A segurança digital como uma vantagem para o crescimento

Autores

Joel Barbier

Lauren Buckalew

Jeff Loucks

Robert Moriarty

Kathy O'Connell

Michael Riegel

Principais insights

- Em uma era de inovação sem precedentes, as empresas precisam começar a ver a segurança digital além da sua função "defensiva" tradicional.
- Como Mike Dahn, chefe de relações de segurança de dados e do setor da Square, Inc., afirmou, "Acho que é realmente importante que paremos de pensar em segurança como uma abordagem centrada na defesa e vendida pelo medo, pela incerteza e pela dúvida. Precisamos começar a pensar nela como um viabilizador que sustenta a inovação e ajuda a empresa a avançar."
- Um novo estudo da Cisco[1] indica que um número crescente de empresas está fazendo exatamente isso.
- 39% dos 1014 entrevistados da pesquisa (executivos seniores de finanças e de linha de negócios) acreditam que o objetivo principal da segurança digital é **viabilizar o crescimento**. 69% ainda consideram que o objetivo principal seja a redução de riscos.
- 44% consideram que a segurança digital seja uma **vantagem competitiva** para sua empresa. 56% a veem como um custo para fazer negócios.
- Os executivos reconhecem a conexão básica entre a segurança digital e a *digitalização*— o movimento de operações, processos e funções de negócios em um único modelo operacional digital novo.
- Há muito em jogo. A Cisco identificou **414 casos de uso** que impulsionarão US$ 7,6 trilhões em receita adicional digital[2] globalmente durante a próxima década.
- Mais de três quartos dessa quantidade envolvem **a segurança digital como um viabilizador de crescimento**.
- Infelizmente, muitas empresas estão deixando essa oportunidade escapar. Nossa pesquisa revela que 71% acreditam que **os riscos da segurança digital impedem a inovação**. 39% **interromperam uma iniciativa de missão crítica devido a preocupações com relação à segurança digital**.
- A incerteza quanto à segurança digital também está fazendo com que as empresas adiem iniciativas digitais essenciais. Essas iniciativas podem ser os principais diferenciais de uma economia cada vez mais competitiva.
- As empresas precisam seguir o exemplo dos **"digitalizadores de segurança"**, que estão plenamente comprometidos com o crescimento através de modelos digitais de negócios e ofertas, com a segurança digital como base essencial.

"A economia digital não é apenas uma versão digitalizada da economia atual. A segurança digital é importante nessa discussão, tanto por conta das ameaças que combate, quanto pelas possibilidades que ela oferece."

– Adriaan Bouten, Fundador e CEO, dPrism

Introdução

Agora, as tecnologias inovadoras aproveitam o poder digital para criar novas fontes de valor que reduzem custos, melhoram a experiência do cliente e expandem suas ofertas.[3] As tecnologias inovadoras digitais também têm uma vantagem decisiva de inovação em empresas estabelecidas: elas podem identificar melhor novas oportunidades e se mover mais rapidamente para aproveitá-las.[4]

Nesse ambiente intensamente competitivo, empresas start-up e empresas ágeis estão ultrapassando os concorrentes com produtos, serviços e modelos digitais de negócios.[5]

Todas as empresas estão sendo atraídas para o centro de um "turbilhão digital", que se caracteriza pelas mudanças exponenciais e pelas linhas indistintas do setor.[6] As empresas devem se adaptar ou suas chances de serem substituídas, ou até de saírem do negócio por completo, aumentam muito. Em um estudo recente feito pelo Centro Global de Transformação Empresarial Digital, uma iniciativa da IMD e da Cisco, prevê que quatro dos 10 líderes de cada setor serão substituídos pelas tecnologias digitais inovadoras nos próximos cinco anos.[7]

Empresas já estabelecidas podem competir e prosperar no turbilhão digital ao encontrar "espaços de valor" – oportunidades de mercado prontas para serem exploradas pelas tecnologias digitais inovadoras–e ao adotar estratégias digitais que levam à busca pela inovação.[8]

A transformação digital, no entanto, exige uma base de segurança digital sólida. Com essa base, as empresas terão confiança para implementar as tecnologias e os processos digitais que impulsionam a inovação e o crescimento. Sem isso, as empresas podem hesitar em iniciar projetos digitais reprimindo o potencial de inovação e abrindo a porta para as tecnologias digitais inovadoras.

Aumenta a ansiedade nos conselhos e na diretoria

A maioria dos líderes de diretoria ainda estão pensando sobre como extinguir ameaças, quando poderiam estar pensando no crescimento real que a segurança digital de qualidade possibilita. À medida que o número de violações de segurança digital se dissemina rapidamente,[9] a outrora surpreendente aceitação de que milhões de registros foram comprometidos por hackers externos tornou-se assustadoramente comum.

Os executivos seniores estão atentos: 87% disseram que estão preocupados com a possibilidade de violações de segurança digital em suas empresas. Quase metade está "muito preocupada". 41% estão "muito mais preocupados" do que estavam há apenas três anos.

Essa ansiedade vai muito além da empresa de TI. Os CEOs e a diretoria são considerados os principais responsáveis por grandes incidentes de segurança digital (veja a Figura 1), mas os executivos responsáveis pelo risco empresarial, os diretores executivos de segurança da informação (CISOs) e os CIOs, e os chefes de departamentos compartilham a responsabilidade quando as coisas dão errado.

Os executivos financeiros e da linha de negócios ressaltaram que a segurança digital se tornou uma preocupação de nível de diretoria. Os comitês de auditoria em particular estão sondando os pontos fracos da segurança digital de suas empresas como parte de suas responsabilidades fiduciárias. A segurança digital se tornou um pilar de gerenciamento de risco empresarial, juntamente com o risco financeiro e de segurança. Dessa forma, os comitês de auditoria exigem que os executivos responsáveis pelo gerenciamento de risco empresarial, como CFOs[2] e os diretores de risco, sejam responsabilizados pela segurança digital.

Os executivos empresariais devem confiar naqueles que entendem o lado técnico do risco digital, os CIOs ou, em alguns casos, os CISOs, para propor consultoria e orientações confiáveis. Como a pesquisa da Cisco mostrou, agora 46% dos gastos de TI são controlados pelos executivos da linha de negócios[2], que também são responsáveis

Metodologia

Sobre a pesquisa

Em outubro de 2015, conduzimos uma pesquisa on-line com 1014 diretores, vice-presidentes e executivos da diretoria. Mais de um terço têm funções financeiras e influência no financiamento da segurança digital; o restante faz parte de uma combinação de áreas de linha de negócios. Os entrevistados representaram Austrália, Brasil, Canadá, China, França, Alemanha, Índia, Japão, Reino Unido e Estados Unidos.

Também realizamos entrevistas qualitativas com 11 especialistas; todos são ou já foram executivos seniores com extensa experiência em segurança digital e dois eram especialistas em consultoria de segurança digital.

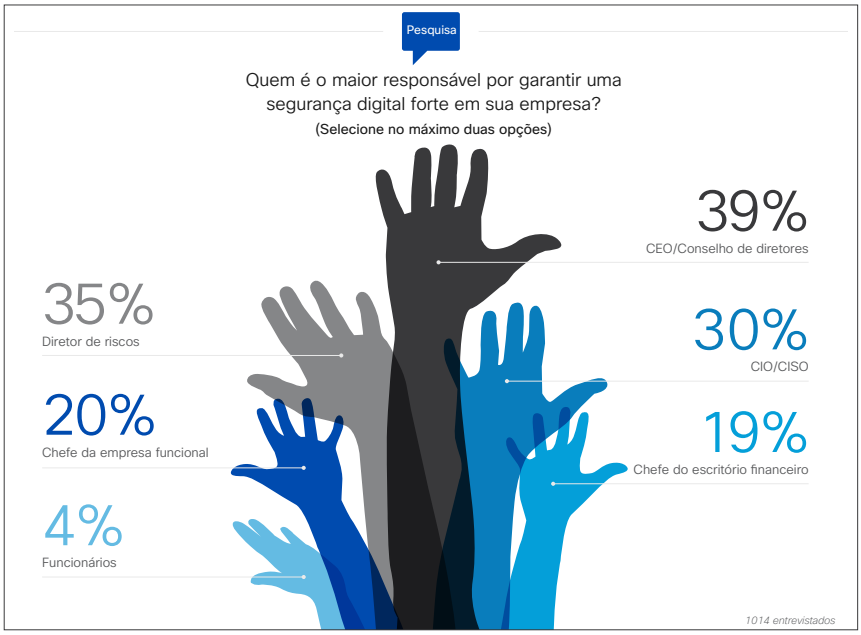

Figura 1
A responsabilidade quanto à segurança digital se estende até o topo

Fonte:
Cisco, 2016

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 que as partes interessadas, como clientes, os responsabilizam " consideravelmente" pela segurança digital.

