O vazamento de dados no mundo: riscos e erros comuns que os funcionários cometem

Resumo executivo

Para entender o desafio que cada vez mais as empresas distribuídas e móveis enfrentam para proteger suas informações confidenciais, a Cisco contratou a firma de pesquisa de mercado InsightExpress para conduzir um estudo com empresas e profissionais de TI em todo o mundo. Como parte desse estudo, foram conduzidas pesquisas em 10 países que a Cisco selecionou devido às diferenças em suas culturas sociais e corporativas. Em cada país, 100 usuários finais e 100 profissionais de TI participaram da pesquisa, totalizando 2.000 entrevistados. A pesquisa concluiu que apesar de todas as políticas de segurança, procedimentos e ferramentas já implementadas, funcionários em todo o mundo apresentam comportamentos de riscos que colocam os dados corporativos e pessoais em perigo. Os comportamentos dos funcionários incluem:

- **Uso de aplicativo não-autorizado:** 70% dos profissionais de TI acreditam que o uso de programas não-autorizados foi responsável por metade dos incidentes de perda de dados em suas empresas.
- **Uso inadequado de computadores da empresa:** 44% dos funcionários compartilham seus dispositivos de trabalho com terceiros sem supervisão.
- **Acesso físico e acesso à rede não-autorizado:** 39% dos profissionais de TI declararam que tiveram casos em que um funcionário acessou partes não-autorizadas da rede ou da instalação da empresa.
- **Segurança de funcionário remoto:** 46% dos funcionários admitiram transferir arquivos entre os computadores da empresa e de casa ao trabalharem em casa.
- **Uso inadequado de senhas:** 18% dos funcionários contam suas senhas para colegas de trabalho. Essa taxa chega a 25% na China, Índia e Itália.

Para reduzir o vazamento de dados, as empresas precisam integrar a segurança na cultura corporativa e avaliar consistentemente os riscos de cada interação com redes, dispositivos, aplicativos, dados e, é claro, outros usuários.

Introdução

Os funcionários em todas as partes do mundo estão usando as redes corporativas para se comunicarem, colaborarem e acessarem dados. As empresas ansiosas por aumentarem a produtividade adotaram a tendência de crescente integração entre as comunicações em rede e as operações corporativas, e incentivaram os funcionários a aproveitarem as vantagens oferecidas pela tecnologia como dispositivos sem fio e hotspots públicos. A produtividade aumentou, mas a colaboração baseada na rede introduz dados corporativos em um ambiente mais amplo que é mais vulnerável e difícil de proteger.

Os dados armazenados na rede corporativa também estão em risco porque acessá-los ficou mais fácil do que nunca. As empresas proporcionam um acesso fácil aos bancos de dados para compartilhamento de informações, e a tecnologia de armazenamento e compactação possibilitou pontos terminais mais poderosos (e que sujeitos a riscos). Um dispositivo móvel de 80 MB agora tem 6000 documentos Microsoft Word ou 720.000 emails, e os novos dispositivos removíveis de 64 GB permitem que um disco rígido inteiro seja copiado em um dispositivo do tamanho de um pacote de chicletes.

Esses dispositivos tornam mais fácil para funcionários, parceiros ou ladrões de dados acessarem, moverem ou perderem propriedade intelectual ou dados dos clientes. Além de ter um maior volume de dados em risco, as empresas hoje sofrem mais consequências se esses dados forem perdidos ou comprometidos. A perda de propriedade intelectual, como planos de produtos proprietários, dados financeiros, e planos de fusão e aquisição, pode arruinar a reputação de uma empresa, prejudicar a sua marca ou tornar a empresa menos competitiva. As violações das obrigações na manipulação de dados confidenciais dos clientes podem minar a confiança do cliente e levar a multas.

