

Certified Information Security Awareness Specialist



Tuniversity

I3

Gewenste voorkennis

Twee jaar ervaring met daadwerkelijke betrokkenheid bij het beveiligen van de bezittingen van de organisatie is gewenst. Deze ervaring kan voortkomen uit een IT- of zakelijke achtergrond. De cursist heeft affiniteit met beide vakgebieden en kent de missie van de organisatie.

Tijdsduur en kosten

De duur van de cursus bedraagt twee dagen. De prijs bedraagt € 1380,-, exclusief 19% BTW. Documentatie, koffie, thee en lunch zijn bij de prijs inbegrepen.

De financiële gevolgen van informatiediefstal zijn enorm. Nog maar te zwijgen over de schade die wordt veroorzaakt aan de reputatie en identiteit van organisaties.

De laatste tien jaar hebben organisaties enorm veel geld uitgegeven aan de meest moderne beveiligingssoftware. Er was echter minder focus voor een belangrijke zwakte in de beveiligingsketen: menselijk gedrag.

Tot voor kort was security awareness, educatie en training voor alle medewerkers maar bij weinig organisaties een aandachtspunt. Deze organisaties realiseerden zich dat de meest voorkomende veiligheids- en confidentialiteitsproblemen hierdoor voorkomen konden worden.

Veel studies tonen dan ook aan dat werknemers een sleutelrol spelen in de informatiebeveiliging maar ook dat ze vaak te weinig kennis hebben van de juiste maatregelen.

Meer dan ooit beginnen organisaties zich te realiseren hoe belangrijk beveiligingsbewustzijnstrainingen zijn en hoe ze de sleutel vormen naar security. Dit leidt tot de vraag of een trainingsprogramma door een extern bedrijf moet worden gegeven of juist door de eigen organisatie.

Doel en doelgroep

Beveiligingsbewustzijn is een geen "one time only" inspanning maar een programma, het is een proces dat herhaald en aangepast moet worden. Mensen hebben herhaling van instructies nodig om scherp te blijven en de regels veranderen mee met de dynamiek van de organisatie.

Om de kosten te beperken van het herhaaldelijk bezoeken van externe trainingen hebben EPI en Tuniversity.nl een cursus ontworpen die u helpt uw eigen security awareness programma te ontwerpen en te implementeren.

Het maken van een eigen security awareness programma biedt de kans de trainingen aan te passen aan de specifieke eisen van de organisatie en te kunnen inspelen op strategische doelen.

Deze training is onderdeel van het CITM programma, het IT manager's framework voor medewerkers die verantwoordelijk zijn voor het beheer van mission critical IT omgevingen. De training is bedoeld voor de medewerkers die verantwoordelijk zijn voor het ontwikkelen, implementeren en monitoren van de informatiebeveiligingspraktijk. Dit betreft ook de medewerkers die verantwoordelijk zijn voor de aspecten rondom de uitvoering van het programma en het informatiebeveiligingsbewustzijn.

Certified Information Security Awareness Specialist

Inhoud van de cursus

1. Introductie Informatiebeveiliging
 - Informatiebeveiliging toegelicht
 - Confidentialiteit, Integriteit, Beschikbaarheid
 - Authenticiteit, Onweerlegbaarheid
 - Wet- en regelgeving
 - Standaarden
2. Onderdelen, rollen en verantwoordelijkheden
 - Onderdelen van de informatiebeveiliging
 - Rollen toegelicht
 - Verantwoordelijkheid bij informatiebeveiligingsbewustzijn
3. Dreiging en gevolg
 - Herkenning van security overtredingen
 - Algemene gevaren
 - Security overtredingen
 - Gevolg
4. Bewustzijn, training en en educatie
 - Definitie en doelstellingen van bewustzijn, training en educatie
5. Project management
 - Selectie van de projectmanagement methode
 - Statement of Work
 - Work Breakdown Structure
 - Planning, tracking en rapportage
6. Ontwerp van het bewustzijnsprogramma
 - Structuur van bewustzijnsactiviteiten
 - Uitvoeren van een behoeften analyse
 - Ontwikkeling van een strategie
 - Prioriteiten vaststellen
 - Complexiteit niveau's
 - Financiering van het programma
7. Ontwikkeling van het bewustzijnsmateriaal
 - Materiaal, Onderwerpen, Bronnen
8. Ontwikkeling van het bewustzijnsmateriaal
 - Voorbeeldonderwerpen
 - anti-virus, spam
 - data netwerken, printers en faxen, VPN
 - Naleving wachtwoordreglement
 - Email gedragsregels, Internetgebruik, etc.
9. Implementatie van het bewustzijnsprogramma
 - Communicatie van het plan, Technieken voor aflevering
10. Na de implementatie...
 - Security incident opvolging
 - Compliance monitoring
 - Feedback en evaluatie
 - Omgaan met verandering
 - Steeds weer verbeteren
 - Succes indicatoren
11. Examen Certified Information Security Awareness Specialist