Como as violações causam danos grandes, os executivos seniores se sentem responsáveis pela sua prevenção.

O custo médio de uma violação de segurança digital é grande e continua crescendo, chegando a US$ 3,79 milhões em 2015 e até US$ 3,52 milhões em 2014.[2]

A repercussão vai muito além dos custos que são mais fáceis de calcular, como resposta a incidentes, investigação forense, auditorias internas e comunicações. De acordo com os executivos financeiros que participaram da pesquisa, a perda de negócio resultante do desgaste da confiança do cliente foi a consequência mais temida (veja a Figura 2). Quando os clientes evitam fazer negócios com uma empresa por temerem que suas contas possam estar vulneráveis a ameaças digitais, milhões em receita podem ser comprometidos.

Figura 2
As consequências das violações são devastadoras e de longo alcance

Fonte:
Cisco, 2016

Informações regionais

Estratégia de segurança digital A responsabilidade varia de acordo com o país

Na China e na Índia, o diretor de risco tem maior probabilidade de ser o principal responsável pela segurança digital (conforme indicado por 44% dos entrevistados em cada país).

No Brasil, Canadá e Reino Unido, o CEO/conselho de diretores é o principal responsável.

Os Estados Unidos foram o único país da pesquisa em que o CIO/CISO ficou em primeiro lugar (37%), com o CEO/conselho logo trás (36%).

O CFO foi identificado como a pessoa responsável em 19% das empresas entrevistadas globalmente. Na China, 29% das empresas consideram o CFO responsável, mais do que em qualquer outro país pesquisado.

Os dados do cliente foram considerados pelos executivos da linha de negócios como os mais importantes a serem protegidos, e o motivo é claro. Os dados perdidos ou comprometidos dos clientes são um catalisador para um host de consequências negativas. As empresas podem esperar a ameaça de processos legais, multas, aumento na regulamentação e custos de correção, além de negócios perdidos. Os executivos foram quase unânimes (92%) quanto à expectativa de uma análise minuciosa de regulamentações e de banqueiros. Anúncios recentes mostram que uma nova onda de regras está a caminho.[2]

Quando as informações do cliente são violadas, as consequências podem ser graves em todos os setores. Por exemplo, se um varejista

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 propriedade intelectual e outras informações confidenciais possam ficar vulneráveis. Os investimentos financeiros e de recursos humanos que as empresas gastam em inovação devem ser levados em conta no custo total de uma violação de dados. Da mesma forma, deve ser levada em conta a perda de posição competitiva quando as empresas concorrentes roubam detalhes de produtos e de planos.

Os executivos também mencionaram a importância de proteger dados financeiros, processos comerciais, fórmulas e contratos com fornecedores. Estão cientes do que os danos perdidos ou os recursos reduzidos podem causar em sua empresa. Muitos temem de onde as ameaças podem vir: 27% identificaram a espionagem industrial como uma das principais preocupações.

A segurança digital inadequada prejudica a inovação e a competitividade

Uma implicação extremamente importante mas frequentemente esquecida da fragilidade da segurança digital é *a forma como ela pode afetar a inovação e o crescimento da empresa*. Isso se aplica especialmente ao desenvolvimento de modelos empresariais e de ofertas digitais.

No nosso estudo, 71% dos executivos disseram que as preocupações com relação à segurança digital estão prejudicando a inovação em suas empresas. 39% dos executivos afirmaram ter interrompido iniciativas de missão crítica devido a problemas de segurança digital (veja a Figura 3).

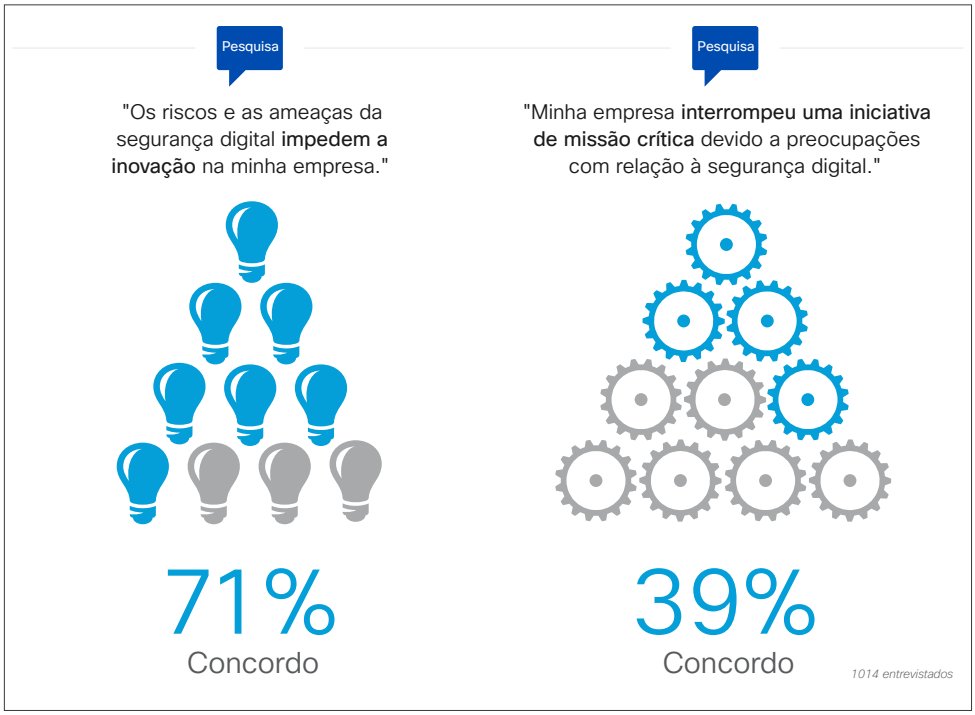

Figura 3
A falta de segurança digital enfraquece a inovação e atrasa os negócios

Fonte:
Cisco, 2016

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. Os líderes de negócios digitais estão bastante cientes dos riscos e benefícios da implementação de produtos e serviços digitais. Eles também têm maior probabilidade de reconhecer a conexão entre segurança frágil e inovação perdida.

A fragilidade da segurança digital é uma "doença silenciosa" que impede a capacidade das empresas inovarem no momento em que menos podem pagar por isso; quando estão sendo arrastados para o turbilhão digital,[2] em que digitalização, tecnologias inovadoras e mudanças exponenciais são o "novo normal".[2] Muitas empresas sofrem dessa doença, mas poucas estão cientes disso. Caso ela não seja tratada, a fragilidade da segurança digital pode ser fatal no turbilhão digital.

No turbilhão digital, as empresas inovadoras normalmente têm três vantagens principais sobre as empresas já estabelecidas: a capacidade de 1) inovar, 2) agir rapidamente e 3) recompensar experiências (veja a Figura 4). Para corresponder ao ritmo e à eficiência das empresas start-up, as empresas já estabelecidas devem estimular seus recursos de inovação. Mesmo assim, 60% dos entrevistados indicaram que as empresas estão relutantes em

"Nossa maior preocupação com as violações de segurança digital está mais relacionada ao impacto financeiro indireto do que ao direto. Qual seria o impacto que nossa reputação sofreria? E se os clientes decidissem que não merecemos sua confiança e mantivessem distância?"

—Greg Kleffner, CFO, Stein Mart

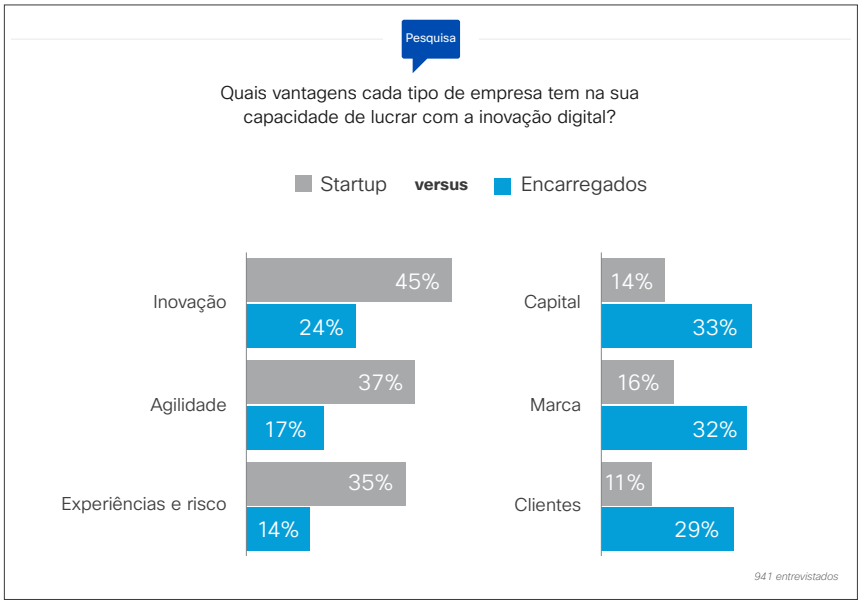

Figura 4
A concorrência tem vantagens, mas ela precisa aprender com as empresas start-up

Fonte:
Centro Global para Transformação Empresarial Digital, 2015

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 posição competitiva possível: não inovam com a rapidez necessária para competir e, ao mesmo, tempo não são seguras o suficiente contra ataques digitais.

