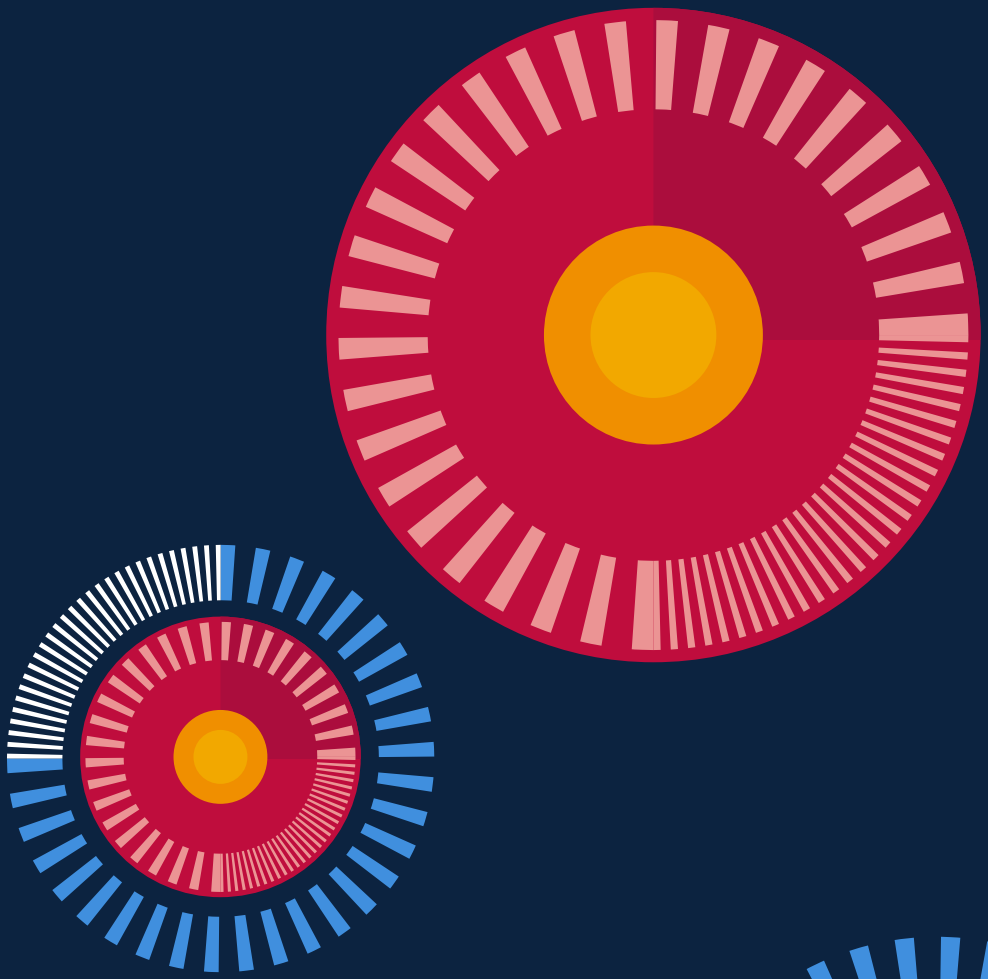
CYBER VIEW

Identificando oportunidades no mercado brasileiro



Estudo desenvolvido pela JLT Seguros

Janeiro 2018

Vivemos a era da hiperconectividade, em que toda e qualquer indústria possui exposição ao risco diante da utilização de tecnologia em suas operações e que podem resultar na paralisação de suas atividades e perdas comerciais. No entanto, muitas organizações não estão abordando o problema estrategicamente para criar respostas efetivas e cruzadas a esse risco. A maioria das empresas não entende a magnitude da ameaça que o ciberataque oferece e não estão calculando o custo possível do mesmo.

Em maio de 2017, o mundo foi surpreendido com um ataque cibernético de escala global, o WannaCry, ransomware lançado pela ShadowBrokers que causou danos a mais de 150 países em empresas de todos os setores incluindo hospitais, bancos, indústrias e telecomunicações.

Os impactos de um ataque estão muito além de uma perda financeira. Uma cadeia de perdas precisa ser considerada desde a receita perdida pela interrupção de serviços prestados, custos de consultoria de investigação forense, possíveis danos causados a terceiros que envolvem custos jurídicos e indenizações, impacto sobre a imagem e reputação da empresa e até mesmo a queda no valor da ação caso a empresa possua capital aberto. No entanto, ainda há muito trabalho a ser desenvolvido a fim de que esses riscos tão complexos sejam compreendidos.

O risco, até então, não era visto como prioridade por diversos gerentes de risco e pelo corpo diretivo das empresas. Era um problema do departamento de TI e passou a ser reconhecido como um fator de grande preocupação.

Foi pensando em tudo isso que a JLT apresenta o Cyber View, um estudo que mostra uma visão geral dos nossos clientes e parceiros em relação aos riscos cibernéticos. Esperamos que esta pesquisa seja um ponto de partida para as organizações redefinirem o cyber como um risco comercial estratégico e começarem a abordar os riscos cibernéticos de forma diferente, a fim de maximizar as oportunidades para mitigar essa crescente ameaça.

Marta Helena Schuh
Gerente de Riscos Cibernéticos

QUAL É A FRONTEIRA DO SEU NEGÓCIO?

COMO INTERNET NÃO TEM FRONTEIRAS, NEGÓCIOS DIGITAIS JÁ NASCEM GLOBAIS. OS RISCOS E AS RESPONSABILIDADES DEVEM LEVAR EM CONSIDERAÇÃO OS LOCAIS DE ATUAÇÃO DE SUA EMPRESA, ASSIM COMO AS INFORMAÇÕES DE CIDADÃOS E EMPRESAS DE OUTROS PAÍSES PARA AVALIAR SEU LIMITE DE RESPONSABILIDADE.

