Fundação Getúlio Vargas - FGV - Management
MBA em Gestão de TI e Gerencia de Projetos
Cadeira de Gestão da Segurança da Informação

Simulado da Prova

Uma das principais dificuldades de se obter sucesso na área de Segurança da Informação decorre de dois fatores:

- A ausência de uma visão holística do risco, devido a incorreta percepção executiva de que a Segurança é responsabilidade do setor de TI, e não de toda a empresa; e
- A incorreta visão empresarial de que segurança apenas envolve custos, sem retorno tangível.

Vencendo estas barreiras, passa-se para outro desafio: identificar corretamente as demandas de segurança da Informação, de forma a possibilitar investimentos compatíveis com o risco, garantindo retorno para a empresa.

Nosso instrumento de avaliação, a prova, busca reproduzir os comportamentos atuais observados na maioria das empresas. Falta de visão adequada do risco, confusão entre os atributos da informação e, principalmente, investimentos inadequados na Política de Segurança e no Plano de Continuidade dos Negócios. A Prova sempre será composta de um ou mais casos reais atuais que espelhem estas discrepâncias, e o aluno é instado a identificá-las e corrigi-las, a luz dos conceitos discutidos durante a cadeira.
Como exercício, será usado o artigo “Renault suspende três executivos por espionagem”. Neste caso, uma grande montadora investe em tecnologia de inovação, buscando um diferencial, e seus projetos são tornados públicos. Naturalmente, independentemente da forma através da qual isso aconteceu, a empresa tem a perda de sua expectativa de retorno dos investimentos.
A seguir, serão feitas assertivas sobre o texto, que deverão ser avaliadas se estão certas ou possuem incorreções conceituais. Você deve identificar tais incorreções e corrigi-las.

Assertiva 1 – A falta de investimentos em proteção da informação estratégica decorre do fato do risco não ser mensurável. Incidentes ocorrem porque situações fortuitas e imprevisíveis acontecem. São os chamados “cisnes negros”;

Assertiva 2 – No texto podem ser identificados componentes do risco. As vulnerabilidades,por exemplo, são elementos ativos que causam incidentes quando combinados com ameaças presentes no sistema. Os executivos acusados, por exemplo, são ameaças presentes no sistema;

Assertiva 3 – A Renault deveria ter implementado um setor de Gestão de Segurança da Informação, que deverá assumir a responsabilidade pela definição e implementação de regras para a Gestão da Segurança. Convém que tenha perfil técnico da área de TI,por possuir formação adequada para os desafios que irá enfrentar;

Assertiva 4 – Ações cotidianas de controle do nível de risco são essenciais para qualquer empresa. No caso da Renault, teria sido importante, para evitar o incidente de segurança, que houvesse um Plano de Contingência que monitorasse e mitigasse o risco do incidente de disponibilidade, caracterizado pela disponibilização das informações estratégicas do projeto do carro elétrico; e

Assertiva 5 – O Plano de Continuidade dos Negócios envolve ações de Administração de Crise (PAC), Continuidade Operacional (PCO) e de Recuperação de Desastres (PRD). Apesar de desastrada e inoportuna, por não agregar valor à imagem da empresa, a ação de comunicação através de seu Diretor Jurídico, declarando a gravidade dos acontecimentos, é uma ação planejada e incluída no PCO.