Para ter acesso a mais informações, visite cs.co/cyberAB

"As inovações estão evoluindo, mas provavelmente avançam apenas de 70 a 80% do que poderiam se existissem melhores ferramentas de segurança digital."

—Robert Simmons, CFO

Os executivos sabem que a segurança digital viabiliza o crescimento, mas mesmo assim não investem o suficiente nessa área

A exigência da digitalização de produtos, serviços e modelos empresariais é claramente reconhecida pelos principais líderes empresariais. 69% dos executivos dizem que a digitalização é "muito importante" para a atual estratégia de crescimento de suas empresas. Eles também reconhecem que a segurança digital é uma base importante para suas estratégias de crescimento digitais: 64% citaram-na como um determinante "significativo" do sucesso de produtos, serviços e modelos de negócios digitais (veja a Figura 5).

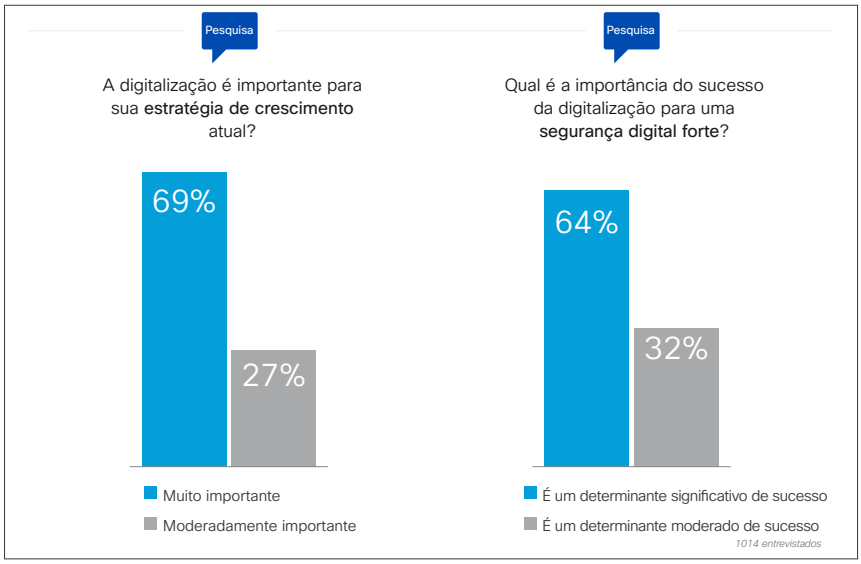

Figura 5
Os executivos compreendem a conexão entre a segurança digital e a digitalização e o crescimento

Fonte:
Cisco, 2016

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".

De forma semelhante, 44% dos executivos consideram que a segurança digital é uma vantagem competitiva para a empresa deles, enquanto 56% a veem como o custo da negociação. A mudança de perspectiva, que deixa de considerar os investimentos em segurança digital estritamente como "defensivos" e passa a considerá-los como a "viabilização" de uma inovação maior, pode estimular a competitividade corporativa.

Países como a China, a Índia e o Canadá (veja a Figura 6) demonstraram otimismo em relação à possibilidade de crescimento e, dentre os entrevistados, os da Índia, da China e do Brasil viram segurança digital como uma vantagem competitiva. Essas opiniões sem dúvida refletem o aumento acentuado da adoção da segurança digital em países em desenvolvimento como China, Índia e Brasil. Na verdade, de acordo com uma análise recente da Cisco, os países em desenvolvimento gerarão quase um terço do valor digital do setor privado mundial até 2024.

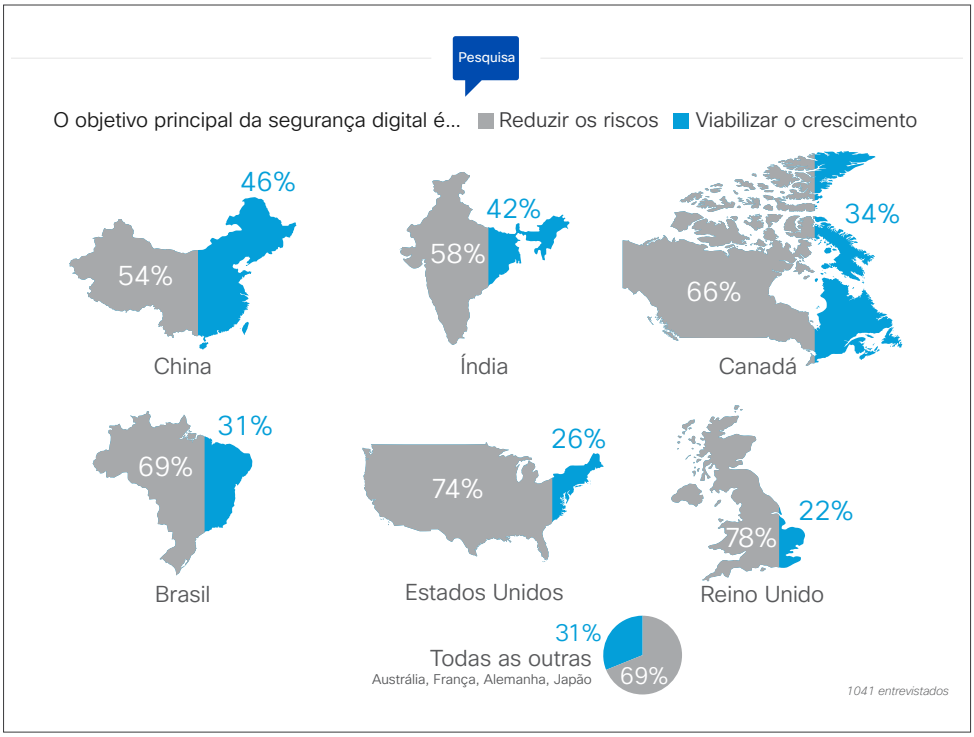

Figura 6
Em todo o mundo, quase um terço dos executivos associam a segurança digital ao crescimento

Fonte:
Cisco, 2016

Os setores de mineração e serviços, varejo e transporte/logística registram as porcentagens mais altas de entrevistados que consideram a segurança digital como um viabilizador de crescimento (veja a Figura 7, na próxima página). Isso mostra que os executivos de quase todos os setores percebem a necessidade de acelerar a inovação e a vinculação crítica entre a segurança digital e os produtos *e* serviços digitais.

As empresas que transformam a excelência em segurança digital em uma vantagem competitiva real podem inovar com mais rapidez e buscar plenamente

"Passar a considerar a segurança digital como uma vantagem estratégica em vez de um mal necessário é uma evolução que coloca você em uma posição de destaque"

—Ex-vice-presidente de RH, banco da Fortune 100

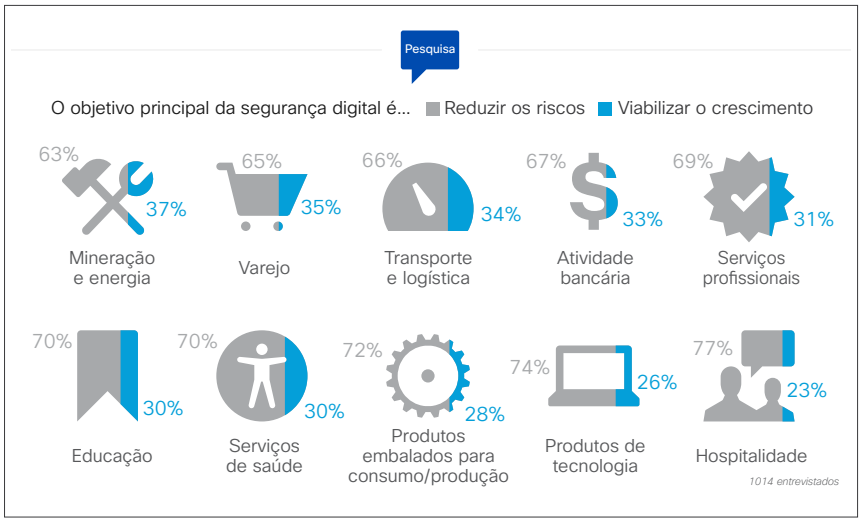

Figura 7
O sentimento de capacitação de crescimento é mais forte nos setores de mineração/energia, varejo e transporte/logística

Fonte:
Cisco, 2016

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]

Esses benefícios estão começando a afetar a maneira como os executivos financeiros investem em segurança digital. Atualmente, a capacidade de viabilizar o crescimento empresarial representa um terço dos critérios de decisão avaliados ao considerar investimentos de segurança digital. Critérios defensivos como a proteção contra ameaças e a conformidade regulamentar representam o restante (veja a Figura 8, na próxima página). À medida que as empresas começam a reconhecer que a excelência em segurança digital pode estimular a agilidade, as operações e a fluência digital, esperamos que a "viabilização do crescimento" se torne um fator mais influente nas decisões de investimento.