RISCO CIBERNÉTICO, UM RISCO DO PRESENTE

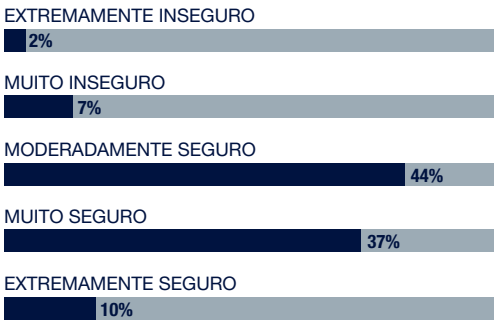
Em um mundo hiperconectado, a digitalização continua a criar maior eficiência em nossas vidas e na operação dos negócios. Sistemas coletam, analisam e compartilham dados financeiros, operacionais e de stakeholders.

As empresas precisam considerar os riscos comerciais, contratuais e reputacionais derivados da não-estruturação de uma política de governança e mitigação de riscos cibernéticos, o que pode implicar no funcionamento de suas operações e competitividade.

As empresas precisam avançar em controles de cibersegurança que vão além de suas arquiteturas de tecnologia integrando todas as áreas e delineando processos para proteção e mitigação de seus riscos. Os ataques cibernéticos têm muitos canais para penetrar uma organização – de fornecedores a clientes e usuários internos – e precisam explorar os pontos de falha para causar um dano em todos os níveis.

FIGURA 1

QUÃO SEGURO VOCÊ SENTE QUE OS DADOS DA SUA EMPRESA ESTÃO PROTEGIDOS?



10%

é o percentual de empresas que sentem que seus dados estão totalmente protegidos com seus sistemas atuais de proteção

COMO AS EMPRESAS SE PROTEGEM DE UM ATAQUE?

A pesquisa demonstra que o envolvimento de todas as partes interessadas em iniciativas de segurança cibernética é alto: 75% empresas se protegem de ameaças digitais. No entanto, ela continua sendo, em grande parte, vista como algo de responsabilidade da área de tecnologia da informação (TI) e pelos sistemas de proteção (figura 3).

De acordo com um dos entrevistados, o motivo para isso é que existe uma falta de compreensão dos riscos pelas áreas de gestão da empresa. Geralmente, quando se fala em linguagem de TI, os termos utilizados são distantes da linguagem de negócios do dia a dia e isso faz com que o corpo diretivo permaneça ainda mais distante das medidas de contingência.

Entretanto, é importante notar que o departamento de TI trabalha para reduzir de forma diligente e proativa o risco de uma violação ou ataque com firewalls, software e antivírus, e, também, que uma política de proteção cibernética é de responsabilidade de toda empresa, começando pelo board executivo.

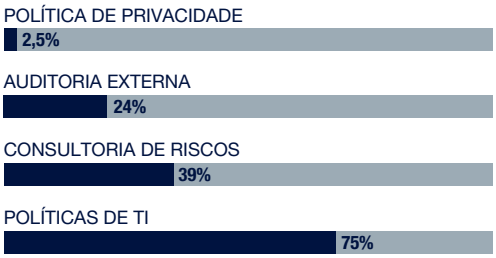
As empresas devem ver a gestão dos riscos cibernéticos da mesma maneira que veem qualquer outro, desde o escopo e mitigação até a determinar recursos para prevenção.

FIGURA 2

SUA EMPRESA SE PROTEGE DE ATAQUES CIBERNÉTICOS?

FIGURA 3

QUAL DOS SEGUINTES MÉTODOS É UTILIZADO POR SUA EMPRESA PARA AVALIAR A SEGURANÇA CIBERNÉTICA?



SEGURANÇA DA INFORMAÇÃO: COMO SUA EMPRESA PODE SE PREPARAR

RH E FINANCEIRO

Definição de impactos ao negócio, clientes, perdas financeiras, cultura e capacidades

GOVERNANÇA CORPORATIVA

Controles *Top Down* de segurança cibernética

SEGURANÇA DA INFORMAÇÃO

Definição de processos em conformidade com os padrões da indústria, alinhamento estratégico de segurança e políticas cibernéticas

GOVERNANÇA CORPORATIVA

Políticas de tecnologia implantadas juntamente com sistemas a fim de suportar processos de segurança

COMPLIANCE

Auditorias regulares para garantir conformidade e desempenho com processos definidos, políticas em todas as linhas de defesa

SEGURANÇA DA INFORMAÇÃO

Controles de acesso, vigilância e gerenciamento de crises para fornecer uma base segura aos processos e infraestrutura de TI

PERCEPÇÃO E PREOCUPAÇÃO DE UM ATAQUE CYBER

Cerca de 85% das organizações pesquisadas veem os impactos de um ataque afetando as operações da empresa como um todo (figura 5), isso deve-se ao fato das empresas usarem cada vez mais tecnologia em suas operações. Cada organização é única em termos de impacto, mas em todas as indústrias existem áreas críticas que dependem do bom funcionamento dos sistemas. O caso recente de WannaCry mostrou que as indústrias, sejam elas automotivas, de telecomunicações, de transportes ou um serviço público, enfrentam ameaças similares. Ao mesmo tempo que os impactos podem afetar as empresas de forma diferente, todas precisam estar preparadas e implementar um processo rigoroso para identificar sua exposição e alocar seus recursos da maneira mais eficiente e otimizada.