Empresas inteligentes instituem políticas de segurança e treinam os funcionários no risco de perda de dados, mas a eficácia dessas ações é questionável. Nos últimos dois anos, mais de 250 milhões de registros confidenciais foram reportados como perdidos ou roubados.1 E os prejuízos nem sempre se originam de ameaças externas. Seja consciente ou inconscientemente, inocente ou maliciosamente, os funcionários têm comportamentos que aumentam o risco.

Para reduzir o vazamento de dados e proteger as informações corporativas, as organizações de TI precisam entender como o comportamento do funcionário aumenta o risco e dar os passos necessários para promover uma cultura corporativa atenta à cultura onde os funcionários aderem a políticas e procedimentos.

Pesquisa profunda expõe comportamentos de risco

Para melhor entender os comportamentos dos funcionários que colocam os ativos da empresa em risco, a Cisco contratou uma empresa de pesquisa de mercado, a InsightExpress, para conduzir um estudo que identifique os erros cometidos por funcionários em todo o mundo que levem a vazamento de dados. Duas pesquisas foram conduzidas em dez países: Estados Unidos, Reino Unido, França, Alemanha, Itália, Japão, China, Índia, Austrália e Brasil. Como a meta do estudo era examinar as tendências comportamentais de funcionários do mundo inteiro, os dez países foram selecionados com base em suas culturas sociais e corporativas contrastantes, assim como o domínio de cada força de trabalho das redes IP corporativa e da Internet. Em cada um dos países, 100 funcionários e 100 profissionais de TI participaram da pesquisa, totalizando 2000 entrevistados.

Os resultados da pesquisa revelam diversos comportamentos de risco e uma completa desconsideração pelas políticas de segurança. Uma das descobertas mais notáveis é a prevalência variável de comportamentos específicos em diferentes partes do mundo. Por exemplo:

- A China tem um nível de abuso de tecnologia da informação tão elevado que os executivos de TI costumam fazer auditoria nos computadores para encontrar conteúdo não-autorizado.
- No Japão, 65% dos usuários finais não aderem à política de TI corporativa o tempo todo, e a pesquisa indica que o abuso da tecnologia da informação pelo usuário final está aumentando.
- Os usuários finais na Índia tendem a usar email e mensagem instantânea para fins pessoais e alterar as configurações de segurança de TI nos computadores corporativos para que possam acessar websites não-autorizados.
- Os funcionários no Brasil usam os computadores da empresa para comunicações pessoais e para outras atividades como download de músicas.
- Os usuários na França têm a menor taxa de conformidade com a política de TI de todos os países pesquisados, com apenas 16% dos funcionários afirmando que aderem às políticas de segurança o tempo todo.

O nível de percepção dos de gerentes de TI sobre o comportamento de risco de funcionários também varia conforme o país. Na China, os gerentes de TI confrontam diretamente os funcionários por não aderirem às políticas de segurança. Os profissionais de TI na Índia possuem uma baixa percepção da extensão a que a segurança está sendo comprometida pelos funcionários, com menos da metade acreditando que os usuários estejam usando programas e aplicativos não

pertinentes nos computadores da sua empresa. O Brasil demonstrou ter o maior alinhamento entre o abuso da TI pelos funcionários e a percepção dos executivos de TI do comportamento dos funcionários, com os executivos de TI avaliando e atualizando as políticas corporativas com mais frequência do que em qualquer outro país pesquisado.

1 http://www.privacyrights.org, 2008

Essas diferenças tornam ainda mais difícil para as empresas multinacionais tentar manter uma política de segurança centralizada para sedes e departamentos de TI distribuídos. E com cada vez mais funcionários aderindo à tendência global de trabalhar em casa e em trânsito, as linhas entre vida profissional e vida pessoal estão ficando ainda mais tênues. Combinar comportamentos culturais com o uso de celulares, laptops, aplicativos Web 2.0, vídeo e outras mídias sociais em casa, no trabalho e em viagens cria um ambiente ainda mais complexo para proteger. As organizações globais precisam entender o ambiente de trabalho hoje e abraçar as diferenças culturais em comportamentos e como elas afetam os riscos para dados, além de ajustar a educação, as políticas e a tecnologia à cultura local.