Embora o Gartner tenha previsto uma diminuição dos orçamentos de TI corporativa em 2015, [2] as empresas estão priorizando os investimentos em segurança digital. 87% das empresas afirmam que aumentarão os gastos em segurança digital no próximo ano para 41%. Os executivos financeiros entrevistados disseram que está cada vez mais fácil financiar projetos de segurança digital porque há mais clareza sobre seus benefícios.

Para ter acesso a mais informações, visite cs.co/cyberMD

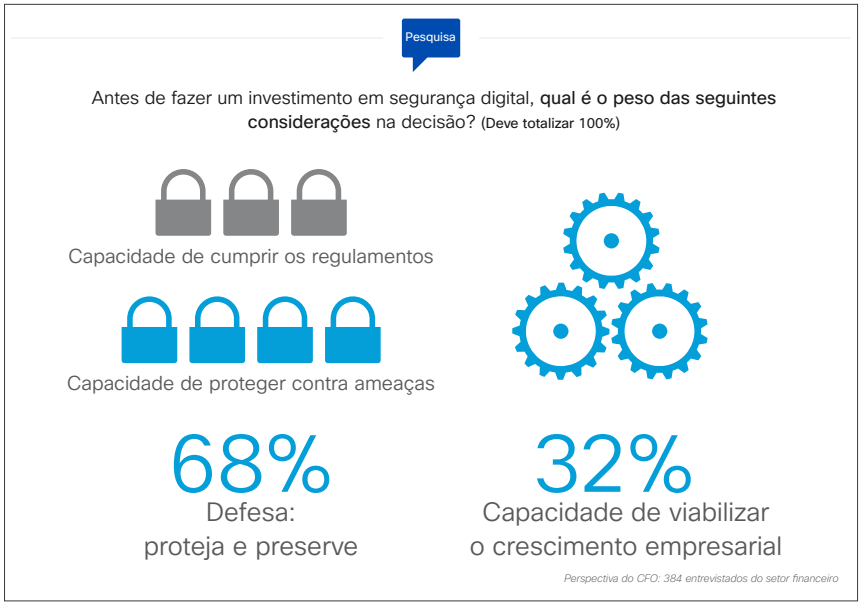

Figura 8
O potencial da segurança digital para estimular o crescimento é uma característica importante para as decisões de investimento

Fonte:
Cisco, 2016

"Não há um livro de regras aqui. É necessário analisar o nível de crise em potencial dos riscos, assim como as oportunidades de crescimento. Acho que a fórmula de alocação é algo com o qual temos dificuldades".

—Robert Simmons, CFO

No entanto, as empresas investiriam ainda mais em segurança digital se pudessem determinar o valor desses benefícios. Aliás, 81% dos executivos financeiros afirmaram que seriam "muito mais" ou "moderadamente mais" propensos a aumentar seus gastos em segurança digital se houvesse uma maneira melhor de avaliar esses resultados comerciais.

Nossos entrevistados reconheceram que têm dificuldades para encontrar as métricas corretas. Embora 88% das empresas usem métricas definidas, como o crescimento de primeiro nível e a lucratividade, para determinar os benefícios comerciais da segurança digital, apenas 42% consideram essas métricas "muito eficientes". As empresas precisam de muito mais que isso para justificar os investimentos estratégicos caros à gerência e às partes interessadas.

Assim, pode-se concluir que a maioria das empresas provavelmente não investe o suficiente em segurança digital. Além disso, nossos entrevistados afirmaram que a falta de investimentos é um de seus maiores desafios de gerenciamento, juntamente com o acompanhamento do ambiente empresarial digital dinâmico e a aplicação ineficiente de protocolos de segurança digital.[2]

Para ter acesso a mais informações, visite cs.co/cyberRS

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, proteção de informações confidenciais nacionais/políticas/do governo e preservação da reputação da empresa.

A maior oportunidade, porém, surge ao tornar a segurança digital a base dos 407 casos de uso digitais que viabilizam a inovação e o crescimento. A Cisco estima que esses casos de uso digitais resultarão em US$ 5,8 trilhões em receita digital adicional entre 2015 e 2024 (veja a Figura 9).

Como determinamos esse valor?

Nosso estudo revelou que as vulnerabilidades e a preocupação com a segurança digital fazem com que muitas empresas hesitem em buscar produtos e serviços digitais. Em alguns casos, as preocupações com relação à segurança digital estão forçando essas empresas a interromper totalmente iniciativas de missão crítica.

Isso tem um custo significativo; as empresas do setor público e privado estão saindo de cena e deixando a inovação digital para os concorrentes mais ágeis. Analisamos o grau de impedimento causado por essas preocupações na realização do valor de mais de 400 possíveis casos de uso digitais ao longo de mais de 10 anos (2015-2024).

Como estabelecer um valor pela segurança

A receita digital adicional é baseada em dois componentes: 1) novas fontes de valor inteiramente provenientes de investimentos e inovações digitais e 2) mudança de valor entre empresas com base na capacidade (ou na incapacidade) de aproveitar os recursos digitais.

A Cisco calculou a receita digital adicional ao adotar uma abordagem "de baixo para cima" usando a soma do valor criado por mais de 400 casos de uso digitais do setor público e privado nos próximos 10 anos (de 2015 a 2024). A receita adicional tem por base o valor líquido: para cada caso de uso, nós consideramos os benefícios e os custos.

Nossos casos de uso refletem o resultado projetado de uma aplicação empresarial da tecnologia; nesse caso, a transformação empresarial orientada pela economia digital/digitalização. Isso difere de "estudos de caso" típicos, que representam os resultados reais da aplicação da tecnologia. O cálculo da receita digital adicional da Cisco abrange os casos de uso específicos do setor e entre setores.

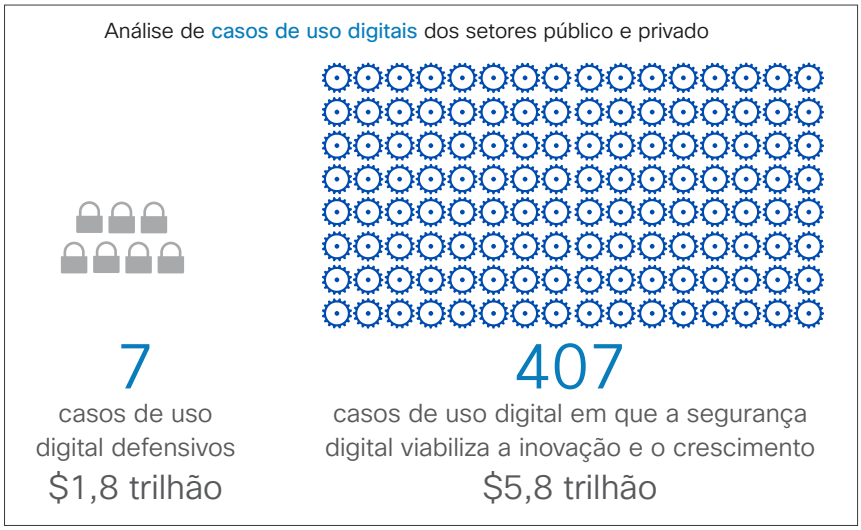

Figura 9
76% do valor da segurança digital está ligado à inovação e ao crescimento

Fonte:
Cisco, 2016

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 atrasem projetos digitais.

Manufatura

Considere o setor de produção, por exemplo. A Figura 10 mostra o impacto potencial dos riscos à segurança digital e dos atrasos de adoção relacionados aos sete casos de uso que gerarão a maior parte da receita digital adicional do setor para a próxima década. Todos esses casos de uso exigem que os fabricantes equipem seus ambientes operacionais com recursos digitais relacionados à Internet das Coisas, à análise e muito mais. Os fabricantes precisam confiar na segurança digital para fazer isso. Se não, perderão valor.