A maior preocupação dos entrevistados é a quebra de privacidade de informação. Isso porque os impactos desencadeiam perdas que contemplam diversas variáveis. Uma proteção de dados questionável impacta diretamente em sua reputação, que por sua vez traz consequências sob sua receita por perda de vendas, possíveis acionamentos jurídicos (pela quebra de confidencialidade, que requer indenizações morais), além de possíveis multas e impactos diante das regulações, como a que entra em vigor em maio de 2018, a General Data Protection Regulation (GDPR).

35%

das empresas desconhecem ou não possuem um plano de respostas para incidentes cibernéticos

Nosso estudo revela um fator preocupante: 35% das empresas não sabem ou não possuem um plano de respostas a incidentes cibernéticos. Pense que a segurança cibernética se assemelha com a segurança patrimonial, ou seja, uma vez que você saiba o que e onde os eventuais perigos estão, é possível, proativamente, mitigar as perdas e os danos. Por exemplo, você pode contratar um especialista para instalar extintores de incêndio, formular um plano de contingência, etc.

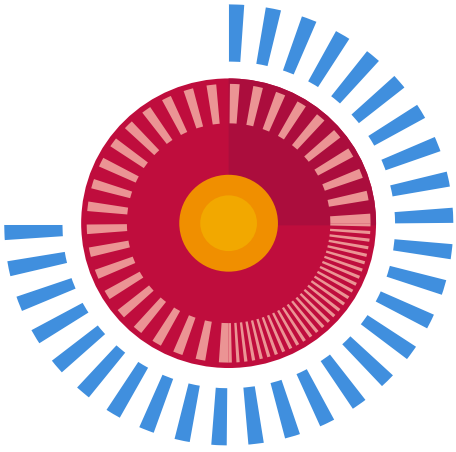


FIGURA 4

SUA ORGANIZAÇÃO POSSUI UM PLANO DE RESPOSTA QUE INCLUEM AS INCIDÊNCIAS DE CUSTOS FINANCEIROS NA EVENTUALIDADE DE UM ATAQUE CIBERNÉTICO?

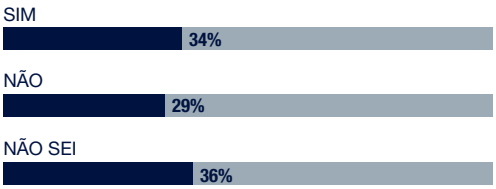


FIGURA 5

COMO SUA EMPRESA AVALIA OS PREJUÍZOS CAUSADOS POR UM ATAQUE CIBERNÉTICO?

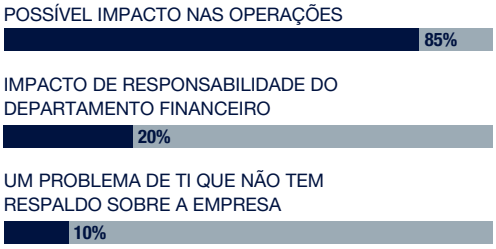
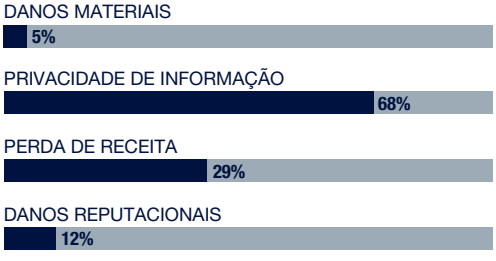


FIGURA 6

QUAL É O MAIOR RECEIO DA SUA EMPRESA EM RELAÇÃO A UM ATAQUE VIRTUAL?



O QUE É GDPR?

A GDPR (General Data Protection Regulation – Regulamentação Geral de Proteção de Dados) é um regulamento que todas as empresas que trabalham com dados de cidadãos da União Europeia devem seguir.

5 principais medidas para garantir a conformidade:

- Designar responsáveis pela proteção de dados (DPOs)
- Estabelecer um programa de segurança cibernética
- Seguir padrões de segurança de processamento de dados
- Responsabilidade documentada
- Entender o consentimento

Organizações que violam a GDPR podem ser multadas em até 4% do seu rendimento global anual ou €20 milhões (o que for maior).

A empresa pode ser multada em 2% por não ter seus registros em ordem (artigo 28), não notificar a autoridade controladora e o objeto dos dados sobre uma violação ou não realizar uma avaliação do impacto.

É importante observar que essas regras se aplicam tanto a controladores quanto a processadores - significando que as 'nuvens' não estarão isentas do cumprimento da GDPR.

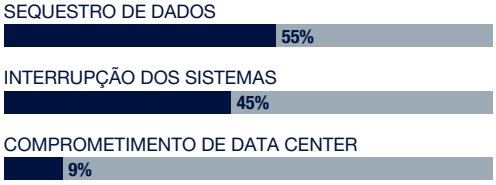
IMPACTOS DE UM ATAQUE

O ambiente cibernético é um espaço em rápida evolução que engloba operações comerciais de indústrias e organizações. Cerca de 1/4 dos entrevistados relataram que suas empresas já foram vítimas de um ataque cibernético e apontaram como consequência principal (figura 7) o sequestro de dados (55%) o que afeta diretamente a reputação da marca. Em seguida vem a interrupção dos sistemas (45%), o que afeta diretamente a operação. Ambos impactos apresentam perdas entre R$ 25 mil e R$ 500 mil.

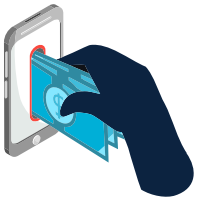
Como consequências de tais incidentes, empresas podem, além de deixar de prestar serviços, ter impactos em perdas de vendas, paralização de produção, possíveis clientes perdidos, entre outras. As interrupções ou capacidades reduzidas podem ainda que breves, gerar efeitos contínuos mesmo após a restauração de serviços. A reputação de uma empresa ainda pode sofrer impactos diante da à perda de receita.

