Os prazeres e as armadilhas do uso de dispositivos pessoais no ambiente de trabalho

Quase todo mundo que tem um smartphone quer trazê-lo para o trabalho e usá-lo profissionalmente. E por que não? Funcionários usando seus próprios smartphones permitiriam que as empresas desfrutassem dos benefícios de uma força de trabalho móvel sem gastar seu próprio dinheiro com a aquisição desses dispositivos. As pequenas empresas seriam capazes de adotar a tecnologia da computação móvel sem fazer grandes investimentos em dispositivos e serviços móveis. De acordo com a Gartner Consultants, o uso de dispositivos pessoais no ambiente de trabalho (BYOD — Bring Your Own Device) será adotado por 38% das empresas até 2016 e metade delas vai aderir ao BYOD até 2017. O BYOD está se tornando a "nova regra".

Mas... espere um minuto. Quase três em cada cinco empresas acreditam que o BYOD representa um problema crescente para suas organizações, de acordo com uma pesquisa realizada em 162 empresas pela Osterman Research em nome da Dell Inc. Embora o BYOD possa melhorar o nível de satisfação no trabalho e a produtividade do funcionário, também pode causar uma série de problemas se não for gerido de forma adequada: é mais difícil dar suporte para dispositivos de propriedade pessoal do que para os fornecidos pela empresa, o custo de gerenciamento de dispositivos móveis pode se elevar e a proteção dos dados e redes corporativas torna-se mais complexa. A pesquisa conduzida pelo Grupo Aberdeen descobriu que, em média, uma empresa com mil dispositivos móveis gasta um extra de US$ 170 mil por ano quando adota o BYOD. Logo, não é tão simples assim.

A CIO Jeanette Horan, da IBM, acredita que o BYOD pode causar tantos problemas quantos ele é capaz de resolver. O BYOD não está poupando dinheiro para a IBM, mas está, de fato, criando novos desafios para o departamento de TI, pois os dispositivos dos funcionários contêm vários softwares que a IBM não controla. A IBM fornece dispositivos BlackBerry seguros para cerca de 40 mil de seus 400 mil trabalhadores, ao mesmo tempo em que permite que mais 80 mil funcionários usem seus próprios smartphones ou tablets para acessar as redes da IBM.

O departamento de TI da IBM descobriu que não tinha domínio de quais aplicativos e serviços seus empregados estavam usando em seus dispositivos pessoais, e os próprios empregados eram "inocentemente inconscientes" dos riscos de segurança apresentados por apps populares. A IBM decidiu proibir o uso de serviços populares como o Dropbox, um repositório de dados baseado em nuvem, temendo que seus funcionários colocassem informações confidenciais da empresa em suas contas pessoais no Dropbox, encaminhassem e-mail interno para serviços de correio públicos da Web ou usassem seus smartphones como hotspots Wi-Fi móveis.

A IBM não permite que um funcionário acesse sua rede corporativa com um dispositivo pessoal, a menos que o dispositivo esteja protegido por suas regras de segurança. O departamento de TI configura o dispositivo de modo que a sua memória possa ser apagada remotamente se ele for perdido ou roubado. O grupo de TI também desabilita programas públicos de transferência de arquivos, tais como o iCloud, da Apple; em seu lugar, os funcionários utilizam uma versão hospedada na IBM chamada MyMobileHub. A IBM desativa até mesmo o Siri, o assistente pessoal comandado por voz em iPhones de funcionários, pois as consultas faladas são enviadas para os servidores da Apple.

O dispositivo de cada funcionário é tratado de maneira diferente, dependendo do modelo e das responsabilidades do cargo da pessoa que o está utilizando. Algumas pessoas estão autorizadas a receber somente e-mails, agendas e contatos da IBM em seus dispositivos portáteis, enquanto outras podem acessar aplicações e arquivos internos da empresa (ver Capítulo 8). Ela equipa os dispositivos móveis dessa última categoria de funcionários com software adicional, como programas que criptografam informações que trafegam de e para as redes corporativas.

Uma empresa que implantou o BYOD com sucesso foi a Intel Corporation, empresa gigante do setor de semicondutores. Cerca de 70% dos 39 mil dispositivos registrados em sua rede são

dispositivos pessoais. A Intel conduziu a implantação do BYOD de uma maneira positiva, tentando encontrar maneiras de fazê-lo funcionar em vez de malográ-lo. Diane Bryant, então CIO da Intel, não queria ser dependente de um único fornecedor ou dispositivo móvel.

