UNIVERSIDADE ESTÁCIO DE SÁ
MBA EM SEGURANÇA DA INFORMAÇÃO

Fichamento de Estudo de Caso

Lenivaldo Dias Almeida de Jesus Junior

Trabalho da disciplina Governança de
Segurança da Informação
Tutor: Prof. Andre Jorge Dias de Moura

Salvador - BA
2015

Estudo de Caso :

GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO
Intel Corp. – Bring Your Own Device.

REFERÊNCIA: Chandrasekhar, R, Compeau, Joe, Haggerty, Nicole: Estudo de Caso: INTEL CORP. – BRING YOUR OWN DEVICE.

RESUMO: O dilema de se colocar em pratica o BYOD sem colocar em risco as informações da empresa, sem expor seus funcionários, de como proteger seus dados sem invadir a vida pessoal de seus funcionários, foi com isso que Malcolm Harkins estava preocupado enquanto analisava se poderia implementar o uso de BYOD na Intel Corp.

Palavras Chave: Fichamento, Segurança da Informação, Governança de Segurança da Informação, Intel Corp., BYOD.

No inicio de 2010, o diretor executivo de segurança da informação, Intel Corp., estava enfrentando dilemas para levar em frente a iniciativa BYOD. A divisão de tecnologia da informação da empresa estava testando a iniciativa há quase um ano. Após a tomada de decisão em favor da implementação, Harkins precisa avaliar como será feita a abertura da tecnologia para toda a empresa.

As principais preocupações enfrentadas por Harkins eram três:

Como exatamente extrairiam valor da iniciativa e tornaria o BYOD uma nova fonte de vantagem competitiva na Intel;

Como garantiriam segurança dos dados corporativos em um dispositivo que um funcionário traz para o local de trabalho;

Como responderiam para o e-Discovery solicitações de informações armazenadas em um dispositivo que não pertence à Intel.

Em 2009, Harkins notou entre os funcionários da Intel a tendência de trazer seus próprios tablets e dispositivos de armazenamento para suas estações de trabalho e usa-los durante suas horas de trabalho. No mesmo período, o uso de smartphones estava crescendo em todo o mundo.

Harkins previu que o número de dispositivos móveis de funcionários da Intel triplicaria em um ano e que, em 2014, cerca de 70 por cento dos funcionários estariam usando seus próprios dispositivos para pelo menos parte de seu trabalho.

As principais preocupações de Harkins relacionavam-se com questões não apenas TI e SI, que eram suas áreas de domínio, mas também financeiro, recursos humanos e o valor de marca da empresa, que não eram sua área de domínio. Funcionários investiram pessoalmente em notebooks, netbooks e dispositivos móveis, e estavam usando-os para trabalho da empresa, fosse no escritório, em casa ou na estrada. Esta prática reduziu os custos da Intel em aquisição de dispositivos, mas aumentou seus custos de avaliação, configuração e suporte. A Intel como organização, precisava acessar e controlar as informações da empresa, mas fazer isso em dispositivos de funcionários sem violar a privacidade individual era complicado.

Como parte do desenvolvimento de uma estratégia, para implementação do BYOD, Harkins estava interessado em juntar a entrada de não apenas funcionários que estavam trazendo seus próprios dispositivos pra trabalhar, mas também aqueles funcionários que não estavam fazendo isso. Por um período ininterrupto de 48 horas, sua equipe respondeu a dúvidas, alternadamente, de quase 7.000 funcionários e respondeu mais de 1.000 posts. A sessão web era uma oportunidade não apenas para funcionários da Intel ao redor do mundo fornecer material sobre como eles queriam usar seus smartphones, mas também para a equipe de SI e TI explicar o que o uso de smartphones significava para a organização. Apesar de apenas 30% dos participantes, do evento, concordarem com o acesso corporativo a seus dispositivos pessoas, havia uma visão quase unânime em favor de a Intel gerenciar a segurança de dispositivos pessoais, e, em troca pela liberdade de trazer seus próprios dispositivos para o trabalho, 100% estavam dispostos a aceitar treinamento e ajustes necessários para seu comportamento.

Era evidente que o BYOD não era uma questão de tecnologia; ele afetava outras funções da empresa, como jurídico, RH e contabilidade, cuja ajuda era requerida na definição de política, incluindo detalhes como privacidade e licenciamento de software e aplicação de conformidade.

A partir da revisão de dados nos últimos trimestres, Harkins acessou uma informação vital para sua tomada de decisão, os funcionários da Intel que estavam usando seus próprios dispositivos estavam gastando, em média, 57 minutos a mais, por dia em trabalho relacionado à empresa. A empresa poderia usar o que era chamado de "taxa de encargo" de cerca de $100 por hora por funcionário para chegar ao ganho em produtividade. Ganhos adicionais poderiam ser percebidos em funcionários aproveitando toda oportunidade, fora das horas de trabalho, para levar os negócios da Intel através de colaboração em tempo real com clientes internos e externos. Os funcionários também estariam gradualmente felizes com o BYOD, o que levaria a ganhos como a resolução conjunta no caso de um prazo final ou uma emergência. Harkins podia ver alguns recursos potenciais de vantagem competitiva. Por exemplo, o networking levaria, com o tempo, ao desenvolvimento de melhores produtos e

serviços. O uso de dispositivo autorizado também minimizaria o perfil de risco geral dentro da TI.

Em um ambiente BYOD tem dois grandes componentes de risco, dispositivos e dados. O dilema diante de Harkins pertencia a duas áreas, a medida na qual a segurança do dispositivo e a medida para a qual a segurança de dados poderiam ser implementada. Tradicionalmente, todo o hardware que era de posse e operado pela empresa era equipado com características de Segurança da Informação embutidas como configurações básicas, procedimentos de login, protocolos de autenticação, controles de acesso, firewalls e softwares anti-malware. A situação BYOD compreenderia tipicamente dois tipos de dispositivos - dispositivos gerenciados e dispositivos não gerenciados. A Intel dividiu em camada seus próprios controles de segurança em todos os dispositivos gerenciados; os controles assumiram duas formas - criptografia e capacidade de apagamento remoto. Como pinos redondos em um buraco redondo, os dispositivos gerenciados se encaixavam perfeitamente com o ambiente de TI e as expectativas de TI. Dispositivos não gerenciados, no entanto, eram como pinos quadrados em um buraco redondo. Nenhuma única solução suportava todos os dispositivos dos funcionários, assim representando um risco de segurança.

Harkins estava procurando oportunidades estratégicas no BYOD para criação de valor. Ele previu não apenas uma infraestrutura de dados segura, mas engajou, motivou e digitalmente permitiu que os funcionários pudessem colaborar livremente, agir inovadoramente e trabalhar mais independentemente que no passado.