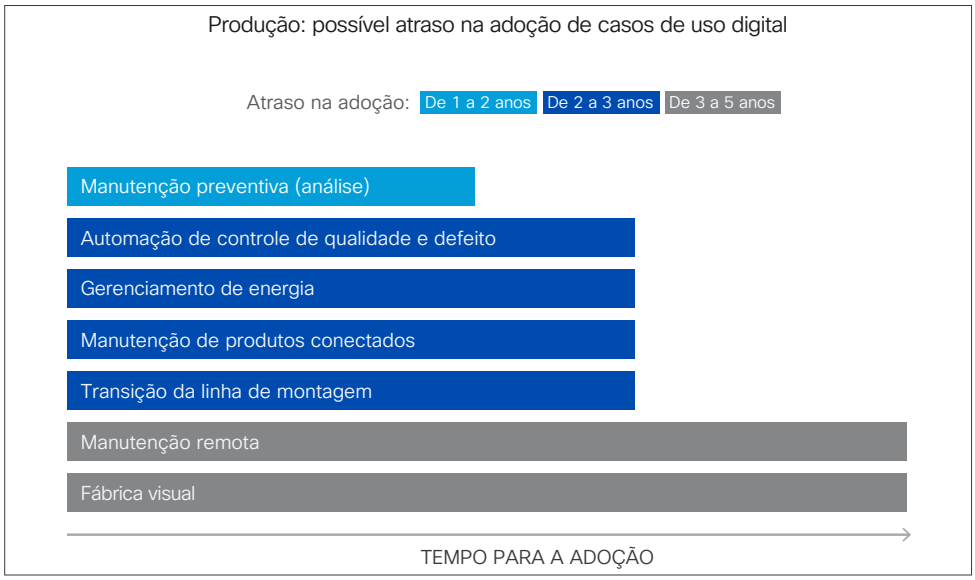

Figura 10
Quando as preocupações quanto à segurança digital atrasam iniciativas digitais, o potencial de crescimento e a posição de mercado sofrem

Fonte:
Cisco, 2016

A manutenção preventiva guiada por análise é um caso de uso digital essencial para os fabricantes implementarem e permanecerem competitivos. Os fabricantes, no entanto, não têm experiência para executar, e ainda mais criar, os algoritmos necessários para a manutenção preventiva. Como resultado, eles estão buscando esse recurso em seus parceiros (construtores de máquina, fornecedores de controles etc.). Isso pode ser no local ou fora das instalações em uma oferta distribuída em nuvem, um novo e assustador conceito para os fabricantes.

Considerando os níveis de risco de segurança digital percebidos associados a esse caso de uso, nós estimamos um atraso de um a dois anos até a adoção dos fabricantes. Por outro lado, se as preocupações quanto à segurança digital fizerem com que os fabricantes atrasem a implementação desse caso de uso específico, eles podem levar de um a dois anos para alcançar a concorrência que já o adotou. Ao atrasar a implementação, os fabricantes deixam de captar sua parte dos US$ 418 bilhões estimados de receita digital adicional que a manutenção preventiva (análise) distribuirá em 10 anos. Como resultado, eles diminuem suas capacidades de inovar e crescer.

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

A manutenção remota às vezes exige que as empresas abram suas redes para fornecedores externos. Esses fornecedores precisam acessar os dados e o maquinário da empresa para que possam identificar e resolver os problemas. Tradicionalmente, as máquinas não são conectadas às redes internas. Portanto, a ideia de fornecer acesso por Internet às máquinas representa uma mudança de paradigma para muitas operações empresariais das empresas. Os operadores, no entanto, reconhecem a demanda pela manutenção remota: ela pode minimizar o período de inatividade das máquinas ao permitir que as empresas resolvam os problemas da rede em vez de precisar enviar um especialista em consertos a um local específico.

Os sistemas centralizados de manutenção remota correm muitos riscos porque as violações podem causar um período de inatividade do sistema significativo. Por exemplo, hackers podem semear o caos nos sistemas de controle e automação de uma fábrica, o que representa um grande desafio à competitividade caso não seja detectado por um período prolongado. Portanto, a Cisco estima que pode levar até cinco anos para resolver e superar problemas de percepção associados à fraqueza da segurança digital para o caso de uso de manutenção remota. O resultado é uma posição de mercado enfraquecida e o crescimento prejudicado.

Os exemplos a seguir mostram como a segurança digital ajuda a gerar receita em outros setores:

Serviços financeiros: *pagamentos remotos*

As instituições financeiras dependem da confiança do cliente. Em particular, as empresas de pagamento móvel dependem totalmente da confiança do cliente. As empresas devem ser capazes de impedir violações à segurança, além de detectá-las e corrigi-las rapidamente, se ocorrerem. As violações à segurança dos pagamentos móveis podem resultar em período de inatividade, perda de receita, queda da reputação da empresa, custos de retribuição para corrigir os danos e perda de dados financeiros.

O que está em jogo? Com a implantação dos recursos adequados à segurança digital, as soluções de pagamento móvel gerarão até US$ 396 bilhões em vários setores de 2015 a 2024.

Varejo: *análise na loja física*

No setor de varejo, a análise na loja física significa a melhoria da eficiência da força de trabalho através de painéis, informações em tempo real, análises operacionais, ferramentas de gerenciamento da força de trabalho e análise de compra. A segurança digital é um viabilizador-chave: a qualidade e a privacidade são essenciais para garantir que a fonte de informações seja sólida e que as informações não tenham sido comprometidas.

Uma violação em potencial à segurança poderia resultar na perda de informações do cliente, assim como em dados infectados. Os clientes também podem perder a confiança em compartilhar dados pessoais com o revendedor, o que torna a análise menos informativa e difusa.

Com a base de segurança digital adequada, a análise na loja física tem o potencial de gerar US$ 285 bilhões em valor digital de 2015 a 2024.

Petróleo e gás: *controle de vazamento de petróleo*

Quando os sistemas digitais de controle de petróleo ficam inacessíveis, vazamentos podem não ser detectados por longos períodos. Muitos desses

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.

Com as práticas de segurança digital e conexões corretas, as empresas de petróleo e gás podem lançar luz sobre os recursos que estão "no escuro" (desconectados) e conquistar parte dos US$ 16 bilhões em valor digital que o controle de vazamento de petróleo gerará de 2015 a 2024.

A inovação, o valor e o crescimento dependem da capacidade das empresas de criar a segurança digital *na base* de suas estratégias digitais. Nosso estudo descobriu um novo segmento de mercado, *os digitalizadores de segurança*[2], que parecem estar fazendo isso de forma mais eficiente que todo mundo.

Digitalizadores de segurança lucram com a segurança digital e competem para ganhar

Para competir de forma mais eficiente com as inovações tecnológicas e melhorar a segurança digital, as empresas já estabelecidas devem buscar a *transformação* digital de negócios.

A verdadeira transformação digital significa uma *mudança organizacional* conduzida por tecnologias digitais e modelos digitais de negócios. Ela dá às empresas a oportunidade de reajustar a maneira como criam valor para os clientes e de mudar suas operações e cadeias de valor para serem mais ágeis. As empresas podem usar tecnologias digitais, principalmente Big Data, análise, IoT e computação em nuvem, para realizar os tipos de melhorias que proporcionam benefícios significativos aos inovadores.

A transformação digital também requer que as empresas incluam a segurança digital em seus planos desde o início.

Por exemplo, a empresa de pagamentos remotos Square inclui especialistas em segurança digital em todas as fases do design do produto. É essencial ter segurança digital avançada desde o início, em vez de acrescentá-la apenas ao final do desenvolvimento do produto. O mesmo ocorre quando a empresa cria novos processos internos. Nada é feito na Square sem que os especialistas em segurança digital colaborem de forma ativa com os executivos e os projetistas. Essencialmente, a transformação digital permite que as empresas criem novos processos digitais que fazem melhor o serviço, com a segurança digital presente desde o início.

A maioria dos executivos entrevistados entende que uma digitalização mais profunda de seus negócios trará a oportunidade de aprimorar a segurança digital e, ao mesmo tempo, redefinirá os processos comerciais, tornando-os mais ágeis. 69% disseram que as preocupações de segurança digital os tornaram mais dispostos a ir atrás de sua estratégia digital.

Novo segmento de mercado

"Digitalizadores de segurança" mostram o caminho

Mais de um quarto dos entrevistados pela Cisco estão buscando a digitalização com uma certa urgência, em parte porque sabem que a digitalização *pode melhorar a segurança digital*.

Esse segmento de mercado, o qual chamamos de "digitalizadores de segurança", está plenamente comprometido com o crescimento gerado através de modelos digitais de negócios e ofertas, com a segurança digital como base essencial. Como resultado, ele tende a gerenciar a segurança digital de forma mais proativa que nossos outros entrevistados. Eles também têm uma probabilidade muito maior de avaliar o impacto empresarial da segurança em diversas frentes.

