

Principais insights	ii
Introdução	1
Aumenta a ansiedade nos conselhos e na diretoria.	2
A segurança digital inadequada prejudica a inovação e a competitividade	4
Os executivos sabem que a segurança digital viabiliza o crescimento, mas mesmo assim não investem o suficiente nessa área	6
A segurança digital viabiliza t343hBiliza t343hBiliza t343hBiliza t343h	

Principais insights

Introdução

pelas fontes de receita e pelas principais operações da empresa. Em última análise, quando uma empresa lança um novo produto ou um aplicativo móvel, um executivo da linha de negócios é responsável pelo desenvolvimento e pela execução, um fato que esses executivos reconhecem. 54% dos executivos da linha de negócios afirmam

sofre uma violação de dados, os clientes não se sentirão mais confortáveis em compartilhar informações pessoais. Como resultado, o varejista não poderá oferecer a [experiência de hiper-relevância](#) guiada por análise nas lojas físicas e on-line que os compradores esperam. Esses clientes mudarão para um varejista que possa proporcionar uma experiência melhor ao cliente executada por dados protegidos.

Os executivos também temem que os recursos estratégicos como a

O estudo não encontrou nenhuma correlação forte entre a localização geográfica e a preocupação quanto ao impacto da segurança digital na inovação. A ameaça percebida pela fragilidade da segurança digital quanto à inovação foi a maior entre os entrevistados da Índia, da China, do Reino Unido e do Canadá, enquanto foi a menor entre os entrevistados dos EUA. A Índia e o Brasil têm as mais altas porcentagens de entrevistados que disseram que sua organização tinha interrompido uma iniciativa de missão crítica devido a preocupações de segurança digital.

Observou-se maior quantidade de ameaças à inovação de serviços empresariais, varejo, bancos e produtos de tecnologia entre os setores. Foi menor nos setores de hospitalidade/viagem/entretenimento e de produção/bens de consumo. Os serviços empresariais interromperam a maioria das iniciativas de missão crítica devido às preocupações com segurança digital, seguidas pelos produtos de tecnologia e pela educação.

Diversos setores têm enfrentado níveis mais altos de impacto digital.

desenvolver produtos e serviços digitais devido aos possíveis riscos de segurança digital.² Infelizmente, são esses os produtos e serviços que eles precisam para competir com as tecnologias inovadoras.

Ao mesmo tempo em que as preocupações com a segurança digital podem dificultar a busca por inovações e modelos digitais de negócios, muitas empresas acreditam que devem prosseguir ou ficarão para trás devido aos avanços digitais e outros concorrentes. Na verdade, 73% dos entrevistados da pesquisa admitiram que frequentemente adotam novas tecnologias e processos comerciais, independentemente do risco de segurança digital.

A segurança digital abaixo do padrão deixa as empresas na pior

Considerando as conexões estreitas entre segurança digital, digitalização e inovação, a excelência na segurança digital está sendo vista cada vez mais como um determinante de valor comercial. De acordo com nossa pesquisa, quase um terço dos executivos (31%) já fez essa conexão: eles veem a "possibilidade de crescimento" como o *principal* objetivo da segurança digital. Enquanto isso, 69% dos executivos consideram que o objetivo principal da segurança digital seja a "redução de riscos".

o tipo de transformação digital que permite uma resposta ágil ao mercados dinâmicos. Essa agilidade torna as empresas mais eficientes e leva a um melhor desempenho financeiro.

A excelência em segurança digital também oferece às empresas a oportunidade de diferenciar suas marcas ao demonstrar que valorizam a confiança do cliente. Quando os prospects e os clientes acreditam que as violações de segurança e privacidade não ocorrerão, essa crença se torna uma característica importante da marca, semelhante à qualidade, ao custo e à experiência do cliente. Se promovida, essa característica pode proporcionar às empresas vantagem competitiva.²

A segurança digital viabiliza a inovação e o crescimento de mais de 400 casos de uso digitais

A Cisco identificou 414 casos de uso digitais que impulsionarão os US\$ 7,6 trilhões em receita digital adicional na próxima década (consulte "Como estabelecer um valor pela segurança" para saber mais detalhes).

Para conquistar sua parte, primeiro você precisa acertar o lado defensivo da segurança digital. Sete casos de uso de defesa específicos disponibilizarão US\$ 1,8 trilhões em receita adicional digital nos próximos 10 anos. Elas incluem a proteção da propriedade intelectual, a redução de dados comprometidos (informações internas e do cliente), maior tempo de atividade da empresa e tempo de inatividade da rede reduzido, proteção de recursos financeiros,

Com base no grau de risco digital associado a cada caso de uso, a análise considerou vários graus de atraso na adoção da segurança digital, variando entre um e cinco anos. Quanto maior o risco, mais tempo leva para enfrentar e solucionar questões de percepção. Este risco pode inibir iniciativas de crescimento que dependam de recursos digitais—e tornar o ritmo de inovação e de transformação digital mais lento.

Portanto, nossa estimativa conservadora de crescimento de US\$ 5,8 trilhões seria ainda maior se não fosse pelo medo em relação à segurança digital que fará com que algumas empresas

Como contraponto, há o caso de uso de *manutenção remota*.

A manutenção remota às vezes exige que as empresas abram suas redes para

sistemas remotos não estão conectados. Ou são conectados sob demanda, o que pode causar a demora da solução de um problema. O resultado é o aumento dos custos de litígio, limpeza e período de inatividade do sistema.

A Cisco determinou que a segurança digital tem um papel determinante no caso de uso de controle de vazamento de petróleo. Como resultado, as preocupações de segurança digital poderiam resultar em um atraso da adoção de três a cinco anos.

Um subconjunto (28%) dos entrevistados, no entanto, está buscando a digitalização com certa urgência. Esse grupo entende que pode melhorar a segurança digital com a transformação digital. Esses "digitalizadores de segurança" parecem melhor preparados para lidar com os avanços digitais e superar outros concorrentes pois estes estão bastante comprometidos com o crescimento através de ofertas e modelos digitais de negócios (veja a [Figura 11](#) e "Os digitalizadores

Como resultado, eles se encarregam de projetos digitais com mais confiança. Isso permite uma inovação mais rápida e a conquista de uma parte maior da receita digital adicional. Na verdade, 62% dos digitalizadores de segurança relatam que têm desempenho muito melhor que seus colegas em termos de receita de novos produtos e

2. Reduza os riscos ao escolher projetos com uma proporção de alto grau entre a oportunidade e o risco, e não apenas um perfil de baixo risco. Os digitalizadores de segurança correm mais riscos, mas a recompensa supera os custos.