Comportamentos de risco revelados

Os funcionários revelaram comportamentos surpreendentes que colocam os dados e ativos da empresa em risco, apesar de as políticas corporativas estabelecerem procedimentos adequados. Os exemplos a seguir demonstram como os funcionários, conscientemente ou não, perdem e vazam dados.

Uso de aplicativo não-autorizado

Usar aplicativos não-autorizados nas redes corporativas pode colocar em risco os dados confidenciais da empresa e as informações pessoais dos funcionários. O email pessoal é o aplicativo não autorizado usado com mais frequência, seguido por banco online, pagamento de contas online, compras online e mensagens instantâneas.

Esses aplicativos apresentam um alto risco para perda de dados por funcionários ou roubo de dados por hackers, já que não costumam ser monitorados e não adotam os padrões de segurança da empresa. Os funcionários que usam esses aplicativos também correm o risco de infectarem a rede em sites maliciosos.

- 78% dos funcionários já acessaram email pessoal dos computadores da empresa. Este número é quase o dobro do nível do uso autorizado.
- 63% dos funcionários admitem usar diariamente um computador de trabalho para uso pessoal, e 83% admitem usar um computador de trabalho para fins pessoais, pelo menos, de vez em quando.
- 70% dos profissionais de TI acreditam que o uso de programas não-autorizados foi responsável por metade dos incidentes de perda de dados em suas empresas. Essa crença foi mais comum nos Estados Unidos (74%), Brasil (75%) e Índia (79%).

Uso inadequado dos computadores da empresa

Muitos funcionários conscientemente usam os computadores da empresa de formas que prejudicam as políticas de segurança de TI. Alguns exemplos incluem alterar as configurações de segurança e compartilhar os dispositivos de trabalho e as informações confidenciais com pessoas que não trabalham na empresa. Os funcionários burlaram as configurações de TI para fazer o download de música, compras on-line, pagar contas e, em alguns casos, visitar sites de jogos on-line e de pornografia. Aproximadamente, um quarto dos funcionários pesquisados admitiu compartilhar informações confidenciais com amigos, familiares ou mesmos estranhos, e quase

metade dos funcionários pesquisados compartilha dispositivos de trabalho com pessoas fora da empresa sem supervisão. Esses comportamentos podem resultar em vazamento de propriedade intelectual da empresa e cair nas mãos de indivíduos que representem sérias ameaças à segurança e à lucratividade da empresa.

- Ignorar a política corporativa e configurações de segurança de TI

  China: 42%
  Brasil: 26%
  Índia: 20%

- Compartilhar informações corporativas confidenciais fora da empresa.

  Brasil: 47%
  Índia: 27%
  Reino Unido: 26%
  Itália: 22%
  Alemanha: 24%

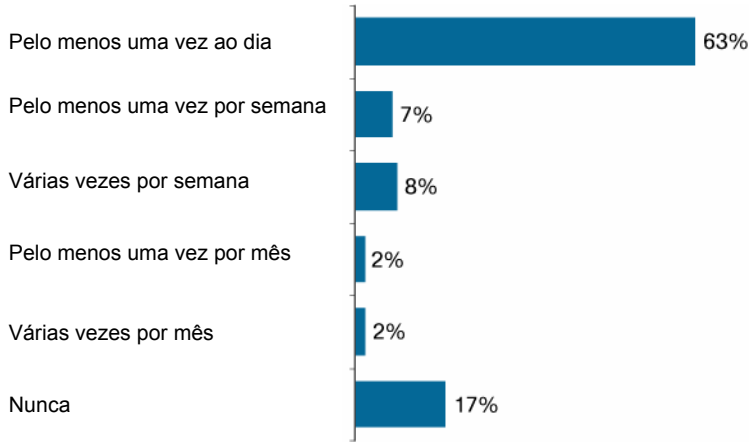
- Compartilhar dispositivo de trabalho com terceiros sem supervisão.

