the smooth transfer from or separation of at-risk individuals from IT systems and workspaces without impacting on the continuity of the businesses strategic and operational goals.

TEACHING STRATEGIES AND APPROACH TO LEARNING

This course will provide real-world examples of insider threats to enhance the participant's skills and experience in dealing with insider threats.

These examples will be provided through the use of case studies, audio visual snippets and quizzes and will offer best practice guidance for the identification and management of insider threat.

Although this self-paced online course is to be completed individually and may require the participant to re-read course material to be able to adequately answer questions throughout the course, post course discussions and regular review of course material is encouraged and will ensure that procedures are implemented and maintained in the most effective and efficient manner.

COURSE LOGISTICS

Location or delivery mechanisms

This course is a self-paced online course with online assessment; however, private in-house courses can be run over an agreed upon number of days by experienced security risk consultants through negotiation.

Duration

The online course will take approximately 2 hours to complete.

Assessment

Although this training package is not pass/fail it is suggested that participants complete all questionnaires to their fullest potential to ensure that they get the most benefit for themselves and the company.

Course registration

Register by calling Agilient on 1300 341 692 or emailing us on securityinsights@agilient.com.au.

More information about Agilient can be found at our website.
See: www.agilient.com.au.

For more information on the course call Agilient on 1300 341 692 or email us on securityinsights@agilient.com.au.

COURSE CONTENT

Participants will be guided through the following topic areas:

1. Defining The Insider Problem – Providing knowledge of what constitutes an insider and the statistical data of impacts they can have on an organisation.
2. Insider Threat – Identifying the types of insider threats and signs to look for to identify "at risk" persons.
3. Personnel Security – Understanding the importance of personnel security in combating the threat from insiders.
4. Identifying Vulnerabilities in Security – Knowing how to identify vulnerabilities in security that can be targeted by insiders and the damage that can be caused.
5. Vetting and Ongoing Suitability – Understanding the importance of onboarding/vetting and maintaining suitability of new and potential staff.
6. Annual Security Awareness Training – The significance of security training and how ensuring all staff complete it will assist in reducing risks.
7. Incident Reporting – Providing information on how incident reporting can enable businesses to develop more robust security strategies and methods of reporting incidents.
8. Separating Staff – Distinguishing strategies for separating staff from a business group or terminating employment utilising best practice procedures to reduce the risk of damage.

Sydney Head Office:
Level 4, 655 Pacific Highway
ST LEONARDS NSW 2065
Australia

Melbourne Office:
Level 9, 440 Collins Street
Melbourne Vic 3000
Australia

Canberra Office:
Suite 117, 2 Endeavour House
Captain Cook Crescent
MANUKA ACT 2603

Brisbane Office:
Level 54, 111 Eagle Street
Brisbane Qld 4000
Australia