MARSH | JLT

CYBER VIEW 2019

Identificando oportunidades no mercado brasileiro

UMA NOVA ERA COM NOVOS RISCOS

Em uma era em que a tecnologia já é parte do cotidiano da maioria da população global, empresas de todos os ramos e segmentos buscam maneiras de inovar, estar presentes digitalmente e até mesmo de reduzir seus custos ou de produzir seus produtos e ofertar seus serviços com a ajuda da tecnologia. Empresas no mundo todo estão investindo em ferramentas de melhorias operacionais, ganho de competividade ou se tornar o próximo unicórnio (termo usado entre as startups para empresas que inovaram a ponto de se tornarem únicos e em que o valuation atinge rapidamente valor igual ou acima de US$ 1 bi).

No entanto, muitas empresas empolgadas com as possibilidades e benefícios que as implementações de novas tecnologias trazem, com frequência esquecem que, ao investir em tais ferramentas um novo risco vem a reboque com o uso da tecnologia, e é preciso contemplar investimento em mecanismos de proteção, processos de controles transferência de potenciais perdas.

No mundo da internet sem fronteiras, em que negócios digitais já nascem globais, os riscos e as responsabilidades devem levar em consideração os locais de atuação de sua empresa, mesmo que sem presença física uma vez que ofertam, coletam e armazenam informações de cidadãos em outros países, passando a ter responsabilidade sobre os dados coletados, processados e usados e sua operação.

No ano de 2018, houve também um grande marco global com a entrada de novos cenários regulatórios como a GDPR (General Data Protection Regulation Directive) na Europa e a aprovação da LGPD (Lei Geral de Proteção de Dados) no Brasil. Tais leis demandam a atenção de empresas de todos os segmentos, independentemente de sua atuação, uma vez que exigem estar em conformidade com uma série de processos para se garantir a segurança de dados pessoais – sejam eles de clientes ou funcionários.

Se por um lado as novas regras trazem maior segurança para o indivíduo, pelo lado da empresa elas podem reduzir e ao mesmo tempo aumentar os riscos cibernéticos. Por exemplo, a regulamentação pode ser um catalisador para melhorar a conscientização e a mitigação dos riscos cibernéticos em uma corporação. Por outro lado, os custos em caso de um incidente cibernético podem aumentar devido a maiores exigências de notificação de incidentes, pagamentos de compensação para terceiros afetados e o potencial para multas maiores.

Após os ataques globais WannaCry e NotPetya que abalaram o mundo, atingindo mais de 150 países, os diversos casos ocorridos no Brasil em 2018 - com vazamento de dados e ações por parte do Ministério Público Federal - mostraram que nosso mercado não está a salvo das ações de hackers como muitos executivos imaginavam devido à não obrigatoriedade de divulgação de vazamento de dados.

Os incidentes atingiram as mais diversas indústrias, nos setores financeiro, de saúde, varejo e serviços. Segundo a empresa Symantec, somos o segundo país com o maior número de crimes cibernéticos no mundo, o que torna imprescindível a criação de uma consciência dos tomadores de decisão de que este não é um risco de TI e sim de toda organização.

Diante de tudo isso, apresentamos a segunda edição do estudo Cyber View, nosso exclusivo e mais completo conteúdo sobre segurança digital do mercado brasileiro. Ao longo de 2018, entrevistamos cerca de 200 empresas de todo o território nacional, 74% delas classificadas como médio ou grande porte, de diferentes segmentos da indústria.

O estudo abrange uma percepção das ameaças, preocupações e contingências de nossos clientes e parceiros em relação aos riscos cibernéticos. Esperamos que este material ajude a sua empresa a entender a complexidade dos riscos cibernéticos em suas operações e auxilie na tomada de decisões.

Marta Helena Schuh
Especialista em Riscos Cibernéticos
Marsh JLT Specialty

CIBERSEGURANÇA

PROCESSOS

Políticas de segurança cibernética
Plano de resposta a incidentes
Controles

PRÁTICAS

Acompanhar novas ameaças
Gerenciamento de fornecedores
Treinamento
Testes de segurança

TECNOLOGIA

Segurança de aplicações
Segurança de dados
Segurança de rede
Segurança operacional
Ferramentas e sistemas

SEGURO

Mitigação de riscos
Transferência de perdas financeiras

RISCOS DIGITAIS E PROTEÇÃO EMPRESARIAL

Não há como fugir: independente de que atividade realize, todo conselho deve ter consciência que sua empresa será vítima de um ataque cibernético e poderá ser responsabilizada diante da não prevenção ou mitigação de um evento. Nossa pesquisa aponta que 55,4% das empresas são totalmente interdependentes do uso de tecnologia em suas atividades. Outras 35% podem ter paralizações severas diante de um problema relacionado a tecnologia (gráfico 1).

Os ataques cibernéticos têm se tornado cada vez mais complexos e, diferentemente de riscos tradicionais, possuem uma alta complexidade e exigem uma série de ações para se averiguar o real impacto de um evento.

10%

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

Diante da falta de evidências tangíveis do risco, com termos definidos em linguagens de códigos, membros do conselho executivo muitas vezes não entendem a criticidade de um ataque em suas operações.

Cerca de 80% dos entrevistados avaliaram que um incidente cyber causaria um impacto operacional com respaldo em toda a empresa, mas apenas 29% já avaliaram monetariamente o que este impacto resultaria às suas organizações (gráfico 2).

GRÁFICO 1

NA SUA VISÃO, QUAL A DEPENDÊNCIA DE SUA EMPRESA NO USO DE TECNOLOGIAS PARA PRESTAÇÃO/EXECUÇÃO DE SUAS ATIVIDADES?

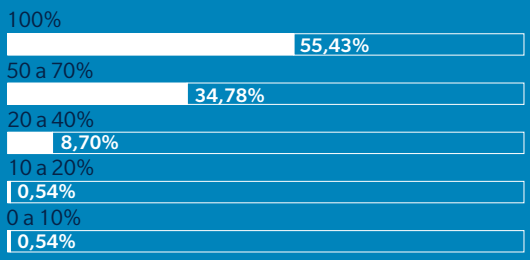
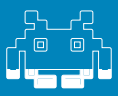


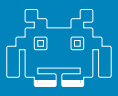
GRÁFICO 2

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

80,23%
Possível impacto operacional que tem respaldo sobre toda empresa



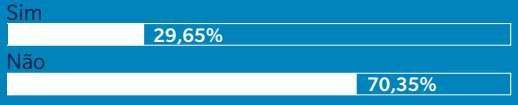
14,12%
Um problema do TI que os demais departamentos não têm responsabilidade



5,65%
Um problema que o departamento financeiro tenha que mitigar

GRÁFICO 3

SUA EMPRESA JÁ QUANTIFICOU O POSSÍVEL IMPACTO DE UM INCIDENTE CYBER?



