Evento reuniu grandes profissionais para discutir os desafios e atualidades do Seguro de Riscos Cibernéticos, legislação de Inteligência Artificial e os danos causados pelas enchentes no Rio Grande do Sul

Na terça-feira (12), a Associação Internacional do Direito do Seguro (AIDA Brasil), realizou a o 6° Encontro Nacional de Seguros e Responsabilidade Civil. O evento é uma realização do GNT de Responsabilidade Civil e Seguro da entidade. Transmitido pelo canal da instituição no Youtube, o encontro foi realizado no IBMEC, em São Paulo, e contou com as presenças de Marcia Ribeiro, Mariana Ferraz Menescal Jahic e Daniela Benes Hirschfeld, como mediadoras dos três painéis respectivamente. Também teve as participações de Allex Amorim, Thiago Amorim, Marck Rodrigues de Sá, Marcos Bruno, Fernando Nery e Henrique Volpi. Teve, ainda, as participações de Rodrigo Cardona, Carlos Eduardo Pianovski Ruzyk e Silvana Speranza, como palestrantes.

Painel 1 - Desafios e Atualidades do Seguro de Riscos Cibernéticos

Allex Amorim explanou sobre me mercado de cibersegurança e o papel do Chief Information Security Officer (CISO). Além de ser um líder frente a esse tema, o CISO tem a responsabilidade de definir toda a estratégia de cibersegurança de uma companhia. Segundo tendência do World Economy Forum, o risco cibernético é o 5° maior do mundo e uma grande preocupação para as empresas. "Mesmo atuando em segmentos distintos, as dores são parecidas. Existe uma dificuldade do board entender a importância da segurança. Muitas empresas acabam virando notícia diariamente e só aí o board começa a ficar preocupado", relatou Amorim.

Em sua apresentação, o executivo compartilhou dados que revelam que o Brasil é o 2° país da América Latina mais atingido por ataques cibernéticos (phishing). Sofreu 103,16 bilhões de tentativas de ataques cibernéticos em 2022, ficando apenas atrás do México, com 187 bilhões. De acordo com o levantamento, os ataques de phishing aumentaram 226%, em comparação com o

último semestre de 2021. Os ataques de ransomware passaram a ser cada vez mais direcionados e as empresas não estão devidamente preparadas para enfrentar esse tipo de ameaça. Ransomwares, trojan bancários e RATs são as ameaças mais utilizadas por cibercriminosos para afetar os dispositivos móveis. As vulnerabilidades mais detectadas estão relacionadas a produtos Microsoft, com falhas descobertas há mais de cinco anos atrás.

Empresas nacionais também tem se tornado estatística e notícia todos os dias, segundo informações do IBRASPD, afetando a sua confidencialidade, integridade ou disposição. Bilhões de dados são expostos todos os dias. O modus operandi dos criminosos segue uma sequência de ações: eles entram/invadem a empresa, fazem um processo de enumeração para conhecer profundamente as suas características e funcionamento; fazem o processo de exfiltração; roubam o máximo de dados possível; entram com um coquetel molotov, o chamado ransomware. “Depois disso todos os dados já foram vazados. E é muito comum que isso aconteça em diversas empresas. Depois começa também o processo de extorsão, de ameaças, a fim de obterem o pagamento de um resgate", advertiu

Pedidos de resgatem sobem 20% em um ano, para US$ 600 mil. O cibercrime é uma preocupação global. É o 5° maior risco discutido. Seu custo supera os US$ 12 trilhões em 2024. Em 2023, o lucro do crime foi US$ 9 trilhões. Se comparado com as grandes potências, o cibercrime seria a terceira potência mundial, no que diz respeito ao faturamento. “Cibercriminosos estão se associando a funcionários para atacar empresas. Profissionais mal pagos podem parar na dark web. E a Inteligência Artificial foi utilizada em mais de 50% dos ataques recentes contra empresas brasileiras”, declarou. Em conclusão, o palestrante falou sobre como um incidente pode impactar a carreira de um CISO e deixou esse ponto como reflexão para os expectadores.