FIGURA 7

QUAIS PERDAS SUA EMPRESA SOFREU EM FUNÇÃO DO ATAQUE?



Q19. Sem empresa já sofreu algum ataque cibernético?
Q21. Qual foi o tamanho do prejuízo?



até R$ 500 mil

os entrevistados apontam como consequência principal de um ataque, o sequestro de dados, o que afeta diretamente a reputação da marca, além de perdas financeiras

A PROTEÇÃO DE DADOS NO BRASIL

No Brasil, atualmente não há uma lei de proteção de dados, no entanto há, pelo menos, três projetos de lei que tramitam no Congresso.

2014 – Lei 12.965 Marco Civil da Internet: Lei que orienta os direitos e deveres dos usuários, provedores de serviços e conteúdos e demais envolvidos com o uso da internet no Brasil.

Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

a) Neutralidade da rede (art. 9, § 1º); b) Privacidade na rede (art. 10, § 4º; art. 11, § 3º e art. 11, § 4º); c) Guarda de registros (art. 13 e art. 15).

PROJETOS DE LEI

PL 5276/2016 (Câmara dos Deputados)
Dispõe sobre a responsabilidade e ressarcimento de danos:

Art.42. – Todo aquele que em razão do exercício de atividade de tratamento de dados causar outrem dano patrimonial, moral, individual ou coletivo é obrigado a repará-lo.

Art.47.- O responsável deverá comunicar ao órgão competente a ocorrência de qualquer incidente que possa acarretar risco ou prejuízo aos titulares.

PL 4060/2012 (Câmara dos Deputados)
Projeto de Lei de Proteção de Dados.

PL 181/2014 (Senado)
Projeto de Lei de Proteção de Dados.

O objetivo da regulação:

definir normas para coleta, armazenamento, utilização e transferência de dados pessoais.

Quem será afetado?

Usuários e/ou consumidores de produtos e serviços online e offline;
Todo o setor privado, nas mais diversas áreas (medicina e saúde, agricultura de precisão, setor financeiro, empresas que prestam serviços para cidades inteligentes, plataformas online, pesquisas científicas, serviços em geral) e independente do tamanho, afetando grandes empresas, startups e fundos de investimento.

SEGURO CYBER E A PERCEPÇÃO DE NOSSOS CLIENTES

Apesar do seguro cibernético ter sido lançado em 2012 no Brasil, 53% dos entrevistados desconheciam essa solução. Isso talvez se deva à pouca divulgação feita antes dos ataques de maio de 2017.

Apenas 13% dos respondentes contratam o seguro cyber, porque, até então, poucas empresas empregavam estratégias de gerenciamento de risco devido à falta de compreensão, disponibilidade ou talvez à crença de que 'nunca acontecerá com eles'.

Fizemos uma abordagem mais detalhada a um cliente que definiu como de extrema importância obter a apólice de seguro, porém, que ainda não possua o seguro. O motivo disso é que, até pouco tempo atrás, ele não havia entendido os benefícios em obter a solução e acreditava que, de certa forma, a mesma conflitava com os sistemas de proteção, tornando-a um investimento pouco efetivo. "Após participar de um seminário e uma reunião onde tivemos um entendimento de como este seguro vem proteger a nossa operação, colocamos no orçamento para 2018".

Isso ressalta a importância de que o mercado segurador eduque seus clientes e deixe claro como o produto faz sentido em suas operações. Por sua vez, os gerentes de risco devem estar posicionados para fornecer ao conselho uma visão abrangente deste tipo de risco e seus impactos financeiros, propondo medidas de segurança em conjunto com a área de TI.

Com os especialistas ressaltando que os ataques cibernéticos só aumentarão e que as empresas devem se emprenhar mais para se proteger gestores de riscos estão perceptíveis a necessidade de contratação do seguro. 93.3% consideram a compra de uma apólice em um futuro próximo.

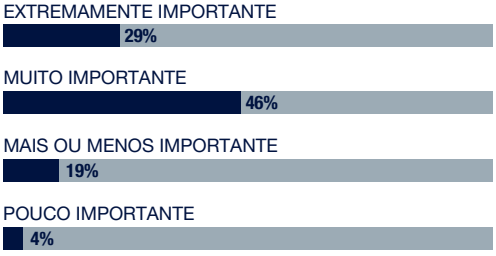
Comprar o seguro cibernético pode ser um exercício de auditoria de processos para algumas empresas. Identificar suas exposições e o impacto comercial pode demonstrar o valor do seguro cibernético de maneira positiva. Lembrando que uma apólice de riscos cibernéticos não está destinada a substituir a função de prevenir incidentes, mas sim a cobrir os custos incorridos pela violação de dados.

FIGURA 8

QUANDO VOCÊ PENSA NESTE NOVO SERVIÇO, VOCÊ PENSA NELE COMO SENDO ALGO QUE AS EMPRESAS NECESSITAM?

FIGURA 9

QUAL É A IMPORTÂNCIA DO INVESTIMENTO PARA O SEU NEGÓCIO AO ESCOLHER ESTE TIPO DE SERVIÇO?



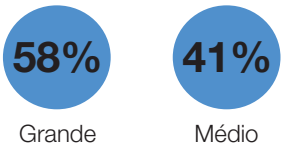
Q12 Você conhece o Seguro Cibernético?
Q13 Sua empresa possui esse tipo de seguro?
Q14 Quando você pensa neste novo serviço, você pensa nele como sendo algo que as empresas necessitam?
Q22 A sua empresa olha para o Seguro Cibernético como uma solução para 2018?

UMA PROTEÇÃO DE DADOS QUESTIONÁVEL IMPACTA DIRETAMENTE NA REPUTAÇÃO DA EMPRESA, QUE POR SUA VEZ TRAZ CONSEQUÊNCIAS NA RECEITA DEVIDO A PERDA DE VENDAS, POSSÍVEIS ACIONAMENTOS JUDICIAIS, ETC.