Aproximadamente 15% avaliaram que este é um problema de TI, sem responsabilidade das outras áreas da empresa. Contudo, a área de TI deixou de ser apenas um suporte para ser estratégica. Diversas empresas possuem sistemas de automação, robôs de atendimento, sistemas de gestão e controles que armazenam as mais diversas informações, relatórios, contratos e até mesmo produtos que impactam diretamente no funcionamento e no desempenho das atividades, independentemente do ramo de atuação. É importante que diretores corporativos comecem a levar a sério a supervisão de segurança cibernética como uma estratégia preventiva administrativa da organização.

Com isso, mais do que nunca, membros do conselho têm de estar a par dos impactos causados. O ex-comissário da SEC (Comissão de Títulos e Câmbio dos Estados Unidos) – equivalente à nossa CVM –, Luis Aguilar, fez seu alerta sobres os riscos cibernéticos. "Bons conselhos também reconhecem a necessidade de se adaptar a novas circunstâncias – tais como os crescentes riscos de ataques cibernéticos. Para isso, a supervisão do conselho no gerenciamento do risco cibernético é fundamental para garantir que as empresas tenham as medidas adequadas para prevenir e reparar os danos que podem resultar em tais ataques. Não há substituição para a preparação adequada, deliberação e engajamento em questões de segurança cibernética. Dada a consciência aumentada destes riscos que estão em rápida evolução, os diretores devem levar a sério suas obrigações em certificar de que suas empresas estão abordando adequadamente esses riscos".

Nosso estudo aponta que, em comparação a outros riscos, os corpos administrativos das empresas consideram a cyber segurança como uma pauta importante, mas não como prioridade.

Lembrando que o risco cibernético tem seus impactos muito além de TI. Empresas também podem sofrer danos a reputação. 29,3% das organizações que responderam nosso estudo afirmam ser essa sua maior preocupação, seguido por 31% que receiam a perda de receita (gráfico 5). Em 2018, nosso estudo demonstrou que as perdas de informações privadas contemplavam 68% da preocupação das empresas.

GRÁFICO 4

EM COMPARAÇÃO A OUTROS RISCOS, O CORPO ADMINISTRATIVO DA SUA EMPRESA CONSIDERA CYBER SEGURANÇA UMA PRIORIDADE?

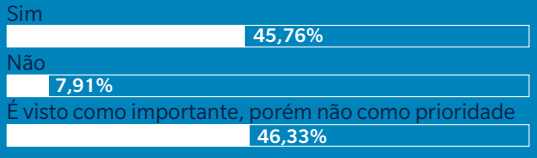
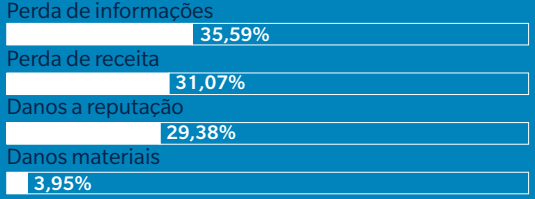


GRÁFICO 5

QUAL O MAIOR RECEIO DA SUA EMPRESA, CASO SOFRA UM ATAQUE VIRTUAL?



CARTILHA
C-LEVEL
PARA REVISAR SUA OPERAÇÃO

ESTRUTURAS POLÍTICAS DE SEGURANÇA CIBERNÉTICA

Um bom começo é estruturar políticas e procedimentos de segurança cibernética – se a sua empresa já tem uma, talvez impor como regra uma revisão periódica e se as mesmas atendem às constantes evoluções tecnológicas.

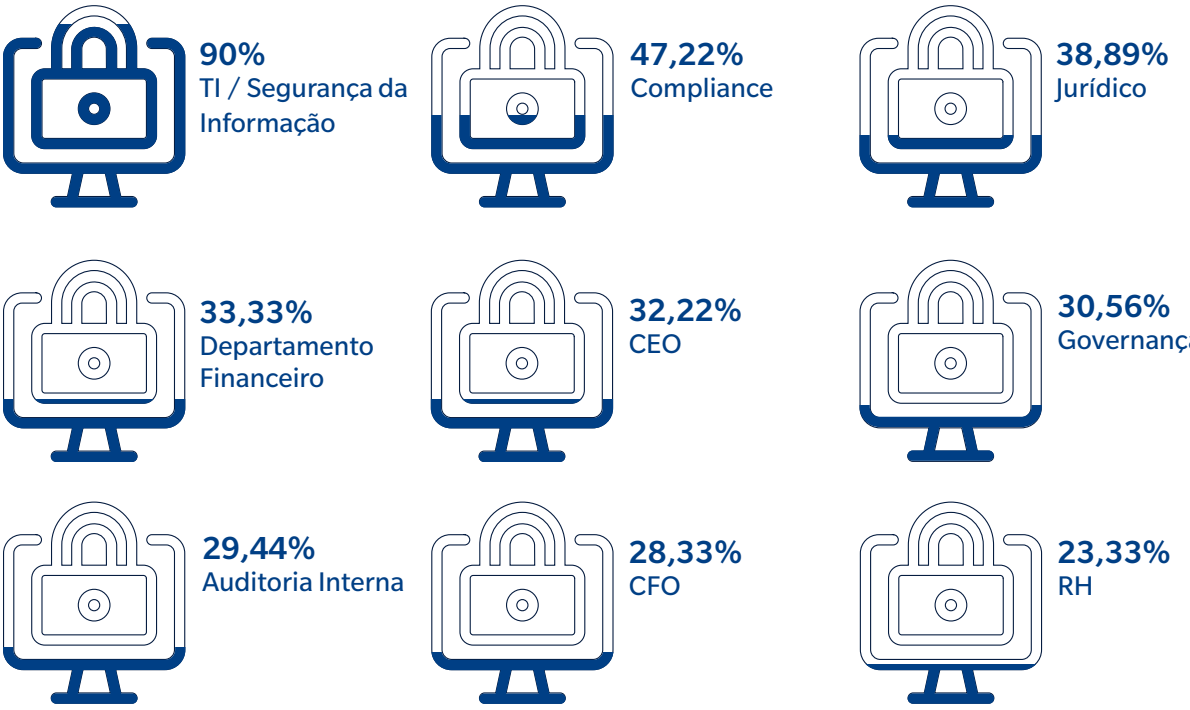
Apontar um responsável com reporte direto ao comitê ou CFO. Este profissional deve contemplar não apenas os aspectos de riscos da TI e segurança da informação, mas também possíveis impactos jurídicos, regulatórios e financeiros e estabelecer responsabilidades entre a política diante das necessidades de performance dos procedimentos pelos departamentos envolvidos, assim como o monitoramento com acompanhamento de relatórios periódicos.