Os digitalizadores de segurança têm maior confiança na segurança de três principais recursos digitais: Big Data/ análise, nuvem e Internet das Coisas. Essa confiança os torna mais dispostos a buscar ofertas digitais, acelerando assim a inovação e o tempo para a comercialização.

Ao competir com os digitalizadores de segurança, as empresas podem superar os desafios de segurança digital, inovar com mais confiança, além de melhorar sua posição competitiva.

"Se você aplicar a segurança digital a seus processos comerciais desde o início, a transformação digital poderá torná-lo mais seguro ."

—Presidente, Empresa de consultoria de segurança digital

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 de segurança mostram o caminho" na página anterior).

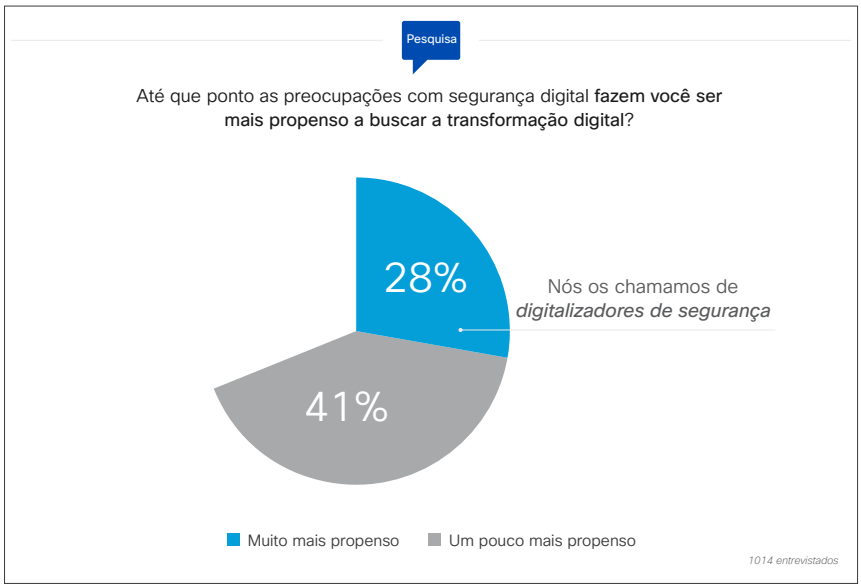

Figura 11
A demanda por segurança digital estimula algumas empresas a acelerar a transformação digital

Fonte:
Cisco, 2016

95% dos digitalizadores de segurança afirmaram que a tecnologia digital é muito importante para suas estratégias atuais de crescimento e 89% acreditam que ela será "muito mais importante" para o crescimento nos próximos dois anos, contra 58 e 35%, respectivamente, de outras empresas já estabelecidas.

Os digitalizadores de segurança estão muito mais envolvidos com os problemas de segurança digital que seus colegas: 66% concordam plenamente que a segurança digital é sua responsabilidade, contra 31% de seus colegas. Em parte, isso acontece porque o CEO, o conselho da empresa e outras partes interessadas importantes os responsabilizam pelos problemas de segurança digital, mesmo que eles não tenham funções técnicas ou de TI.

Como os digitalizadores de segurança contam muito com as ofertas e os modelos digitais de negócios para promover o crescimento, eles reconhecem que as preocupações com segurança digital podem deter a inovação e impedir o crescimento. Assim, estão tomando medidas agressivas para melhorar a segurança digital enquanto se transformam.

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 serviços. Somente 33% dos entrevistados que não são digitalizadores de segurança podem afirmar o mesmo.

Como tornar a segurança digital a base de suas estratégias digitais

Em uma era de inovações tecnológicas constantes e descobertas contínuas, a capacidade de usar a segurança digital como um meio para melhorar a agilidade estratégica e a excelência operacional será um diferencial fundamental para as empresas que desejam acelerar seu crescimento. Ao pensar como as práticas de segurança digital da empresa podem evoluir, considere as seguintes melhores práticas dos digitalizadores de segurança:

1. Transforme a segurança digital em uma vantagem de crescimento. Os digitalizadores de segurança assumem o controle da segurança digital: 80% estão " muito preocupados" com a segurança digital, em comparação com 36% dos outros; 83% devem assumir " um maior grau" de responsabilidade pela segurança digital, comparados aos 39% de todos os outros; e 66% concordam plenamente que " como líder, considero que a segurança digital é minha responsabilidade", em comparação aos 31% de todos os outros.

   Como resultado, a abordagem deles quanto à segurança digital é mais proativa. Por exemplo, 66% empregam recursos de segurança digital exclusivos, em comparação com 42% dos outros entrevistados; 65% disponibilizam financiamento para iniciativas de segurança digital, contra 41% de todos os outros; e 65% incorporam ativamente ferramentas e melhores práticas de segurança digital em suas operações, em comparação com 47% de todos os outros (veja a Figura 12).

Para ter acesso a mais informações, visite cs.co/cyberSD

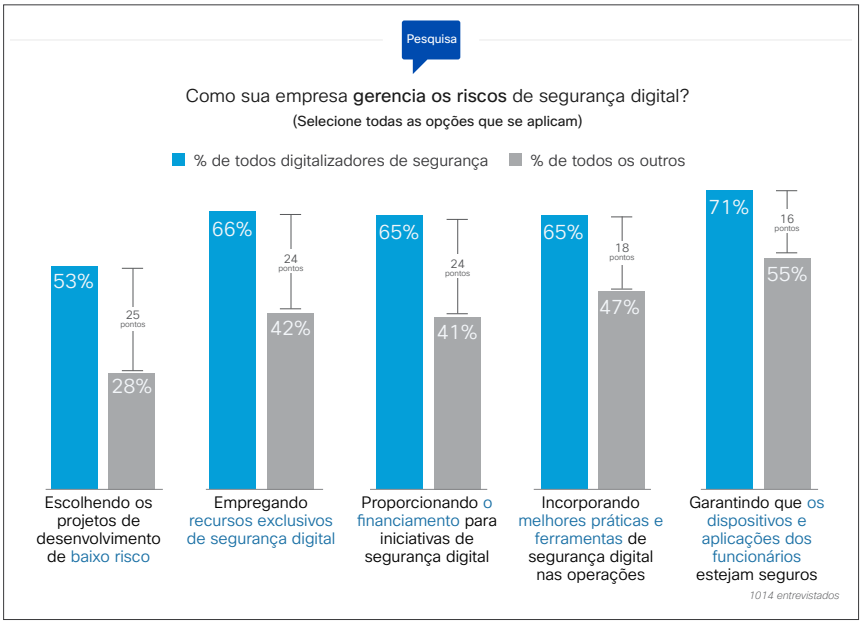

Figura 12
Os digitalizadores de segurança gerenciam a segurança digital de forma mais proativa

Fonte:
Cisco, 2016

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.

   Felizmente, há vários casos de uso digital com uma proporção de alto grau entre a oportunidade e o risco, começando pela própria segurança digital. Outros recursos digitais avançados que já oferecem valor comprovado incluem colaboração remota, funções do suporte do Centro de excelência, eficiência aperfeiçoada de recuperação de petróleo (petróleo e gás), transformação de serviços e vendas e recursos omnicanal (serviços financeiros) e análise de manutenção preventiva (produção).

   Como Mike Dahn, chefe de soluções de segurança de dados da Square, explicou, "Falamos muito sobre os riscos da segurança digital, mas, na verdade, uma das coisas das quais poderíamos estar falando é a viabilização da segurança.

   "Com a explosão de dispositivos, temos um risco em potencial mas também uma oportunidade em potencial", ele continuou. "Acho que o risco estará sempre presente. Devemos estar cientes dele, mas precisamos começar a pensar além do antigo modelo centralizado na defesa, e em um novo modelo de viabilização da segurança. Esse é realmente o centro da inovação; quando começamos a olhar os produtos e, em vez de dizer: "Como posso protegê-los?", dizemos: "Como esses produtos podem ser usados para nos proteger?"

   Os digitalizadores de segurança se sentem mais preparados que nossos outros entrevistados para lidar com os desafios de segurança digital em três principais áreas de tecnologia digital: análise, IoT e computação em nuvem. Como consequência, os digitalizadores de segurança se sentem muito mais confiantes para incorporar tecnologias digitais às ofertas e aos processos comerciais (Figura 13).