  China: 43%
  Índia: 28%

- Comentários gerais: 44% (32% dos entrevistados compartilharam dispositivos de trabalho com colegas, e 19% compartilham seus dispositivos de trabalho com familiares e amigos que não trabalham na empresa).

A Figura 1 mostra a frequência com que os computadores corporativos são usados para uso pessoal.

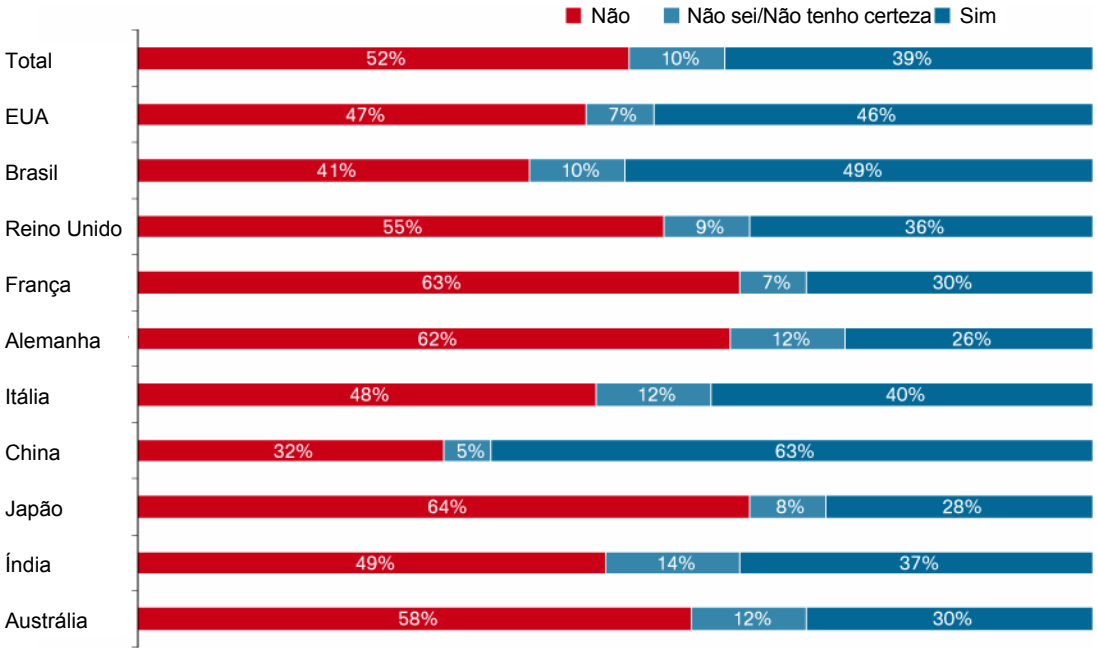
Figura 1. Frequência de uso pessoal



Acesso físico e acesso à rede não-autorizados

Muitos funcionários permitem que pessoas desconhecidas entrem nas instalações da empresa junto com elas sem se identificarem ou permitem que não-funcionários circulem com liberdade pelas instalações da empresa sem supervisão. Essas ações dão a indivíduos não-autorizados a oportunidade de roubar fisicamente recursos corporativos ou acessar informações confidenciais. Às vezes, os próprios funcionários são culpados por acessar partes não-autorizadas de uma rede ou instalação. A Figura 2 mostra o número de vezes que a TI teve que lidar com um funcionário para acessar redes ou instalações não-autorizadas:

Figura 2. Os executivos de TI encontram acesso não-autorizado físico ou à rede



- 39% dos profissionais de TI afirmam que tiveram casos em que os funcionários acessaram partes não autorizadas da rede ou das instalações da empresa, com praticamente metade dos profissionais de TI reportando isso no Brasil (49%) e nos Estados Unidos (46%), e 63% na China. Embora o Japão (28%) e a Alemanha (26%) tenham apresentado menos incidentes entre profissionais de TI, em todos os países, pelo menos um quarto de seus profissionais de TI registrou esses tipos de incidentes.
- O acesso físico e o acesso à rede não-autorizados são maiores nas empresas de médio e grande porte (46%), mas as pequenas empresas também têm incidentes frequentes (32%).
- 22% de funcionários alemães permitem que não-funcionários perambulem pelos escritórios sem supervisão.