Outro ponto importante é incentivar um programa de treinamento estruturado que contemple a empresa como um todo. A maior vulnerabilidade de segurança cibernética em qualquer empresa é sempre humana, segundo Casey Flemming – CEO, BLACKOPS Partners – Intelligence, Cybersecurity, o elemento humano é crítico em 95% dos incidentes e a tecnologia é apenas 4% efetiva.

Quando não há cumprimento das regras de segurança cibernética e conscientização das necessidades em segui-las, as violações ocorrem mesmo com o mais alto nível de investimento em ferramentas de proteção. Por isso, ter um programa de treinamento em segurança cibernética com campanhas de phishing periódicas durante o ano são essenciais. Os treinamentos devem ter um approach interativo que engaje o usuário – em tempos de excessos de informações é importante que seus funcionários não vejam como algo monótono.

GRÁFICO 6

EM COMPARAÇÃO A OUTROS RISCOS, O CORPO ADMINISTRATIVO DA SUA EMPRESA CONSIDERA CYBER SEGURANÇA UMA PRIORIDADE?



PLANO DE RESPOSTA A INCIDENTES

De acordo com a ISO 22301, Plano de Continuidade de Negócios é definido como "procedimentos documentados que as organizações precisam como um guia" para responder, recuperar, retomar e restaurar a um nível pré-definido de operação após a interrupção.

44,2%

das empresas não possuem plano de contigência, nem provisionaram em seus orçamentos uma possível crise

Nosso estudo aponta, pelo segundo ano consecutivo, que as empresas não estão devidamente preparadas com um plano de incidente a repostas e contingenciamento à sua operação. Em 2017, 35% dos nossos respondentes mencionaram não ter um plano; este ano, 44,2% não apenas não possuem um plano de contingência, como também não provisionaram em seus orçamentos uma possível crise (gráfico 7).

Leis como a GDPR, Resolução 4.658/2018 do Bacen e a LGPD exigem que as organizações que sofram uma violação de dados o relatem o mais rápido possível. Mais detalhadamente, sob a LGPD, uma violação de dados pessoais é "ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares" (Art. 48) e, assim sendo, empresas precisam estar preparadas para agir rapidamente diante de um incidente.

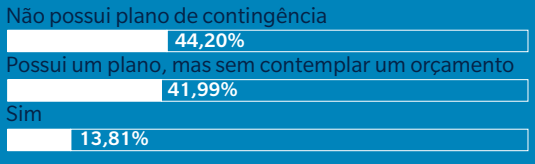
Além disso, empresas geralmente têm um plano de continuidade de negócios voltado para a parte operacional – contemplando ações da natureza ou em caso de incêndio – mas, em diversas vezes, temos visto que não há abrangência sistêmica que possua um grande impacto financeiro – muitas delas até maiores que um incidente operacional. Estruture o plano de continuidade de negócios contemplando os impactos no negócio, estratégia de continuidade de negócios e quais áreas devem estar envolvidas com suas devidas responsabilidades.

Contemplar um plano de resposta a incidentes, com canais de comunicação para eventos com menor ou maior criticidade, são fundamentais. Lembre-se que seu e-mail/plataforma de chamados podem não funcionar, então, é necessário criar canais alternativos.

Por último, simule a execução deste plano. Teste em uma simulação como se fosse D-DAY, verifique o resultado e revise com as lições aprendidas ao menos uma vez por ano.

GRÁFICO 7

A SUA EMPRESA POSSUI UM PLANO DE CONTINGÊNCIA PARA ATAQUES CIBERNÉTICOS QUE INCLUI UM BUDGET PARA AS DESPESAS A UM ATAQUE?



ACOMPANHE AS AMEAÇAS DE SEGURANÇA

Nem todas as empresas enfrentam as mesmas ameaças de riscos cibernéticos. Não existe uma abordagem "tamanho único". O risco é uma constante evolução e não há nenhuma ferramenta que garanta 100% da integridade protecional de sistemas.

Cerca de 34% das empresas que responderam nossa pesquisa relataram ter sofrido algum tipo de incidente cibernético nos últimos 12 meses (gráfico 9), com 29% sofrendo impactos operacionais, 27,8% com altos custos de reconstrução sistêmica e 4% com impactos reputacionais diante de seus clientes (gráfico 11).

Empresas que retêm grandes quantidades de dados pessoais precisam adequar suas defesas e planos de mitigação e incidente para garantir a seus usuários/clientes a segurança dos mesmos. Já em certas indústrias, os riscos de uma invasão nos sistemas operacionais podem ter um teor catastrófico, gerando perdas operacionais.

Com isso, um plano de investimento e acompanhamento contínuo na área de segurança é de suma relevância em qualquer operação. As empresas precisam se manter atualizadas sobre as ameaças mais recentes e preparar-se de acordo. Preparação é a chave.

Ter um cronograma definido de atualizações de patches e versões atualizadas de software também podem ser uma maneira simples de ajudar sua empresa a estar em dia com a higiene de segurança. Além disso, a questão orçamentária precisa vislumbrar que custos atrelados a uma violação podem sair muito além do esperado.

GRÁFICO 8

NOS ÚLTIMOS 12 MESES, ONDE SUA EMPRESA INVESTIU PARA A MELHORIA DA SEGURANÇA CIBERÉTICA?

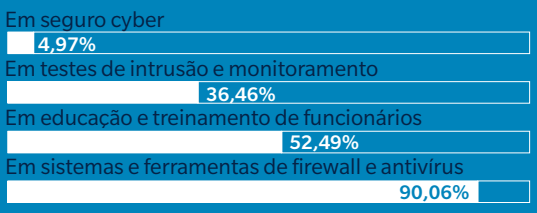


GRÁFICO 9

NOS ÚLTIMOS 12 MESES HOUVE ALGUM INCIDENTE CYBER NA SUA EMPRESA?

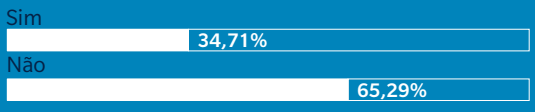


GRÁFICO 10

NA VISÃO DA SUA EMPRESA, QUAL O MOTIVO PARA INVESTIR NA PREVENÇÃO DE INCIDENTES CYBER?