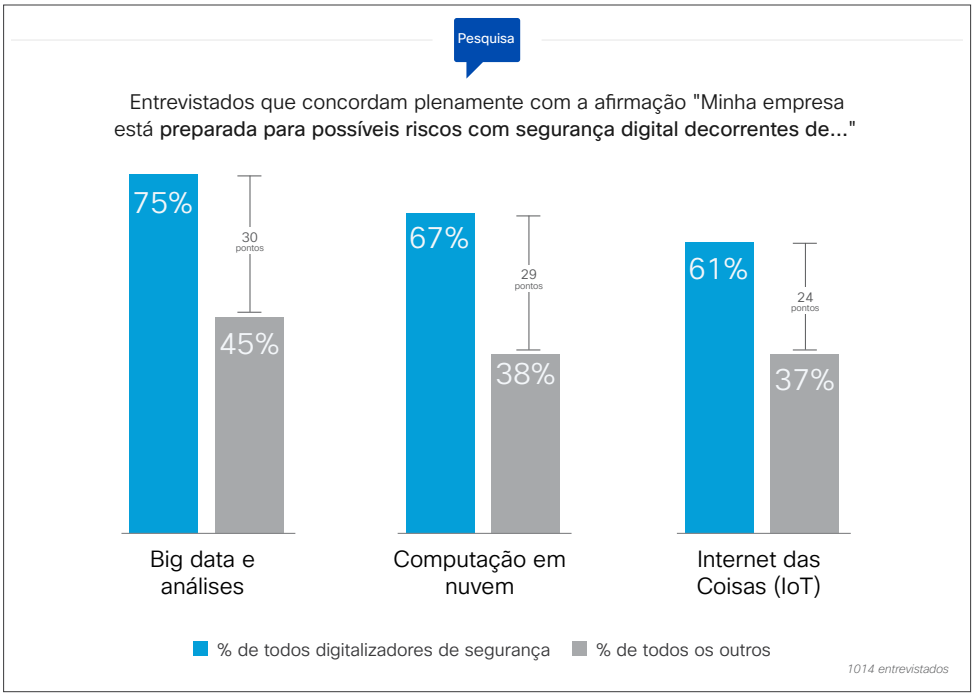

Figura 13
Os digitalizadores de segurança estão muito mais confiantes na segurança de suas estratégias digitais

Fonte:
Cisco, 2016

3. **Processos digitais recriados tomando por base a segurança digital.** A própria segurança digital é um mecanismo para a transformação empresarial digital. À medida que evoluem, as empresas devem identificar as tecnologias que não são seguras, assim como os processos comerciais que viabilizam, e substituí-las por outras que integram a segurança digital desde o princípio. Os digitalizadores de segurança já fazem isso muito melhor que empresas estabelecidas (veja a Figura 14). Como Adriaan Bouten, CEO e fundador da dPrism, destacou "Se você não lidar com a segurança digital desde o início, terá o dobro do trabalho para arrumá-la depois".

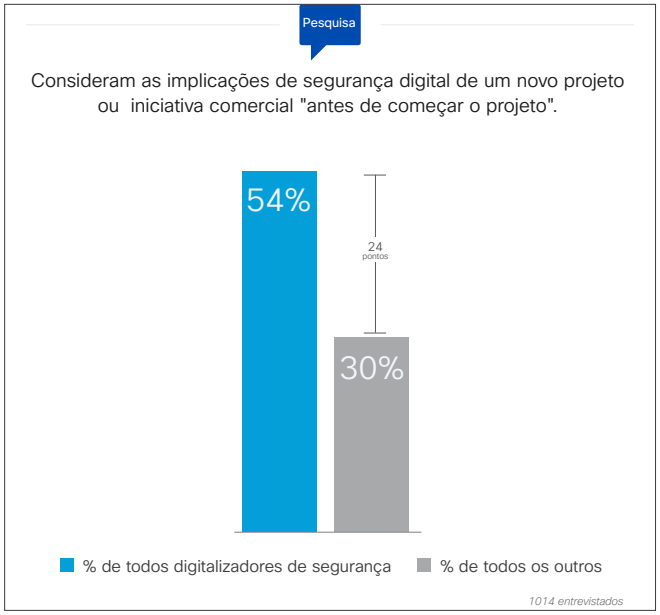

Figura 14
Os digitalizadores de segurança compreendem que a segurança digital é fundamental

Fonte:
Cisco, 2016

4. **Institua a segurança digital em todos os níveis da empresa.** As mesmas medidas proativas que ajudam as empresas a dominarem a segurança digital também podem impulsionar o desenvolvimento de produtos, a redução de riscos, a análise de ameaças e a resposta em outras partes da sua empresa. Isso estimula a inclusão de especialistas em segurança digital em várias funções diferentes da empresa e a adoção de uma mentalidade que preveja ameaças digitais para informar outros aspectos do planejamento estratégico e das operações da empresa.

   "A participação engloba desde o conselho até a equipe de limpeza e literalmente todo mundo entre eles", explicou o CFO Robert Simmons. "Não é mais domínio da TI. Acho que quanto mais cedo as empresas perceberem isso, melhor será a posição em que estarão para colocar esse tipo de programa em funcionamento na era digital atual."

Para ter acesso a mais informações, visite cs.co/cyberMD2

5. **Avalie o que você valoriza.** 75% dos digitalizadores de segurança têm processos bastante detalhados para determinar a eficiência das iniciativas de segurança digital em suas empresas funcionais, contra 21% de outras empresas. Esses processos avaliam uma variedade maior de informações, inclusive o impacto sobre os recursos digitais e o nível adequado de investimento em segurança digital (veja a Figura 15, na próxima página).

   Avaliar o impacto das proteções de segurança digital faz os executivos ficarem mais cientes das ameaças às operações e aos recursos estratégicos da empresa. Isso ajuda a estimular os outros investimentos a melhorarem suas proteções.

   65% dos digitalizadores de segurança afirmam que podem avaliar esses benefícios empresariais de forma muito eficiente. Apenas 30% das outras empresas afirmam o mesmo. Esse fato ajuda a explicar por que mais que o dobro dos digitalizadores de segurança espera aumentar os gastos de segurança digital no próximo ano (64% contra 31%).

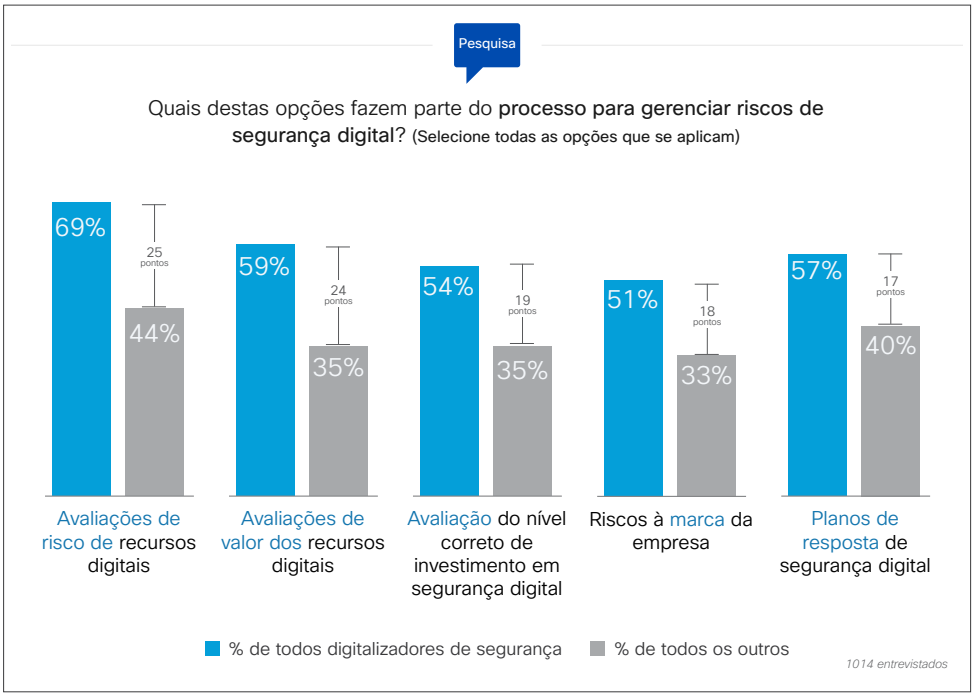

Figura 15
Os digitalizadores de segurança estão muito mais confiantes na segurança de suas estratégias digitais

Fonte:
Cisco, 2016

Para saber o quanto investir, as empresas precisam calcular o valor do que estão protegendo:

"Trata-se de compreender os riscos associados à proteção de informações que precisam ser protegidas, mas também de compreender o valor dessas informações para a empresa, caso elas caiam nas mãos erradas", explica Steve Durbin, diretor de gerenciamento do Information Security Forum. "Você começa com a seguinte perspectiva: 'Há uma grande possibilidade de que perderemos algumas informações em algum momento. Qual o valor dessas informações? Que o nível de dificuldade devo criar para as pessoas obterem acesso de fora da empresa? Depois, isso se traduzirá no foco dos recursos e nos gastos associados à proteção dessas informações."