Segurança de funcionário remoto

Como as empresas estão cada vez mais distribuídas, os funcionários móveis ampliam o risco potencial para perda de dados. Comportamentos como transferir arquivos de um dispositivo de trabalho para um computador doméstico que não seja protegido ou mantido conforme os padrões da TI, usar comunicações pessoais que não sejam seguras para comunicações corporativas, conversar sobre informações corporativas onde outras pessoas possam ouvir a conversa, e não usar uma proteção de privacidade no laptop ao trabalhar remotamente em um local público, tudo isso convida ao roubo de informações. Os funcionários também não protegem equipamento como computadores laptop e dispositivos de armazenamento portáteis, que pode ser roubados ou perdidos.

- 46% dos funcionários admitiram transferir arquivos entre os computadores de trabalho e pessoal ao trabalhar de casa.
- Mais de 75% dos funcionários não usam uma proteção de privacidade ao trabalhar remotamente em um local público. Esse número é bem maior no Brasil, na China e na Índia—os países que apresentam o comportamento mais imprudente.
- 68% das pessoas não se lembram de falar baixo ao telefone quando estão em locais públicos fora do escritório.
- 13% das pessoas que trabalham em casa admitem que não conseguem se comunicar pela rede da empresa, e mandam email para clientes, parceiros e colegas através de seu email pessoal.

Mau uso das senhas e procedimentos de login/logout

Fazer o logout de um computador e usar senha são alguns dos meios mais antigos e simples de proteger o computador. É difícil imaginar que usuários com bons conhecimentos técnicos ignorem esses recursos de segurança básicos, mas eles o fazem, e em números surpreendentes. Pelo menos, um a cada três funcionários afirmaram que deixam os computadores conectados e desbloqueados quando saem de suas mesas, como quando vão almoçar ou vão para casa à noite. Outra prática comum é deixar um laptop na mesa durante a noite, muitas vezes sem fazer o logoff. Um em cinco funcionários armazenam informações de login do sistema e senhas no próprio computador ou anotam e deixam na sua mesa, em armários não trancados ou colados em seus computadores.

Qualquer dessas falhas em observar o protocolo de segurança fornece oportunidades perigosas para os hackers. Reunidas, elas não apenas abrem a porta para ameaças em potencial, mas também convidam o invasor a entrar. Por exemplo, um funcionário que deixa um sistema ativado em uma mesa e com uma senha colada nele está convidando um invasor a roubar o computador agora e usar os dados confidenciais como bem entender. Se o funcionário usou o computador para fins pessoais, essas informações agora também estão disponíveis para o invasor.

- 28% dos funcionários na China armazenam as informações de login e senha para contas financeiras pessoais em seus dispositivos de trabalho.
- 18% dos funcionários compartilham senhas com colegas, e essa taxa pula para 25% na China, na Índia e na Itália.
- 10% dos funcionários na Índia, nos Estados Unidos e na Itália mantêm anotações com as informações de login e senhas na sua mesa de trabalho, tornando os dados confidenciais acessíveis se a máquina for roubada mesmo que eles tenham feito o logoff do computador.
- 5% dos funcionários no Reino Unido e na França deixam as senhas de contas pessoais e financeiras impressas em suas mesas em trabalho, portanto suas informações podem ser roubadas com qualquer outro computador, mesmo que o seu computador de trabalho esteja protegido.