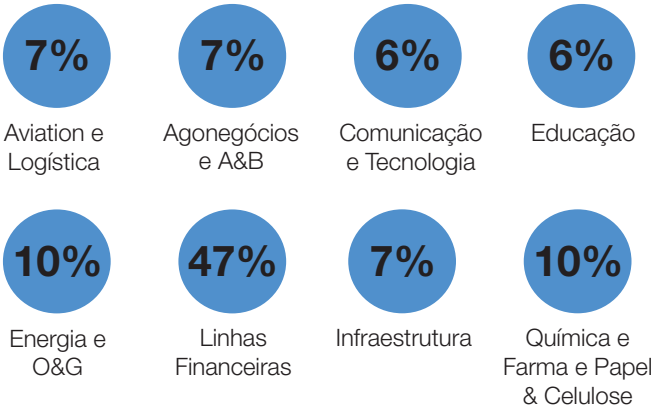
METODOLOGIA E PERFIL DOS PARTICIPANTES

Um total de 60 entrevistados completaram a pesquisa: 37 são de empresas parceiras; 23 são clientes da JLT Brasil.

PORTE



SEGMENTO



CARGO

Referências

1. The Economic Impacts of Cyber Crime and Cyber Espionage report by McAfee
2. Beneath the surface of a cyberattack - Deloitte
3. The Impact of the General Data Protection Regulation on Responses to Data Breaches Involving EU Personal Data by Michael G. Morgan Romain Perray
4. JLT Cyber Decoder

O QUE MAIS VOCÊ PRECISA SABER?

GLOSSÁRIO CYBER

Quais são os riscos cibernéticos?

O risco cibernético emana de fontes online e offline. Por exemplo, um hacker ganhando acesso físico para fazer upload de malware em um sistema de emissão de bilhetes online, um dispositivo móvel perdido contendo informações confidenciais ou um arquivo em nuvem roubado. Embora a dependência da comunicação eletrônica e dos processos direcionados pela tecnologia conectada no mundo de hoje exponha as empresas ao risco cibernético, os elementos de privacidade de dados do risco são prevalentes offline.

Os incidentes cibernéticos podem ser perpetrados por vários atores com diversas motivações. De um modo geral, eles podem caber em quatro categorias:

O mais prevalente e temido é o ator malicioso externo, que poderia ser um criminoso, um grupo politicamente motivado de hacketivistas que procuram causar perturbações ou terroristas que procuram usar a tecnologia para causar danos físicos.

Atores maliciosos também existem dentro das empresas e podem ser indivíduos desencantados com conhecimento ou acesso altamente técnico, ou simplesmente aliciar um funcionário de empresas que são abordados por um criminoso que os induz a roubar dados, introduzir código malicioso ou simplesmente fornecer acesso físico a empresa.

Os funcionários também podem causam incidentes cibernéticos por erro humano. Por exemplo, clicando no link em um e-mail de phishing, esquecendo um laptop no aeroporto, conectando-se a redes wifi desacreditadas ou não verificando as credenciais de segurança de um indivíduo em um site de trabalho.

Atualmente, diversas empresas dependem de uma vasta rede de fornecedores e empresas terceirizados, e ainda que apliquem rigorosas normas de segurança e privacidade de dados em fornecedores de alto risco percebidos, como os processadores de dados, mas não consideram que fornecedores de baixo risco podem ser um fator de risco cibernético.

O que é o seguro cibernético?

O seguro de responsabilidade civil é projetado para mitigar os custos de primeira (empresa) e terceira partes (clientes, funcionários) que você pode estar sujeito em um ataque cibernético. Os custos de primeira parte são aqueles que sua empresa pode incorrer diretamente como resultado de um incidente cibernético, enquanto os custos de terceiros são aqueles que você pode ser obrigado a pagar a outros.

Por que as empresas precisam de seguro cibernético?

Cada vez mais as diferentes indústrias tornaram-se dependentes da tecnologia e de dados. Se por um lado isso representa uma oportunidade para melhorar a eficiência e a rentabilidade, por outro, traz consigo uma série de riscos emergentes. As exposições cibernéticas são reais, ainda que não tangíveis.

Os incidentes cibernéticos podem afetar qualquer empresa de várias maneiras. Os dados são, muitas vezes, o alvo de um ataque cibernético, quer se trate de informações pessoalmente identificáveis de funcionários ou clientes; informações confidenciais de outras empresas compartilhadas sob um acordo de confidencialidade; ou os dados confidenciais da empresa, como segredos comerciais, protocolos de negócios ou lista de clientes, ou resultados financeiros.

O conteúdo de mídia publicado no ciberespaço também entra em escopo de risco e pode resultar em alegações de difamação ou violação de propriedade intelectual. O uso das mídias sociais pelas empresas pode incidir em danos de reputação e problemas de segurança.

Hoje, o tema tecnologia (tecnologia da informação e tecnologia operacional) não estar segregado das demais operações diárias da maioria das empresas. Uma empresa vítima de um ataque cibernético pode ter interrupção de negócios resultando em uma perda de receita e/ou consequências de responsabilidade.

Equívocos comuns cometidos pelas empresas:

"Não somos alvo de hackers"

A tecnologia e a segurança cibernética estão se tornando cada vez mais sofisticadas, mas o erro humano continua a ser a principal causa de incidentes cibernéticos. Se um empregado deixa acidentalmente uma senha aberta ou clicar acidentalmente em um website/email com malware a sua empresa pode sofrer consequências de um ataque ciber.