Marck Rodrigues de Sá abordou os seguros para riscos cibernéticos, a exposição das empresas e a necessidade de contratar uma apólice de seguros. O seguro de risco cibernético nasceu no Brasil para atender a demanda das empresas que estavam cada vez mais dependentes de sistemas de dados, muitas delas engatinhando em suas medidas de segurança e políticas de proteção de dados. "Identificamos que havia um nicho a ser explorado, que poderíamos oferecer uma proteção adicional para as empresas", contou.

As empresas estão sujeitas a diversos incidentes cibernéticos, desde extorsão até eventual interrupção de serviços, necessidade de contratação de um especialista em gestão de crise no momento de um incidente cibernético, multas governamentais e responsabilidade perante terceiros, em caso de vazamento de informações de algum cliente ou fornecedor. “O seguro surgiu com o objetivo de proteger a própria empresa e para oferecer cobertura para terceiros. Ele tem um papel crucial. É mais uma camada de proteção”, adicionou.

Outros pontos abordados pelo executivo foram análise de risco, a dependência da empresa de fornecedores críticos que ofereçam risco e possam, por consequência, causar um evento cibernético, não apenas em uma empresa, mas em uma gama de companhias de um mesmo setor da sociedade ou de um país, e impactar de maneira sistemática a todos.

Para executar seu trabalho de maneira eficiente, as seguradoras contam com equipe de riscos interna, profissionais especializados em risco cibernético e em tecnologia. Realiza entrevistas (assessment risk) com as empresas tomadoras, para identificar as medidas de segurança que já estão em vigor, assim como pontos de melhoria. Sugere plano de ação e disponibiliza relatórios internos para que as empresas possam trabalhar na melhoria de suas políticas de gestão de dados. "Também temos trabalhado para ampliar a oferta de serviços, oferecer campanhas de phishing, realizar treinamentos dentro das empresas, entre outros serviços, para trabalhar em parceria com as empresas que buscam o seguro para esse risco que é tão atual na nossa sociedade”, pontuou.

O painelista defende que a ideia do seguro é trazer tranquilidade para as empresas, um suporte financeiro, para que a seguradora possa apoiar o cliente em caso de sinistro. Para o caso de ele ter um incidente cibernético e todas as outras medidas de segurança e política de gestão de dados falhar. Mark falou ainda de uma figura muito importante além do CISO, que é a do Data Protection

Officer (DPO), responsável pela proteção de dados nas empresas.

O profissional precisa ter vasto conhecimento da regulamentação do setor, que sofre constantes mudanças. Também precisa circular muito bem dentro da organização e identificar as medidas de segurança que precisam ser implementadas nas diferentes áreas, para que ele possa atuar em conformidade. Além disso, tem que gerir múltiplas tarefas simultaneamente para implementar o máximo de medidas de segurança possíveis, dentro do orçamento e da capacidade empresa, para coibir a exposição a riscos cibernéticos.

“O DPO precisa atuar na companhia com muita autonomia, independência e sem conflito de interesse, devido a todos os riscos com os quais ele está envolvido. Acima de tudo, ele precisa do apoio da empresa, por meio de ferramentas tecnológicas, recursos financeiros, políticas de segurança, entre outros, para que ele possa implementar essas medidas e criar dentro da companhia uma cultura de gestão de dados”, esclareceu.

Já o gestor de riscos e seguros do Ifood, **Thiago Amorim**, falou sobre os desafios na contratação de uma apólice de seguro cibernético. Segundo ele, o programa de cyber security foi implementado na empresa há seis anos, mas até hoje ele não conseguiu contratar a apólice desejada. Atualmente, o Ifood faz 110 milhões de entregas mensais para 45 milhões de usuários. O caixa da empresa movimenta R$ 6 bilhões por semana. Cerca de 350 mil entregadores estão ativos em uma base de mais de 2 milhões de pessoas. A empresa tem 400 mil estabelecimentos parceiros (farmácia, supermercados, restaurantes e Fintechs). "E quando me sento para negociar com as seguradoras eles se assustam bastante com o tamanho da empresa e com os balanços financeiros”, argumentou.