Por que os funcionários colocam os dados em risco

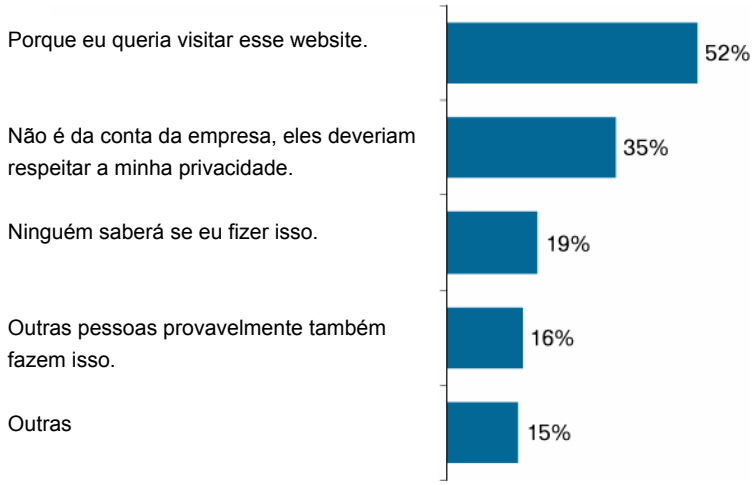
Desenvolver estatísticas que mostrem como muitos funcionários apresentam comportamentos que reduzem a segurança dos dados é um exercício compensador, mas o verdadeiro valor é obtido com a compreensão de como alterar esses comportamentos e aumentar a segurança dos dados. Para isso, as empresas precisam entender como os funcionários veem a segurança e por que ignoram os procedimentos da empresa.

A pesquisa InsightExpress analisou além das estatísticas e perguntou aos funcionários por que eles se comportaram de uma maneira que coloque os dados em risco. A pesquisa apresentou essas conclusões no contexto de empresas de grande e pequeno porte, culturas diferentes e perspectivas de funcionários e profissionais de TI.

Como os resultados da pesquisa relevaram, a não-conformidade de funcionários frequentemente supera a importância da conformidade das políticas de segurança. Quando a pesquisa perguntou por que os funcionários compartilham informações confidenciais da empresa; por exemplo, 44% responderam que precisam “trocar idéias com as pessoas”. Outras razões comuns são “Eu preciso ventilar as idéias" (30%) e “Não vi nada de errado com isso” (29%). Quando perguntados por que alteraram as configurações de segurança nos computadores em um claro desrespeito às medidas de segurança da empresa, a resposta foi ainda mais insolente, já que 35% acreditaram que “não é da conta de ninguém”. E esses funcionários incluíram a equipe de TI nesta crença. Cinquenta e dois por cento responderam que queriam ver o site não-autorizado, independentemente de isso não ser permitido pela política da empresa. Trinta e cinco por cento acharam que isso passaria despercebido e ninguém se daria conta.

A Figura 3 mostra em formato gráfico as razões que levaram os funcionários a alterar as configurações de segurança em seus computadores.

Figura 3. As razões para alterar as configurações de segurança.



Em algumas situações, o motivo para colocar os dados em risco era financeiro. É simplesmente mais barato usar o computador fornecido pela empresa para uso familiar ou doméstico. Esse é um motivo bem sedutor em culturas onde um grande número de familiares mora na mesma casa, mas isso aumenta bastante o potencial de não-funcionários acessarem informações da empresa.

É claro, em alguns casos, o problema não é que o funcionário simplesmente ignore a ameaça, o próprio funcionário é a ameaça. Se os funcionários estiverem insatisfeitos com seus trabalhos, com raiva de seu gerente ou com sentimento de vingança por qualquer que seja o motivo, eles podem se tornar uma “ameaça interna” que deliberadamente danifica ou vaza dados.

Apesar de todos os esforços do departamento de TI, é possível que alguns funcionários não entendam os procedimentos de segurança implantados no ambiente de trabalho. O número de funcionários que usa os serviços de comunicação comparado ao número que tem autorização do departamento de TI para tal revela algumas diferenças interessantes. Mais claramente, uma parte consideravelmente maior de usuários finais usa o email pessoal no trabalho (49%) comparado à proporção que diz que isso é permitido na sua empresa (40%). Na China e no Japão, a diferença entre aqueles que usam email pessoal no trabalho e os que afirmam que isso é autorizado pela TI é ainda maior.