"Nós não vendemos produtos ou serviços online, portanto não estamos expostos ao risco cibernético"

Se sua empresa captura ou armazena dados de clientes e fornecedores, você possui risco cibernético. As apólices de Cyber são projetadas para o risco de utilizar tecnologia, computadores e a conectividade com a internet, enquanto conduzem negócios diários que incluem a captura, armazenamento e uso de dados todos os dias.

A indústria 4.0 em que sensores controlam as linhas de produção, sistemas de gerenciamento logístico, com rastreamento de contêineres, caminhões, sistemas de armazenamento e outras máquinas estão cada vez mais inteligentes e interconectados resultando em um risco operacional. Sistemas de controle industrial (ICS) são um dos objetivos principais para ataques cibernéticos. As arquiteturas de automação, como HMIs (Human Machine Interfaces) e SCADA (Supervisory Control And Data Acquisition), e os riscos da segurança incidentes são cada vez maiores e as consequências tem uma grande abrangência - ativos, ambientes, vida humana e a reputação.

"Usamos fornecedores para todos os nossos serviços de TI"

De acordo com os regulamentos de dados, a empresa que coleta dados e registros de clientes é responsável se ocorrer uma violação de dados. A responsabilidade legal não pode ser transferida por contrato; portanto, se um dispositivo de ponto de venda estiver comprometido, a obrigação de notificar as partes afetadas cairá no proprietário da empresa e não no fornecedor que processa ou armazena informações de pagamento. Isso se cabe também a empresas que

utilizam sistemas de nuvem, há uma série percepções em torno da nuvem e da responsabilidade de dados. Muitas empresas assumem que transferiram seus riscos quando seus dados estão em mãos de terceiros. A realidade é que na maioria dos casos, há muito pouca proteção em termos de responsabilidade com os provedores da nuvem.

Os contratos de indenização normalmente limitam o recurso ao valor do contrato. No entanto, uma violação média de dados envolvendo registros financeiros pessoais poderia custar uma empresa de milhões.

"Temos uma segurança de primeira linha no lugar"

Não existe segurança perfeita. As agências do FBI, NSA, empresas como Google, Microsoft foram afetadas por ataques internos e externos, provando que nenhuma solução de segurança é impenetrável.

"Nossa apólice de responsabilidade civil geral/property cobrirá a perda"

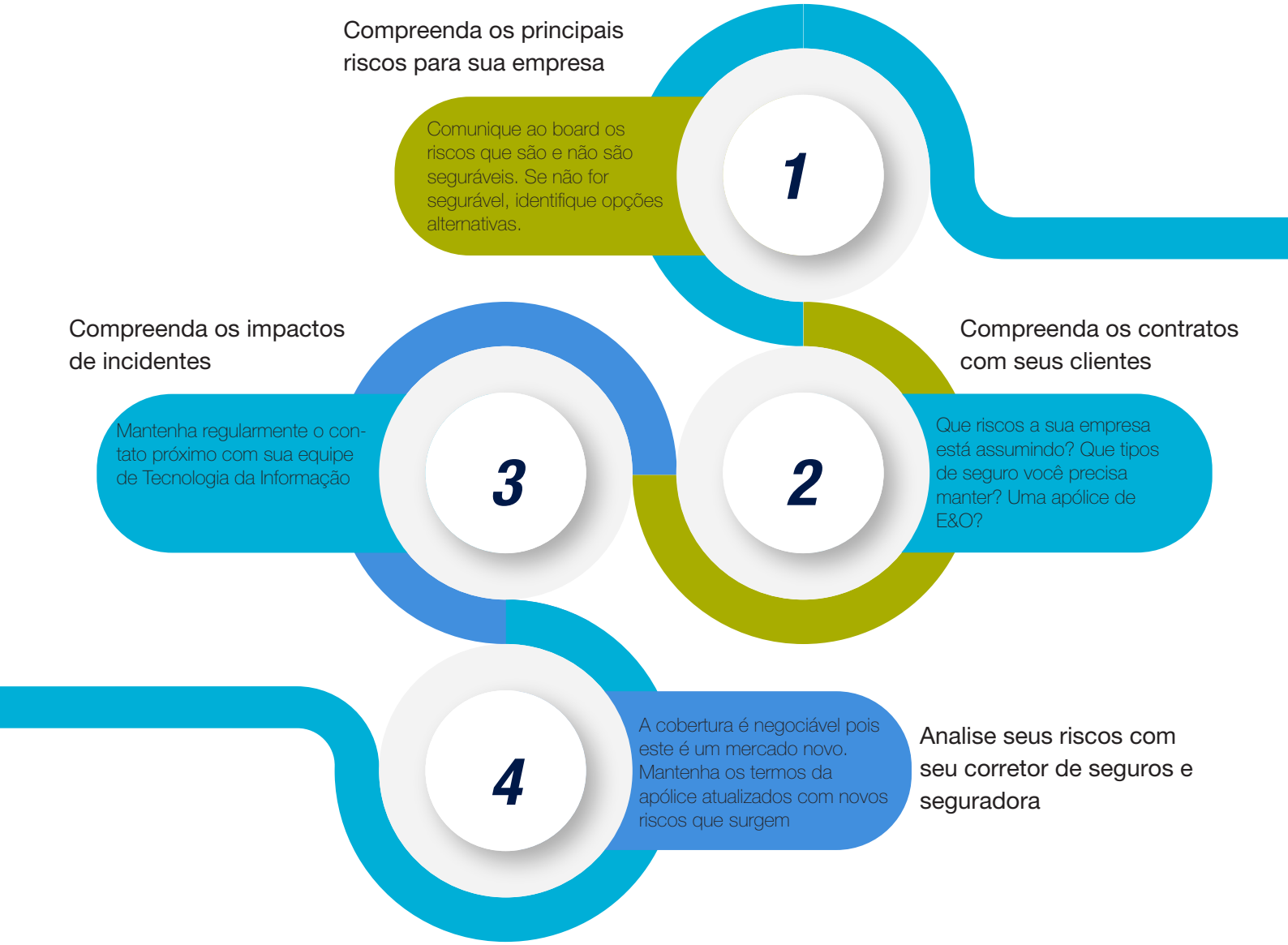
As apólices de responsabilidade geral atualmente não têm a flexibilidade para enfrentar novos e emergentes riscos cibernéticos. Na verdade, a maioria das apólices excluem especificamente o ciber.