Periodicamente, Amorim e sua equipe fazem roadshows por diversos países, a fim de mostrar as medidas de proteção, a base de gestão de riscos implementada, com o objetivo de minimizar os riscos e conquistar o limite desejado. O executivo destacou a importância do trabalho das grandes corretoras e da área interna da empresa para calcular o tamanho da exposição ao risco e apontar os principais caminhos. Em sua visão, os questionários das seguradoras também foram bastante aprimorados nos últimos anos, conferindo precisão e rapidez na coleta de informações.

Em sua fala, o executivo salientou a dificuldade de colocar o tamanho do risco de exposição da empresa. Isso porque, para a maioria das seguradoras, as fintechs já são um risco declinado e, quando além de ser uma fintech a empresa é uma adquirente, fica ainda mais difícil.

"Em contrapartida é uma minoria das empresas de tecnologia que sofrem cyber attacks. Porque isso é o core business do nosso negócio. Estamos olhando e atentos a essas questões o tempo inteiro. O time e os diversos CISOS do Ifood desenvolvem constantemente modelos de Inteligência Artificial que nos auxiliam na missão de prover a primeira camada de segurança", reforçou. O gestor considera fundamental que a gestão de risco cibernético faça parte da cultura da empresa e que todos os colaboradores que estejam no organograma e façam parte da gestão de risco, assim como todos os funcionários, consigam rodar todos os modelos.

Painel 2 - Legislação de Inteligência Artificial e a Responsabilidade Civil

Fernando Nery teve a missão de falar sobre os desafios da multidisciplinaridade, que é pouco regulamentado no país. O Brasil ainda não tem regulamentação em agência de segurança cibernética, de Inteligência Artificial, de aposta online ou de passagem de responsabilidade para os fornecedores. “Um ponto que é importante é que você pode fazer a convergência da conformidade. Você tem uma espinha dorsal e esse modelo atende a diferentes formas de regulamentação”, comunicou.

A legislação de Inteligência Artificial tem uma série de definições, é baseada em direitos fundamentais. No artigo primeiro do projeto de lei consta o termo direitos fundamentais, assim como na LGPD. “Trata-se de uma lei de direitos fundamentais e que promove e exige essa questão da multidisciplinaridade. Exige que você tenha a visão multidisciplinar para que se aplique o direito

fundamental em um ambiente tecnológico", explicou.

Na visão de Nery, existe hoje uma grande confusão. As organizações têm dificuldade de identificar as diferenças e as semelhanças entre a gestão de incidente cibernético e a gestão de incidentes com dados pessoais. E esses pontos são importantes quando da criação de um processo multidisciplinar. Outro tópico abordado pelo painelista foi a conformidade a partir de equipes multidisciplinares. O modelo interdisciplinar considera que haja diversas pessoas. "Ter uma equipe multidisciplinar é um grande desafio. Um desafio organizacional e de pessoas. O maior desafio na segurança cibernética é o ser humano. A gente avalia isso na hora que vai olhar a responsabilidade civil, o seguro, porém existem os modelos de implementação de governança", sinalizou.

Nery defende que as pessoas sejam preparadas para deixarem de ser o elo mais fraco, porque organizações que conseguem conscientizar e engajar as pessoas fazem de suas equipes a principal barreira de segurança. Caminhando para o final de sua palestra, o executivo compartilhou um exemplo de framework de implementação que considera cinco elementos: inventário, resposta, monitoramento, gestão e governança. "Ressalto que é a gestão integrada de riscos que que possibilita realmente ter uma visão ampla. E esse é o grande desafio da Inteligência Artificial, fazer gestão de risco", acrescentou.