Os números da pesquisa indicam que embora muitas empresas tenham tentado evitar que os funcionários vazem dados, seus esforços não estão atingindo os resultados desejados.

Contendo o vazamento de dados

As ameaças à segurança dos dados continuam a evoluir. Os hackers estão cada vez ligados ao crime, e os ataques têm como objetivo o lucro. A maioria dos perigos é originada na Internet, que é um componente vital da infraestrutura corporativa de hoje. E neste ambiente perigoso, os funcionários de todo o mundo estão vazando dados, apesar de todos os esforços da TI para interromper esse fluxo.

Com ignorância, desobediência e puro descuido como principais causas do vazamento de dados por funcionários, não existe receita mágica para proteger os dados da empresa, especialmente já que as empresas e seus dados se tornam bem mais móveis e operam com limites virtuais, em vez de físicos. A forma mais eficiente de evitar o vazamento de dados é oferecer suporte a um processo contínuo com uma abordagem geral que seja holística e estratégica.

Muitas empresas erram ao confiar demais no poder da tecnologia, ou ao iniciar um programa de segurança com um bombardeio de tecnologias. A melhor tecnologia de segurança do mundo não oferecerá um bom retorno do investimento sem uma base adequada de processos, políticas e educação de segurança.

Em vez disso, as empresas devem começar avaliando o comportamento de cada funcionário e os riscos associados a ele com base em fatores como localização e cenário de ameaças. Em seguida, um programa educativo sobre as ameaças, treinamento em segurança e processos corporativos podem ser elaborados com base nessas informações de inteligência. Neste ponto, os investimentos apropriados em tecnologia da segurança poderão ser aplicados.

Essa abordagem abrangente é a melhor forma de obter uma segurança sustentável. Ela cria uma base para analisar continuamente os riscos de cada interação entre usuários e redes, pontos terminais, aplicativos, dados e, é claro, outros usuários. Principalmente, ela torna a segurança parte integrante da cultura da empresa como ela é parte da infraestrutura de TI.

Veja alguns passos tangíveis que você pode dar para evitar o vazamento de dados.

Conheça seus dados e gerencie-os bem — Como o objetivo da colaboração é ser aberta e compartilhar informações, proteger seus dados começa pela compreensão de como as pessoas interagem entre elas diariamente.
É aconselhável:

- Implantar ferramentas e processos que monitorem a movimentação de seus dados para que você saiba onde eles estão armazenados, como são acessados e por quem estão sendo usados.
- Identificar os tipos de dados que exigem uma proteção especial dentro e fora das paredes da sua empresa.
- Considerar novas abordagens de segurança para ferramentas e recursos de próxima geração.

Proteja os dados da empresa como se fosse seu bem mais precioso — Ensine os funcionários que os dados da empresa são fundamentalmente dinheiro: perder ou vazar dados corporativos é como jogar dinheiro fora e permitir que as pessoas que apresentam a maior ameaça a você tenham acesso e os usem contra você. E os dados provavelmente serão usados para prejudicar a marca da sua empresa, a receita, o preço da ação e a credibilidade do mercado.Os funcionários devem entender e implementar procedimentos de segurança básicos:

- Proteger sistemas usando apenas aplicativos e métodos de acesso autorizados, mantendo o software de segurança como aplicativos antivírus, respeitando e mantendo as configurações de segurança, entendendo as consequências de aprovar e negar as ações de pop-up do

Cisco® Security Agent e preparando-se para se proteger de spam, malware, phishing e outros métodos de ataque.
- Proteger dispositivos portáteis mantendo-os em sua posse ou travados o tempo todo, sem compartilhar seus dispositivos de trabalho ou usá-los para atividades pessoais, não transferir informações confidenciais dos sistemas de trabalho para dispositivos pessoais e não acessar sites indevidos ou fazer download de informações inadequadas.
- Evitar acesso a dados não-autorizados fazendo logoff ou bloqueando sistemas quando você se ausenta por alguns instantes ou vai para casa, usando boas técnicas de criação de senha e não compartilhar as senhas e armazená-las com segurança.
- Evitar o roubo de dados ao viajar falando baixo quando tiver que conversar sobre informações confidenciais em locais públicos, usar filtros de privacidade para evitar que as pessoas espiem, usar uma VPN, e nunca usar uma impressora a menos que você esteja do lado para pegar o papel.