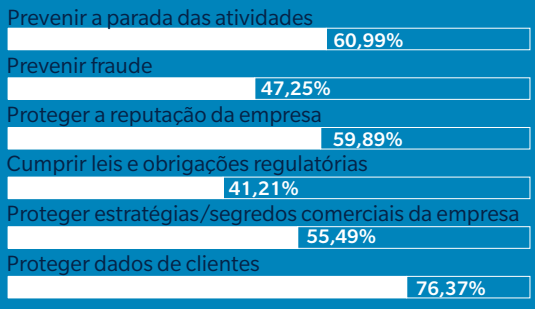
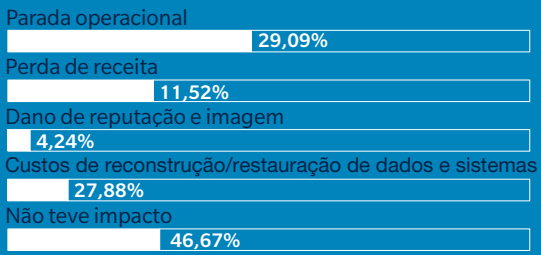


GRÁFICO 11

SE A SUA EMPRESA JÁ SOFREU UM EVENTO CYBER, QUAIS FORAM OS IMPACTOS?



CONTROLE E PROCESSOS

Com tantas ferramentas de gestão disponíveis, muitas empresas subestimam a importância de se ter procedimentos definidos e acessíveis quando seus sistemas falharem. O estudo aponta que cerca de 90% dos executivos responderam que é mais importante a prevenção de incidente que a agilidade em uma crise (gráfico 12).

Contudo, é necessária a estruturação de procedimentos de controles para se evitar incidentes e, na eventualidade de uma ocorrência, ter detalhes de procedimentos e evidências eletrônicas, uma vez que se tornaram cada vez mais demandadas quando há um incidente. Alguns órgãos reguladores demandam que empresas tenham documentado procedimentos, por isso, ter formalizado procedimentos de logs, classificação e inventário de dados, controles de acesso, processo de retenção e descarte de dados não devem ser somente preservados em sistemas, mas considerar um acesso alternativo que, na eventualidade de um ataque, sua empresa consiga começar o processo de investigação.

Preservação é um fluxo de trabalho crítico durante um ataque cibernético. Conseguir identificar quais sistemas e dados foram afetados é o primeiro passo e um dos mais críticos, permitindo o time de forense digital fazer o processo de engenharia reversa de malware.

A análise de sistemas comprometidos conhecidos ou suspeitos identifica as ameaças, passando, então, por uma análise de tráfego de rede e registros, também uma varredura de hosts e, a partir disso, se possível, corrigir o malware, reconstruir sistemas comprometidos, redefinir as credenciais da conta comprometida, bloquear endereços IP e iniciar adequadamente o monitoramento de rede e host em um esforço para detectar tentativas adicionais do atacante para recuperar o acesso.

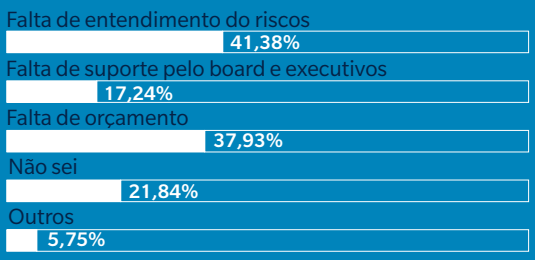
A preservação de backups também é crítica porque os investigadores provavelmente precisarão vasculhar todas as evidências eletronicamente armazenadas com a intenção de identificar o endereço IP.

GRÁFICO 12

EMBORA NÃO EXISTAM SISTEMAS E FERRAMENTAS QUE GARANTAM 100% DE SEGURANÇA, O QUE É MAIS IMPORTANTE NA SUA VISÃO: PREVENÇÃO OU UMA RESPOSTA ÁGIL AO INCIDENTE?

GRÁFICO 13

QUAIS SÃO OS MAIORES OBSTÁCULOS EM SUA ORGANIZAÇÃO PARA ENDEREÇAR UM PROGRAMA DE SEGURANÇA CIBERNÉTICA COM ROBUSTEZ?



GERENCIAMENTO DE FORNECEDORES E TERCEIROS

A terceirização de serviços como TI, folha de pagamento, serviços contábeis, advocatícios, entre outros, normalmente envolve a transferência ou permissão de acesso de interconexão entre sistemas de sua empresa para seu fornecedor.

Dado que os cyber-invasores costumam atravessar a rede de uma empresa e entrar nas redes de seus fornecedores ou vice-versa, os ataques cibernéticos podem, muitas vezes, resultar em disputas sobre a responsabilidade do ataque. Como resultado, na maioria dos cenários em que incidentes ocorrem, fornecedores e empresas podem acabar apontando o dedo um para o outro por suas respectivas falhas de segurança cibernética.

Assim, os conselhos devem estar preocupados se qualquer fornecedor terceirizado tiver acesso às redes de sua empresa, dados do cliente ou outras informações confidenciais. Além disso, devem entender se e como a empresa incorpora requisitos relacionados ao risco cibernético em seus contratos com fornecedores que vão além da mera prestação e entrega dos serviços através de um SLA.

Com a entrada de legislações como GDPR e LGPD, fornecedores que processam e têm acesso a dados sensíveis têm responsabilidades diante da segurança cibernética a serem cumpridas e é dever da empresa contratante solicitar o compliance das normas.

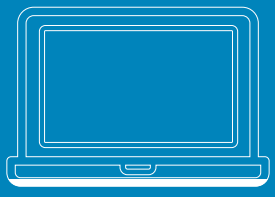
Os conselhos de administração devem perguntar sobre a segurança da informação da empresa, os procedimentos (incluindo treinamento) referentes a fornecedores terceirizados autorizados a acessar a rede e também proteção contratual, que vai além de uma penalização de multa ao fornecedor – seguro de E&O é contratado pelo fornecedor que visa a cobrir as reclamações feitas por clientes, decorrentes de danos causados pelo fornecedor em falhas ou erros na prestação dos seus serviços profissionais.

GRÁFICO 14

SUA EMPRESA ADOTA MEDIDAS DE PREVENÇÃO DE DANOS AO CONTRATAR DE FORNECEDORES QUE CONVERSAM COM OS SEUS SISTEMAS?