"Meu maior risco é minha reputação, e isso o seguro não pode cobrir..."

Sua reputação está entrelaçada com sua capacidade de lidar com um incidente cibernético. A evidência mostra que uma reação rápida para mitigar os impactos de uma violação de dados minimizará os custos imediatos e reduzirá potencialmente a exposição a custos subsequentes, que incluem danos à reputação e perda de vantagem competitiva.

Como as empresas podem gerenciar melhor o risco cibernético?

Sugerimos às empresas gerenciar proativamente seus riscos cibernéticos:



CASES DE SINISTROS DE RISCO CIBERNÉTICO

1. Ransomware

Uma indústria de produção de alimentos e bebidas foi vítima de ramsoware em maio de 2017. Os hackers acessaram o sistema do segurado através de um ataque de phishing. O ramsoware criptografou todos os dados do segurado. Sete servidores e centenas de PCs foram afetados.

Os hackers exigiram 12 bitcoins (cerca de R$ 600mil reais) para as chaves de criptografia. O segurado acionou a apólice com o time de breach response da seguradora para coordenar a violação de privacidade e uma empresa forense para investigar o evento. A empresa segurada e forense não conseguiram descriptografar os dados do segurado e, após consulta com a seguradora e advogados, o segurado tomou a decisão de pagar o resgate.

Facilitamos a retenção de fornecedores para obter o montante necessário de bitcoins para o pagamento do resgate. Uma vez pago, o segurado recebeu as chaves de criptografia necessárias liberação dos sistemas que voltaram gradualmente e precisavam de verificação dos dados.

A empresa foi afetada em seus sistemas offline por 2,5 dias úteis. A seguradora reembolsou ao segurado pelo resgate, R$ 480 mil em bitcoins com despesas de aquisição e pagamento, R$ 950 mil em investigação forense e remediação, R$ 65 mil em custos jurídicos. Além disso, a seguradora reembolsou o segurado em R$ 500 mil por sua receita perdida e R$ 300 mil por despesas emergenciais associadas à interrupção.

Total indenizado: R$ 3.295.00,00

2. Ataque de DDOS (Negação de serviços)

Uma empresa varejista teve um ataque de DDOS durante a Black Friday. O data center que hospeda site online tornou-se alvo e os hackers inundaram a rede do data center com tanto tráfego que a rede entrou a colapso. Isso fez com que o site de e-commerce da empresa ficasse inacessível por um período de 10 horas até o backup de sistemas ser capazes de restaurar 100% da funcionalidade. Depois de reportado o incidente através do breach response, o segurado recebeu custos de despesas emergenciais por contratar uma empresa para restaurar o serviços o mais breve possível no valor de R$ 40 mil, perda de receita diante da interrupção do site (uma vez que o segurado perdeu vendas no tempo de inatividade do site) no valor de R$ 1 milhão, adicionalmente as despesas de resposta ao incidente que abrangem a empresa de forense de TI, reconstrução de dados e despesas emergenciais em R$ 150 mil.

Total indenizado: R$ 1.190.000,00

3. Malware

Um escritório de advocacia teve seu servidor com todos os registros de importantes informações deletados por um malware. Ainda que o segurado possuísse um backup, o mesmo não estava 100% atualizado e grande parte dos arquivos foram perdidos. O Segurado acionou a apólice que cobriu as despesas de reconstrução e restauração de dados através de uma consultoria de TI com gastos em R$ 250.000.

**Os casos divulgados foram concedidos pelas seguradoras.*

4. Ataque a sistemas

Uma companhia aérea sofreu ataque que causou pane em todos os sistemas o que resultou em 14 horas de total paralização, incluindo o website de booking online, controle operacional no aeroporto e escalas da tripulação. Após esse período, os sistemas voltaram a funcionar, no entanto os efeitos duraram quatro dias com 2.500 voos atrasados ou cancelados. A seguradora rapidamente entrou na gestão de crise e o segurado recebeu a indenização de U$$ 79.850.000. A construção do cálculo de sinistro segue abaixo:

Perda de Receita	US$
Cancelamento de voos	30 milhões
Cancelamento de vendas	14 milhões
Cargo e voos	200 mil
Diversos	32 milhões
Total	**76,2 milhões**

Despesas Extras	US$
Salários/Despesas	
Pilotos	3 milhões
Operação de ground	5 milhões
Serviço de atendimento (call center)	500 mil
Manutenção	150 mil
Comissários de bordo	2 milhões
Marketing	1 milhão
Deslocamento de equipe	12 milhões
Despesas emergenciais	5,5 milhões
Total	**29,15 milhões**

Reparo de Sistemas	US$
Consultoria	3,5 milhões
Restauração e reconstrução de dados	2,5 milhões
Total	**6 milhões**

Totais	US$
Total de perdas	99,850 milhões
Franquia	20 milhões
Total indenizado	**79,850 milhões**

**Os casos divulgados foram concedidos pelas seguradoras.*

OS RISCOS CIBERNÉTICOS DEIXARAM DE SER UMA RESPONSABILIDADE DA ÁREA DE TECNOLOGIA. PREPARAMOS ALGUMAS PERGUNTAS QUE TODO CEO DEVERIA SABER RESPONDER:

1. Quão confiante sua empresa está em relação à segurança de informações importantes que estão sendo gerenciadas corretamente e a salvo de ameaças cibernéticas?