Institucionalize os códigos padrão para conduta de segurança na sua empresa — As políticas de segurança da informação são parte integrante da conduta do código de negócios da empresa e precisam ser lidas, entendidas e seguidas. Os profissionais de TI devem pensar globalmente e agir localmente definindo objetivos de políticas globais e criando educação que seja adequada a cultura de um país e ao cenário de ameaças. Os funcionários precisam entender que eles têm uma função crítica na manutenção da segurança da empresa e aceitar a sua responsabilidade na proteção da empresa. Sacrificar a qualidade e a garantia de segurança para obter maior agilidade é um erro que as empresas não podem se dar ao luxo de cometer. Cada funcionário deverá:

- Conduzir atividades diárias de acordo com o código de conduta de negócios da empresa, particularmente as que pertencem à segurança da informação.
- Estar constantemente atento ao seu ambiente e ser cuidadoso com a segurança em todas as ações realizadas no escritório, em casa ou em viagem.
- Aprender como tratar os diferentes níveis de confidencialidade da documentação da empresa. Isso inclui a compreensão das diferenças entre “pública”, “confidencial”, “altamente confidencial” e “restrita”.

Promova uma cultura e ambiente aberto e confiável — Os funcionários devem se sentir confortáveis com o cenário de segurança da empresa para implementar as diretivas de segurança. Eles devem conhecer a segurança apropriada da empresa para reportar comportamentos suspeitos, ataques identificados ou incidentes de segurança (mesmo que eles sejam a causa) e se sintam confortáveis iniciando o contato. Os profissionais de TI devem ensinar aos funcionários:

- Como evitar os erros de segurança identificando áreas de grande vulnerabilidade.
- Práticas apropriadas para proteger sistemas e dados.
- O que é um incidente de segurança e como ele é reportado.

Estabeleça uma conscientização sobre a segurança e práticas educativas sua empresa — Criar uma conscientização sobre questões de segurança é essencial para obter o envolvimento dos funcionários. Os funcionários que acreditam que os programas de segurança são importantes têm maior probabilidade de seguir procedimentos específicos. Uma prática de educação deve:

- Educar e treinar os funcionários com relação às expectativas da empresa para proteger os dados.
- Incluir a conscientização da segurança e práticas em eventos de orientação de nova contratação.
- Treinar funcionários sobre as considerações de segurança ao atender o telefone e conectar a Web 2.0, sites de rede social e colaboração.
- Treinar funcionários em questões de segurança física, como permitir que apenas funcionários devidamente identificados com crachás entrem no edifício.

Um futuro seguro

Evitar o vazamento de dados é um desafio que precisa contar com a participação de toda a empresa. Quanto mais pessoas entenderem esse desafio, desde profissionais de TI a executivos e funcionários em todos os níveis de responsabilidade, mais bem-sucedida será a empresa em proteger seus ativos críticos. O principal objetivo é que todos, em todos os níveis, acreditem que a segurança corporativa é fundamental, entendam as políticas e os procedimentos necessários para atingir um ambiente seguro e implementem as atividades necessárias todos os dias. Essa mudança de cultura é um processo. E de acordo com a pesquisa da InsightExpress, é um processo para o qual as empresas em todo o mundo precisam dedicar mais recursos. Com vontade e investimentos suficientes, as empresas podem reduzir vazamento de dados. A recompensa valerá o esforço.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**