62,72%
Não

32,54%
Sim, nosso contrato contempla multa em um percentual do mesmo



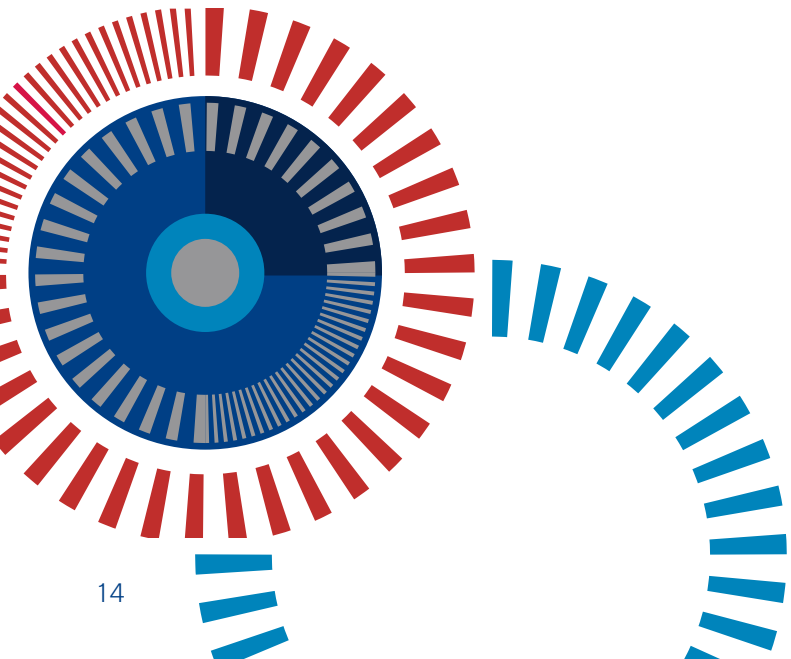
4,73%
Sim, nossa empresa exige uma apólice de E&O e Cyber Risks de nossos fornecedores

SEGURANÇA FÍSICA

Os ataques cibernéticos em estruturas físicas já são uma realidade. O aumento da digitalização através de dispositivos e sistemas inteligentes IOT continua a criar eficiências e oferece às mais diversas indústrias oportunidades de melhora no gerenciamento e até mesmo no aumento de produção.

A interconectividade dos sistemas ICS e SCADA podem levar um incidente a ter consequências nocivas ao mundo físico, como a perda de controle de equipamentos, o que resulta em avaria das máquinas, incêndio, explosão ou ferimentos, com impactos significativos nas operações de ativos de empresas, comunidades locais e a economia.

Ataques cibernéticos podem, às vezes, começar por meio de uma violação física, mesmo que seus sistemas industriais estejam em uma rede interna isolada. Isso parte especialmente quando há a necessidade de atualização/manutenção/reparo do equipamento em que fornecedores, então, são acionados e interconectam seus equipamentos que podem estar infectados. Outros métodos incluem o descuido de funcionários que possam causar acidentalmente um evento.



Já há diversos casos divulgados globalmente de danos físicos causados por ataques cibernéticos, como na empresa Aramco, maior produtor mundial de petróleo e gás, onde alguns sistemas ficaram inoperantes por 10 dias e 85% do hardware da empresa foi destruído. Em dezembro de 2018, a italiana Sapiem sofreu um ataque malicioso que afetou os servidores e infraestrutura em diversos locais de operação, incluindo Arábia Saudita, Emirados Árabes e Escócia.

A pequena barragem de Bowman Avenue, próxima a Nova Iorque, também foi vítima, quando hackers obtiveram acesso parcial aos sistemas usando malware e destacando a vulnerabilidade de toda a infraestrutura. Já na indústria, os ataques WannaCry e NotPetya paralisaram as plantas dos segmentos automotivo, alimentício e bens de consumo.

Cerca de 46% das empresas que participaram da pesquisa State of Industrial Cybersecurity 2018* sofreram um incidente cibernético nos últimos 12 meses. Mais de três quartos das empresas acreditam que elas provavelmente se tornarão alvo de um ataque de segurança cibernética no espaço OT/ICS em pouco tempo.

Assim, empresas devem fazer uma revisão da segurança física e instalações, incluindo planos da administração para checkpoints de recepção e entrada; scanner de identificação e outros registros de acesso; vídeo ou imagens fixas; registros de elevador e garagem, além de controles de acesso a redes.

*Realizada pela Kaspersky Lab com base nas respostas de 320 profissionais no mundo com poder de decisão em cibersegurança OT/ICS.

SEGURO CYBER

A sua empresa certamente contrata algum tipo de seguro para mitigar possíveis impactos – seja seguro de transportes, automóvel, patrimonial, responsabilidade civil, D&O, entre outros. Assim como nos ramos tradicionais, empresas públicas e privadas devem levar em consideração os riscos cibernéticos e pensar o gerenciamento total de riscos corporativos e mecanismos de transferência de risco através de uma apólice de seguro.

Cada vez mais o seguro cibernético tem se tornando um elemento básico de proteção corporativa devido aos severos danos que os impactos podem resultar. As apólices de seguros são projetadas para reduzir perdas de uma variedade de incidentes, incluindo violação de dados, interrupção de negócios e danos a rede, assim como custos de defesa, danos à imagem da empresa, entre outros.

Definir a cobertura ideal de uma apólice cyber deve começar com uma revisão das políticas da empresa em retenção de perdas e, também, uma análise de risco apurada do que seria mais impactante à sua operação – vazamento de dados? Quebra de equipamento? Fraude? Reputação?

OOs membros do conselho devem perguntar se seus executivos consideraram a revisão de ataques em suas áreas, analisando o impacto na realização das atividades de cada departamento separadamente, e como a quebra do fluxo de um departamento afetado pode afetar outro que talvez não teve seus sistemas contaminados. Por exemplo, o departamento jurídico é atacado e o departamento de vendas não, no entanto, há uma interdependência na aprovação e liberação contratual. Assim, também deve-se considerar o todo dentre sua operação – quando a empresa toda para diante de um ataque.

Ao fazer esse exercício de revisitar as realidades e economia de diferentes departamentos, uma empresa conseguirá, então, contemplar as prioridades na definição de limites, franquias e coberturas da apólice.

Por último, quando um ataque cibernético ocorre, muitas vezes há dúvidas quanto à cobertura, o que pode afetar a resposta a incidentes. Assim como nos outros ramos, a reivindicação de seguro seguirá, sem dúvida, todas as faturas relativas aos fluxos de trabalho enumerados, além de documentação de processos e perícia de investigação. Para máxima objetividade, é fundamental ter um corretor que conheça o produto para auxiliar na regulação e ter um profissional da equipe de resposta a incidentes, acompanhar solicitações e revisões de investigação e manter um relatório periódico. Isso ajudará na coleta do “pacote de documentação” para ter o reembolso da seguradora para os custos da violação.

O aumento global de ataques cibernéticos fez com que as empresas considerassem uma apólice de seguro cyber de cobertura ampla e bem planejada, não apenas para cobrir os riscos decorrentes de uma violação de vazamento de dados, mas também para o imediato acesso a especialistas previstos nestas apólices.