A Intel elaborou uma estratégia de adoção do BYOD e criou um acordo de nível de serviço para o usuário final, esclarecendo que eles estavam voluntariamente aderindo ao BYOD e não sendo obrigados a isso. A empresa desenvolveu diferentes políticas, regras e limites de acesso para cada tipo de dispositivo — smartphone, tablet ou laptop — com aplicação de múltiplos níveis de controle. Ela mantém uma lista de dispositivos aprovados. Se um dispositivo não satisfaz seus requisitos, ele é bloqueado a partir da rede. Hoje, o programa BYOD da Intel oferece 40 aplicativos proprietários, incluindo ferramentas de viagem para ajudar o agendamento de voo e localizadores de sala de conferência. A empresa tem uma loja interna de "apps" e usa uma variedade de software e ferramentas de segurança, incluindo software de gestão de dispositivos móveis (MDM — Mobile Device Management) e de gestão de aplicativos móveis (MAM — Mobile App Management).

O objetivo da Intel para o BYOD não é poupar dinheiro, mas tornar os funcionários mais felizes e produtivos. Os funcionários gostam da possibilidade de usar seu próprio dispositivo e seus apps, juntamente com os apps especializados da Intel. Em média, os trabalhadores dizem que usar seus próprios dispositivos os faz economizar um tempo de aproximadamente 57 minutos por dia, o que equivale a 5 milhões de horas por ano em toda a empresa.

A Canadian Tire decidiu não permitir o BYOD amplamente e dotou seus 3 mil funcionários corporativos com novos smartphones BlackBerry Q10 e Z10. (A Canadian Tire é uma das maiores empresas do Canadá, com uma loja on-line de e-commerce e 1.200 pontos de venda comercializando produtos automotivos, esportivos, para lazer, para o lar, vestuário, postos de combustíveis e serviços financeiros.) A empresa sentiu que, para seus propósitos, o modelo BYOD não era suficientemente seguro. O executivo-chefe de tecnologia (CTO — Chief Technology Officer) Eugene Roman, da Canadian Tire, teme que uma mensagem de e-mail possa enviar um vírus para a infraestrutura central da empresa. No momento, a gestão da Canadian Tire pensa que BYOD é interessante, mas ainda não está pronta para as aplicações tradicionais de negócio da empresa.

Para implantar dispositivos móveis com êxito, as empresas precisam examinar cuidadosamente seus processos de negócio e determinar se a mobilidade faz ou não sentido para elas. Nem toda empresa se beneficiará da mobilidade com a mesma intensidade. Sem uma ideia clara de como os dispositivos móveis se encaixam nos planos de longo prazo das empresas, elas acabarão desperdiçando dinheiro em dispositivos e programas desnecessários. Uma das maiores preocupações que os gestores têm sobre a mobilidade é a dificuldade de medir o retorno sobre o investimento. Muitos trabalhadores são bastante comprometidos com seus dispositivos móveis e os benefícios são muito significativos para serem ignorados, mas quantificar quanto dinheiro é ganho ou poupado pela adoção de uma estratégia móvel pode ser uma tarefa difícil.

Fontes:

Fred Donovan, "The Growing BYOD Problem", FierceMobileIT, 13 fev. 2013;

Brian Bergstein, "IBM Faces the Perils of 'Bring Your Own Device'", MIT Technology Review, 21 mai. 2013;

Matt Hamblen, "Canadian Tire forgoes BYOD, issues BlackBerries to workers", Computerworld, 20 mai. 2013; e

Boonsri Dickinson, "Security Headaches: BYOD Users Expected to Double by 2014", Information Week, 8 ago. 2012.

PERGUNTAS SOBRE O ESTUDO DE CASO

1. Quais são as vantagens e desvantagens de permitir que os funcionários usem seus smartphones pessoais para as atividades profissionais?

2. Quais fatores pessoais, organizacionais e tecnológicos devem ser considerados na tomada de decisão sobre permitir que os funcionários usem seus smartphones pessoais no trabalho?

3. Compare as experiências de BYOD da IBM e da Intel. Por que o BYOD funcionou tão bem na Intel?

4. Permitir que funcionários utilizem seus próprios smartphones no trabalho poupará dinheiro para a empresa. Você concorda? Justifique sua resposta.