A análise eficiente requer uma metodologia que determine os ganhos e as perdas associados à segurança digital. Muitas vezes, as empresas não conseguem estabelecer metas que considerem o desempenho desejado e as consequências imprevistas das mudanças criadas pelas novas estratégias empresariais digitais.[2]

Em uma era de inovações digitais, produtos e serviços digitais são o caminho necessário para o crescimento e até mesmo para a sobrevivência. Entretanto, devido às práticas de segurança digital abaixo do padrão, muitas empresas estão em uma posição difícil: não inovam com a velocidade e a confiança necessárias para ganhar, e, devido à pressão competitiva, fazem testes sem realizarem as práticas corretas de segurança digital. Enquanto isso, os inovadores mais ágeis, menos sobrecarregados com sistemas antigos de TI e com maior probabilidade de investir em segurança digital como um viabilizador de crescimento, avançam rapidamente.

Seguir os passos dos digitalizadores de segurança permite buscar inovações digitais de forma ousada e aumentar seu crescimento na era digital.

"Quando você lança uma nova iniciativa, a segurança digital está incluída no seu caso de negócios e no processo de gerenciamento do projeto. Você precisa tentar de tudo. Etapas precisarão ser cumpridas para a segurança de dados. Você terá pessoas de conformidade envolvidas. Todos precisam aprovar."

—Ex-vice-presidente de RH, banco da Fortune 100

1. Para entender como as empresas de médio e grande porte incorporam a segurança digital em seus negócios, realizamos uma pesquisa on-line com 1014 diretores, VPs e executivos da diretoria em outubro de 2015. Mais de um terço (38%) dos entrevistados tinha funções financeiras e influência financeira em segurança digital. Os outros 62% dos entrevistados são provenientes de uma combinação de domínios de linha de negócios. Eles tinham um conhecimento amplo ou moderado sobre a estratégia e as práticas de segurança digital em suas empresas, mas estavam nos departamentos de tecnologia da informação ou segurança de informações. Entrevistamos executivos dos seguintes países: Austrália, Brasil, Canadá, China, França, Alemanha, Índia, Japão, Reino Unido e Estados Unidos. Além disso, realizamos longas entrevistas qualitativas por telefone com 11 especialistas da rede de especialistas da GLG. Todos eram executivos seniores (na ativa ou aposentados) com ampla experiência em segurança digital em empresas estabelecidas, em funções no setor de finanças e de linha de negócios. Dentre eles, dois eram especialistas em consultoria sobre segurança digital.
2. A receita digital adicional baseia-se em dois componentes: 1) novas fontes de valor inteiramente provenientes de investimentos e inovações digitais e 2) mudança de valor entre empresas e setores com base na capacidade (ou na incapacidade) de aproveitar os recursos digitais (essencialmente, o valor que passa de "perdedores" para "vencedores").
3. Por "ofertas", queremos dizer os produtos e serviços que as empresas oferecem. Às vezes, essas ofertas não estão completamente em conformidade com a definição comum de um produto ou serviço e modelos empresariais tradicionais. Por exemplo, os inovadores digitais estão apresentando ofertas com modelos de consumo exclusivos, através de modelos empresariais nos quais a própria oferta é gratuita, e a receita é gerada por atividades correlatas. Para ver uma análise detalhada das fontes de valor que as inovações digitais estão criando e os modelos empresariais usados para criá-las, consulte New Paths to Customer Value: Disruptive Business Models in the Digital Vortex, Centro Global para Transformação Empresarial Digital (Centro DBT), uma iniciativa da IMD e da Cisco, novembro de 2015.
4. Em contraste com as empresas start-up e outros inovadores digitais ágeis, as empresas já estabelecidas ou concorrentes têm um grande número de funcionários, tendem a ter cadeias de valor tradicionais e a possuir mais de seus próprios recursos produtivos que as empresas start-up. A pesquisa da Cisco concentrou-se exclusivamente em empresas já estabelecidas: todas tinham pelo menos 500 funcionários. 83% eram empresas com pelo menos 1.000 funcionários, inclusive 19% com pelo menos 10.000 funcionários.
5. Por digital, queremos dizer a convergência de várias inovações tecnológicas viabilizadas por conectividade de alta velocidade onipresente. Essas inovações tecnológicas incluem Big Data, análise, computação em nuvem, Internet das Coisas (IoT), mobilidade, mídias sociais e aprendizagem automatizada. Para definir "digital" e outros termos relacionados, usamos Defining the Digital Vortex, desenvolvido pelo Centro DBT.
6. Definimos "digitalização" como gerar ou converter informações que podem ser utilizadas e compartilhadas por tecnologias digitais. As informações digitalizadas são a base dos processos comerciais e modelos empresariais digitais. Consulte "Defining the Digital Vortex", Centro DBT, dezembro de 2015.
7. The Digital Vortex: How Digital Disruption Is Redefining Industries, Centro Global para Transformação Empresarial Digital, junho de 2015
8. Disruptor and Disrupted: Strategy in the Digital Vortex, Centro Global para Transformação Empresarial Digital, junho de 2015
9. Em 2014, mais de um bilhão de dados foram comprometidos, acima dos 54% anuais, boa parte devido a violações no varejo. Na primeira metade de 2015, o número de violações aumentou em 10% em relação a 2014H1, mas o número total de registros comprometidos ficou abaixo de 41% para 246 milhões de registros. Gemalto, setembro de 2015; ZDNet, janeiro de 2016.
10. "Data and Dollars: The Role of the CFO in Cybersecurity", Steve Durbin, diretor de gerenciamento, Information Security Forum, Connected Futures.
11. Fast IT: Acelerando a inovação na Era da Internet de Todas as Coisas, Cisco, 2014.
12. ""2015 Cost of Data Breach Study: Global Analysis", Ponemon Institute, maio de 2015.
13. "Businesses Braced for Bout of Regulation on Cyber Security", Financial Times, e "New York Bank Regulator Details Cybersecurity Regulations", The Wall Street Journal, novembro de 2015.
14. "Digital Vortex: How Digital Disruption Is Redefining Industries", Centro Global para Transformação Empresarial Digital, junho de 2015.
15. Em outro estudo, quando perguntado "O que impede uma empresa de ser inovadora?" 28% dos entrevistados responderam "A crença de que a inovação aumenta o risco à segurança". Consulte "Risk & Innovation in Cybersecurity Investments", Instituto Ponemon de LLC e Lockheed Martin, abril de 2015.
16. Essa descoberta se alinha com as feitas em um estudo recente conduzido pela Ping Identity ("Secure Access for the Digital Enterprise", Ping Identity, 2015), que revelou que a segurança é o principal desafio da adoção de tecnologias digitais para 51% das empresas, e que 78% das empresas atrasaram sua mudança para a nuvem devido a preocupações com a segurança.
17. "" Seven Ways CEOs Can Apply Digital Business for Competitive Advantage", Hung LeHong, Gartner, junho de 2015.
18. De acordo com a Gartner, os gastos mundiais do setor de TI diminuíram em 2015.
19. Quando solicitados a identificar os maiores desafios de gerenciamento e de política de segurança digital, 32% dos entrevistados da pesquisa da Cisco selecionaram "Incapacidade da política de segurança digital acompanhar o ritmo das mudanças empresariais"; 27% selecionaram "Carência das métricas corretas para determinar a eficiência da segurança digital"; 26% selecionaram "Investimento insuficiente em segurança digital"; e 24% selecionaram "aplicação ineficiente de políticas de segurança digital". O aumento do investimento geral em segurança digital não é um remédio para todos os males: para maximizar o valor, as empresas devem priorizar investimentos em iniciativas que tenham definido as métricas de sucesso e que sejam gerenciadas de forma eficaz.

Confirmações

Os autores são muito gratos pelas contribuições das seguintes pessoas no desenvolvimento deste artigo: Debbie Abbott, Caroline Ahlquist, Sara Aiello, Kevin Bandy, Ruba Borno, Kristine Briggs, John Choi, Lynne Cox, David Goeckeler, Dan Gould, Gene Hall, Amy Henderson, Lisa Lahde, Rob Lothman, James Macaulay, Melissa Mines, James Mobley, Bryan Palma, Robert Pepper, Caroline Robertson, John Stewart, Ann Swenson, Greg Thomas, Virgil Vidal, Michael Zielenziger e Elisabeth Zornes

20. Os digitalizadores de segurança são um novo segmento de mercado identificado pela Cisco como parte deste estudo de pesquisa. A segmentação do mercado envolve a divisão de um mercado-alvo amplo em subconjuntos de empresas que têm, ou que parecem ter interesses, comportamentos e prioridades em comum.
21. "Using Risk-Adjusted Value Management to Close the Strategy Gap and Gain Competitive Advantage", Michael Smith e Paul E. Proctor, Gartner, dezembro de 2015.

C45-BCI0416-00 04/16