Além disso, com a entrada de leis de proteção de dados e normas de segurança cibernética por diferentes órgãos reguladores, se cria também uma exposição significativa não apenas para o seguro cyber, mas também para o seguro de D&O. Com a prestação de contas e compliance das medidas como um tema central nos novos regulamentos, o seguro cyber não é o único relevante a ser considerado e a ênfase também deve ser colocada no seguro de responsabilidade de diretores.

A constante evolução das ameaças está claramente impondo responsabilidades adicionais aos diretores e conselho administrativo. O impacto financeiro de uma violação de dados pode ser enorme; como tal, os diretores devem se preocupar tanto com sua obrigação fiduciária perante a empresa quanto com seus acionistas, bem como com os seus ativos pessoais, que estão em risco no caso de uma reivindicação por alegada gestão ilícita.

Em uma situação em que um incidente cibernético tem um efeito material no valor do acionista da empresa, ou mesmo no valor da reputação, os litígios certamente ocorrerão, especialmente se houver um lapso por parte do conselho para garantir o risco.

Empresas que mantêm o seguro cibernético também demonstram ter uma melhoria significativa em sua segurança cibernética, políticas e práticas. O serviço da Marsh JLT Specialty antes de uma empresa obter cobertura de seguro cibernético inclui uma revisão rigorosa de procedimentos, processos, sistemas. Assim, são feitas recomendações de melhorias – muitas vezes as mesmas não requerem quaisquer investimentos em sistemas, apenas a definição de processos que até então não estavam sendo contempladas e poderiam dificultar na aceitação, precificação e regulação de um sinistro. Assim sendo, o seguro cibernético pode ajudar no gerenciamento e impactos de uma violação de dados, mas também na melhoria da segurança e postura da empresa.

GRÁFICO 15

SUA EMPRESA POSSUI UMA APÓLICE DE SEGURO CYBER?

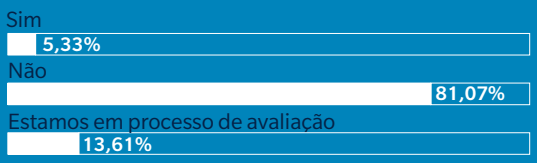
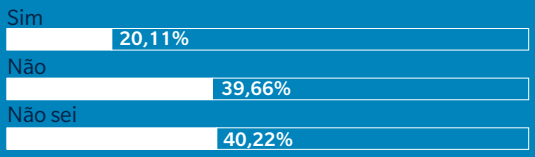
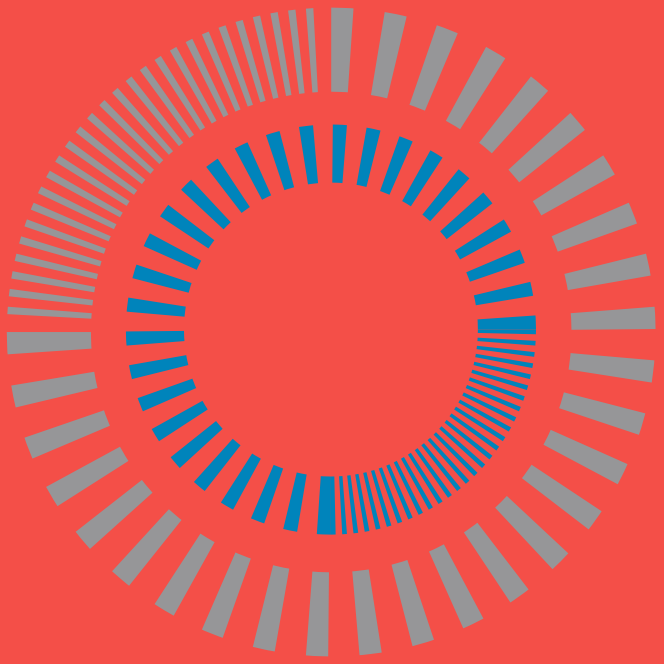


GRÁFICO 16

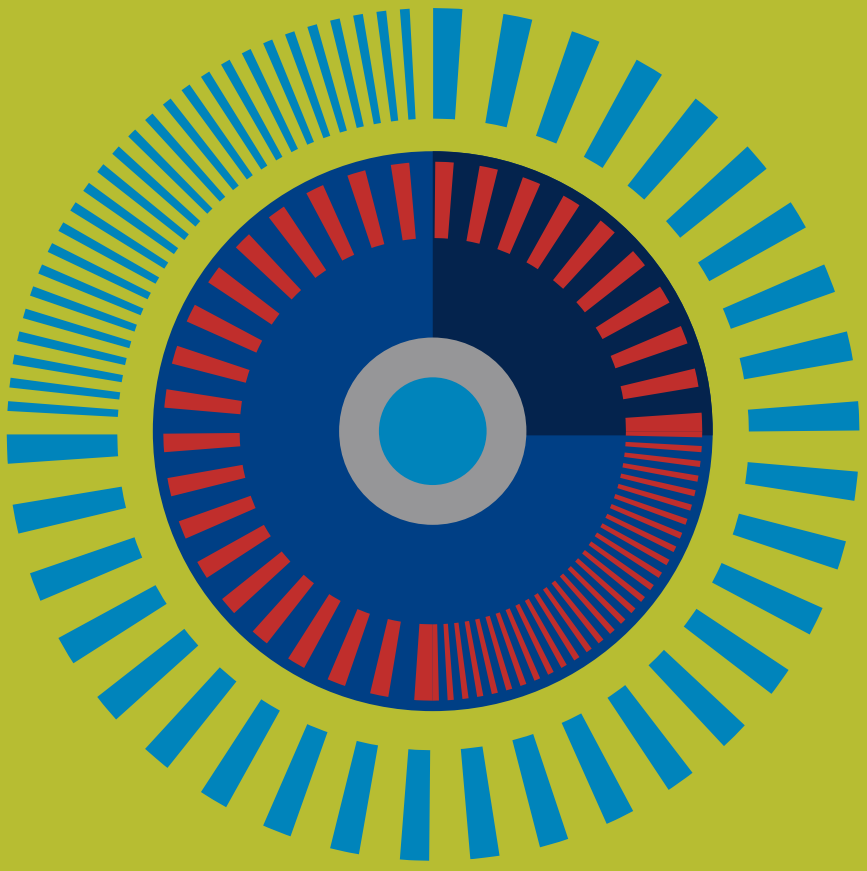
SUA EMPRESA ESTÁ PLANEJANDO A CONCENTRAÇÃO DE UMA APÓLICE CYBER NOS PRÓXIMOS 12 MESES E JÁ INCLUI EM SEU ORÇAMENTO?