2. Qual o impacto na reputação da nossa empresa na eventualidade de um ataque em que informações confidencias de clientes sejam perdidas, ou divulgadas?

3. Qual o impacto no negócio se nossos sistemas forem interrompidos por um período curto ou sustentado?

4. Identificamos nossos principais recursos de sistemas e avaliamos minuciosamente as suas vulnerabilidades a ataques?

5. A responsabilidade pelo risco cibernético foi alocada adequadamente e a área de gestão de riscos está envolvida com a equipe de tecnologia?

6. Temos uma política escrita de segurança da informação e que inclui um plano de emergência?

SEGURO DE RISCOS CIBERNÉTICOS

O potencial de ataques cibernéticos está aumentando em todos os setores e indústrias à medida que a tecnologia se torna mais complexa e sofisticada. É por isso que todas as empresas e organizações precisam estar preparadas com um seguro de riscos cibernéticos. Muitas empresas estão acostumadas a proteger seus ativos físicos com apólices de seguro e, atualmente, os ativos digitais são tão valiosos quanto, porém não recebem a atenção necessária.

O risco cibernético não deve ser considerado apenas como um risco de TI, mas sim ser tratado como um risco operacional chave que exige gestão abrangente em todas as áreas da empresa, inclusive sua reputação.

ONDE?

Apesar do nome, os riscos cibernéticos estão ligados tanto a fontes online como offline. Eles dependem da comunicação eletrônica e processos em rede, mas os elementos de privacidade de dados de risco permanecem mesmo fora da internet. É o caso de um celular perdido que contém informações confidenciais, ou um hacker que consegue inserir um malware em um equipamento da empresa, resultando em uma falha de prestação de serviços ou até mesmo de fabricação de produtos.

QUEM?

Qualquer empresa que usa tecnologia ou coleta dados está sujeita a um ataque cibernético. Incidentes de cyber podem ser causados por inúmeros fatores com diversas motivações. A entrada de um acidente em uma empresa pode ocorrer através de hackers motivados por questões individuais e financeiras, com alto grau de conhecimento tecnológico, e também por funcionários. As empresas são responsáveis por seus dados online, independente de onde estiverem armazenados. Se ele está em servidores próprios, externos ou na nuvem, sua empresa pode ser responsabilizada por qualquer informação individual exposta.

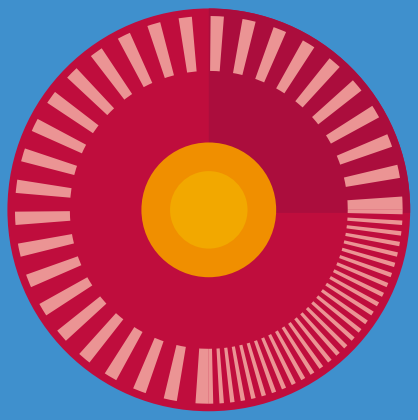
O QUÊ?

TECNOLOGIA MÍDIA DADOS

Incidentes cibernéticos podem afetar uma empresa de diversas maneiras e causar perdas catastróficas a uma organização. Qualquer informação sob a custódia de uma empresa, sejam dados de identificação de funcionários ou clientes, contratos comerciais, mesmo que protegidos por acordo de confidencialidade, e até um conteúdo publicado na rede, pode ser alvo de ataques, resultando em difamações ou uso indevido de propriedade intelectual e perdas financeiras. Mídias sociais usadas pelas companhias e seus funcionários podem aumentar o risco de imagem e reputação e segurança. Finalmente, tecnologia está em tudo o que é feito dentro das empresas, tanto na parte informacional como operacional, que pode resultar em ataques cibernéticos que levam a interrupções e consequências danosas aos negócios.

O seguro cibernético é essencial para ajudar sua empresa a se recuperar após uma violação de dados, com custos que podem incluir:

- Perdas de receita
- Consultores forenses
- Honorários jurídicos
- Consultor de crise
- Despesas com relações públicas para gerenciamento de imagem
- Danos a equipamentos
- Investigação de incidentes e custos de resposta
- Custos relacionados a restaurar/ reconstruir dados
- Custos de reparo de imagem



Nosso time de Cyber Risks oferece uma solução personalizada para atender às suas ameaças e necessidades específicas. No Brasil, a JLT conta com uma unidade especializada e dedicada exclusivamente à consultoria de riscos, due diligence e cyber risk & security com um time de especialistas altamente capacitados para identificar e compreender os riscos que sua operação está exposta e seus possíveis impactos determinando de forma assertiva a contratação da apólice de seguros.

SOMOS ESPECIALISTAS EM CLIENTES

de clientes JLT satisfeitos*

Quando você escolhe a JLT, você é atendido por especialistas técnicos do seu segmento que se tornam parceiros dos seus negócios.

Conte com o time reconhecido por mais de 96% dos clientes pela ética, profissionalismo e atendimento de qualidade.

Estamos ansiosos para trabalhar com você e vencermos juntos.

*Pesquisa de Satisfação Client First JLT 2017.

brasil.jlt.com

Para mais informações sobre riscos cibernéticos, fale com a gente!

falecom@jltbrasil.com

Autorizada e regulamentada pela Autoridade de Condução Fiscal.
Membro do Grupo Jardine Lloyd Thompson. Sede no Brasil:
Av. Eng. Luís Carlos Berrini, 105 Cidade Monções, São Paulo - SP
CEP 04571 010. Registrada na SUSEP nº 10.0058858.
Tel +55 11 3156 3900

BR18001

brasil.jlt.com