COBERTURAS SEGURO CYBER


Despesas em conexão com uma investigação ou processo resultante de uma violação de dados confidenciais, algumas seguradoras ofertam multas por danos de reparação do consumidor
#Jurídico #Financeiro
Custo de recuperação ou recuperar dados que foram destruídos, danificados ou corrompidos devido a um ataque de computador
#TI
Perda de receita líquida e despesas extras decorrentes de um ataque que desabilita os sistemas e impede que o segurado forneça serviços profissionais
#Financeiro
Despesas com reclamações (custos de defesa) e danos por terceiros (funcionários, clientes ou outros) decorrentes de violação de segurança que expõe dados privados
#Jurídico
Custo da investigação e o montante da extorsão relacionado com a ameça
#TI
Perda de dados
Procedimento regulatório
Extorsão ou sequestro de dados
Responsabilidade de privacidade
Coberturas da apólice_
Interrupção de negócios
Gestão de crise
Investigação e perícia
Responsabilidade de mídia
Despesas emergenciais
Custos de relações públicas, notificação dos indivíduos, call center para atenção aos envolvidos
#Marketing #Financeiro
Custos para investigação e perícia do incidente
#TI
Danos sofridos por terceiros provenientes de danos pessoais e violação de propriedade intelectual (exceto violação de patente) por conteúdo distribuído
#Jurídico
Despesas razoáveis e necessárias incorridas pelo segurado durante o período de restauração para minimizar, evitar ou reduzir uma interrupção de serviço
#Empresa

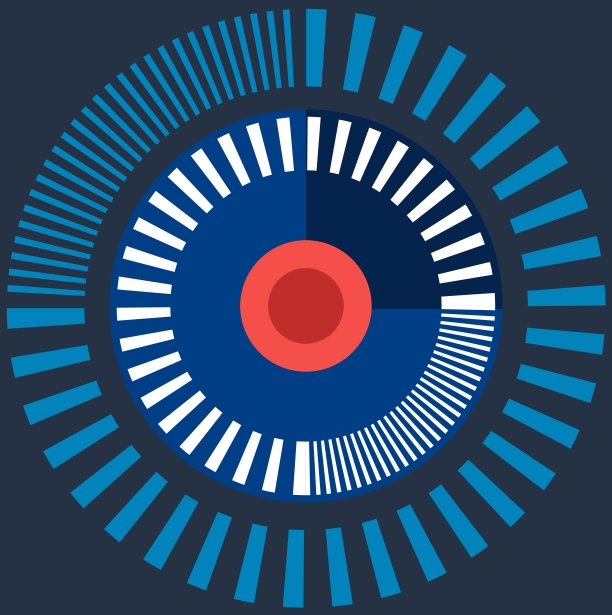


12 PONTOS PRINCIPAIS SOBRE A LGPD

LEI DE PROTEÇÃO DE DADOS DO BRASIL


AUTORIDADE
Previsão de Autoridade Nacional de Proteção de Dados, responsável por garantir cumprimento da Lei
NOTIFICAÇÕES OBRIGATÓRIAS
em caso de incidentes de segurança envolvendo os dados nas situações aplicáveis
APLICAÇÃO EXTRATERRITORIAL
Aplica-se também a empresas que não possuem estabelecimento no Brasil
ESCOPO DE APLICAÇÃO
Afeta qualquer atividade que envolva utilização de dados pessoais, incluindo o tratamento pela internet, de consumidores, empregados, entre outros
DADOS: SENSÍVEIS, DE MENORES E TRANSF. INTERNACIONAL
Regras específicas para tratar dados sensíveis, transferência internacional de dados e utilizar dados de crianças e adolescentes
AUTORIZAÇÃO PARA O TRATAMENTO DE DADOS
O consentimento será uma das 10 possibilidades que legitimarão o tratamento de dados pessoais
ASSESSMENT SOBRE O TRATAMENTO DE DADOS
Necessidade de realizar assessment de impacto à proteção de dados (semelhante ao DPIA)
PRINCÍPIO DE PROTEÇÃO DE DADOS
Introduzidos 10 princípios da proteção de dados, incluindo-se o de demonstrar medidas adotadas para cumprir a lei (prestação de contas)
MAPEAMENTO DO TRATAMENTO DE DADOS
Atividades de tratamento de dados devem ser registradas em relatório
SANÇÕES
Multas de até 50 milhões de reais por infração, entre outras sanções
DIREITOS DOS TITULARES DE DADOS
Titulares de dados terão amplos direitos: informação, acesso, retificação, cancelamento, oposição, portabilidade, entre outros
DATA PROTECTION OFFICER (DPO)
Toda empresa responsável por tratamento de dados deverá nomear encarregado de proteção de dados pessoais

CONCLUSÃO



A segurança cibernética emergiu rapidamente como uma área-chave de risco corporativo e, portanto, o conselho de administração deve levar seus impactos seriamente. Na percepção da maioria de clientes, empresas que sofrem violações de dados e causam impactos são vistas como culpadas diante do ocorrido.

Conselhos de administração devem estar mais envolvidos na garantia das organizações, abordando adequadamente a segurança cibernética. Para as corporações, este é o alvorecer de uma nova era de riscos, em que tentar evitar um ataque cibernético representa proteger a empresa de grandes perdas até maiores das que tradicionalmente estão acostumadas.

Se anteriormente esta era uma responsabilidade do diretor de TI, a pauta passou a ser de responsabilidade do conselho, que tem o dever fiduciário de entender e supervisionar, já que os impactos atingem a organização e resultados como um todo. Hoje, os conselhos e as empresas as quais governam estão sujeitos ao escrutínio público imediato e esta nova realidade essencialmente removeu a distinção entre membro do conselho e o executivo de TI.

O engajamento de segurança cibernética para os membros do conselho de administração não significa que os membros devem obter graus de ciência da computação ou supervisionar pessoalmente o firewall, implantações de sistemas ou testes de intrusão. Conselhos de administração podem realizar a supervisão da segurança cibernética através do envolvimento ativo de acompanhamento das medidas descritas aqui, em que as mesmas estão sendo executadas. Apoiar as iniciativas de TI não só no que se diz respeito a aquisição de ferramentas operacionais, mas o investimento em segurança se torna crucial. Ter um comitê estruturado para acompanhamento das medidas e uma auditoria anual também devem ser considerados e, é claro, seguro, porque nenhuma ferramenta é 100% eficaz e se o hacker entrar e causar prejuízos a empresa terá que arcar com os custos.

Historicamente, as empresas têm associado risco cibernético a ataques maliciosos e violações de dados. No entanto, os números do mercado segurador apontam um aumento no número de incidentes cibernéticos que resultaram em interrupção substancial da operação, impactando significantemente os sistemas de TI nas áreas de logística, distribuição, financeiro e operações – como o ocorrido à Reckitt Benckiser, que relatou estimativa perda de vendas de £100 milhões, em consequência de um incidente de impacto operacional.

Além disso, com a entrada de leis de proteção de dados, normas de segurança cibernéticas por diferentes órgãos reguladores, há uma exposição significativa de perdas das organizações. A LGPD (Lei 53/2018) do Brasil contém princípios semelhantes às leis de proteção de dados da UE (GDPR), que entrou em vigor na Europa em maio de 2018. Como a GDPR, a lei brasileira vem com penalizações severas ao não cumprimento, podendo resultar em uma multa de até 2% da receita ou R$ 50 milhões por infração. Quando implementada, o Brasil se tornará a mais recente jurisdição a introduzir leis abrangentes de proteção de dados em conformidade com a GDPR da UE.

REFERÊNCIAS

1. Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," Speech by SEC Commissioner Luis Aguilar, disponível em:
<http://www.sec.gov/News/Speech/Detail/Speech/1370542057946#.VPxpsEJtIRF>. Acesso em novembro de 2018

2. Economist Intelligence Unit Report, "Reputation Risk: Risk of Risks", disponível em:
<http://databreachinsurancequote.com/wp-content/uploads/2014/10/Reputation-Risks.pdf>. Acesso em novembro de 2018

3. Techtarget, disponível em:
<https://searchsecurity.techtarget.com/definition/cybersecurity>. Acesso em novembro de 2018

4. World Energy Council - New cyber resilience report: energy sector prime target for cyber-attacks, disponível em:
<https://www.worldenergy.org/news-and-media/press-releases/new-cyber-report-energy-sector-prime-target-for-cyber-attacks/>. Acesso em dezembro de 2018

5. Symantec – Relatório de Ameaças à segurança na Internet 2018, disponível em:
<https://www.symantec.com/pt/br/security-center/threat-report>. Acesso em dezembro de 2018

6. GDPR and privacy lawsuits an emerging exposure, disponível em:
<https://www.jlt.com/insurance-risk/cyber-insurance/insights/gdpr-and-privacy-lawsuits-an-emerging-exposure>. Acesso em dezembro de 2018

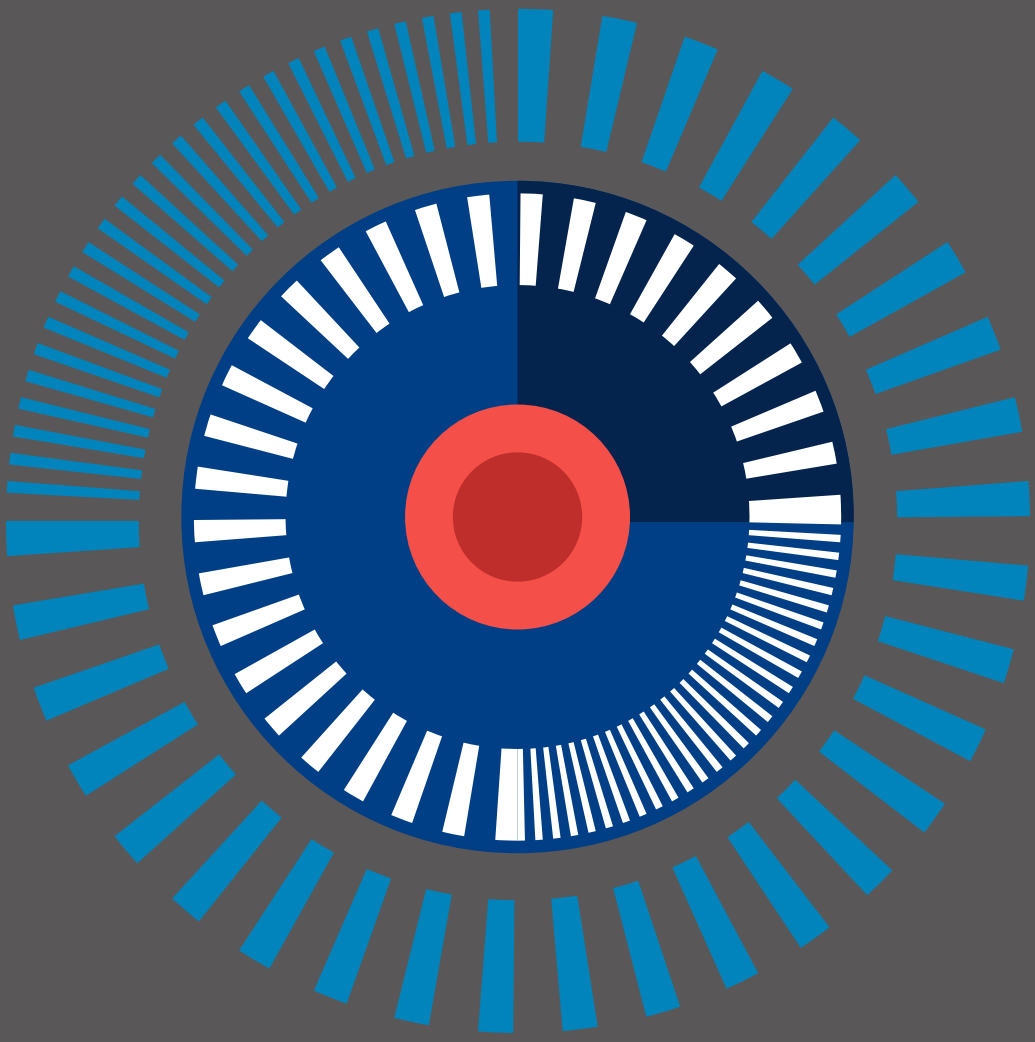
7. Risk managers want to transfer cyber risk, disponível em:
<https://www.jlt.com/insurance-risk/cyber-insurance/insights/risk-managers-want-to-transfer-cyber-risk>. Acesso em dezembro de 2018

8. State of Industrial Cybersecurity 2018, disponível em:
<https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2018/>. Acesso em janeiro de 2019

9. Industrial and utility companies tardeted by cyber attacks, disponível em:
<https://www.jlt.com/insurance-risk/cyber-insurance/insights/industrial-and-utility-companies-targeted-by--cyber-attacks>. Acesso em janeiro de 2019

10. Cyber insurance guide to aid discussions, disponível em:
<https://www.jlt.com/insurance-risk/cyber-insurance/insights/cyber-insurance-guide-to-aid-discussions>. Acesso em janeiro de 2019

11. Risk managers take centre stage managing cyber risk, disponível em:
<https://www.jlt.com/insurance-risk/cyber-insurance/insights/risk-managers-take-centre-stage-managing--cyber-risk>. Acesso em janeiro de 2019



Autorizada e regulamentada pela Autoridade de Condução Fiscal.
Membro do Grupo Marsh McLennan Companies. 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

BR19017

marsh.com