O advogado Dr. **Marcos Gomes** da Silva Bruno veio com a proposta de trazer uma abordagem prática do tema, contextualizar o momento em que estamos vivendo, mostrar um pouco do quanto a inteligência artificial está presente no nosso dia a dia e como é possível diminuir os riscos. "Os dados estão cada vez mais presentes no nosso dia a dia. Obviamente, eficiência é uma necessidade. E ao contrário do que ocorria antigamente, quando o departamento jurídico muitas vezes era encarado como centro de custos, hoje a área já se posiciona como centro de receita e de resultado para a empresa", expôs Gomes, acrescentando que dentro de áreas específicas do escritório de consultoria relacionadas a processos, há melhoria de departamentos jurídicos.

Hoje são realizados trabalhos incríveis com os departamentos jurídicos para gerar eficiência. E tudo isso, o uso de dados, a eficiência, seja no mercado de seguro ou em qualquer outro mercado, está muito ligado à Inteligência Artificial, porque ela confere a possibilidade e a capacidade de processar esses dados com muito mais rapidez. Para exemplificar, o advogado compartilhou alguns cases de IA como ferramenta de negócios no ramo de seguros, relacionados a análise de risco, subscrição automatizada, detecção de fraudes, principalmente no seguro saúde, gestão de sinistros e marketing personalizado.

A Inteligência Artificial nos traz alguns desafios éticos, a questão de viés e discriminação, transparência e explicabilidade e ainda manipulação de comportamento. Além dos desafios éticos existem também os desafios legais. "Como eu disse no início, não temos uma lei específica, relacionada à Inteligência Artificial, mas isso não significa que nós podemos fazer o que quisermos, porque existem leis que se aplicam", salientou. Há uma regulamentação em evolução, existe responsabilidade civil por lei e uma farta regulação específica que trata de privacidade e que tem muito a ver com inteligência artificial.

Por fim, o advogado compartilhou cases de responsabilidade civil relacionados a LGPD, falou sobre o PL 2338/23, que dispõe sobre o uso da Inteligência Artificial, e ainda sobre governança. "O texto do PL tem, sem dúvida, algumas provisões e determinações bastante pesadas para essa indústria. Porém é extremamente necessário que nós tenhamos regulação", advertiu.

Durante sua fala, **Henrique Volpe** falou sobre a criação e a evolução da KaKau Seguros, empreendedorismo no Brasil e tomada de risco. "Quando começamos a KaKau, em 2017, éramos um MDA. Ou seja, fazíamos tudo o que uma seguradora deveria fazer no meio digital e subscrevíamos para os parceiros. Começamos com a Generaly, depois fizemos parceria com a score e a fomos evoluindo, sempre com foco em tecnologia", relembrou.

No início, a empresa fazia seguro de celular e de bicicleta. Também fez alguns White labels específicos, alguns riscos pequenos, porém corporativos. Em 2021 a Kakau recebeu sua primeira

premiação. Porém, o ano histórico para a empresa foi o de 2022, quando recebeu a autorização da SUSEP, a licença sandbox. No mesmo ano, seus sócios criaram a Kakau Tech, uma empresa de tecnologia, para atender a demanda de parceiros que estavam em busca da tecnologia que a empresa vende no processo SAS. “Embora estejamos falando muito aqui de mitigar risco, controle de risco, eu estou indo mais para a linha de tomar risco. O empreendedor no Brasil por definição é um grande tomador de risco e pagador de impostos”, frisou.

Segundo **Volpe**, a empresa começou a licenciar essas tecnologias e foi a primeira startup na América Latina, segundo a XL a ter um seguro ciber em meados de 2018. A visão da companhia é a de que a seguradora do futuro é uma empresa de serviços tecnológicos, principalmente, e que por acidente vende de algum tipo de apólice. Então cada vez mais o “tech” vai ser o drive dessa conversa com o cliente, seja ele corporativo ou pessoa física. E junto com esse serviço, com essa tecnologia, com mitigação de risco e controle vem uma apólice de seguro adequada a necessidade e a realidade do segurado.

De acordo com o Market-sizing Model da Mckinsey, o mercado de Embedded Finance (conceito que permite que empresas não financeiras ofereçam serviços financeiros aos seus clientes) alcançou receitas de R$ 20 bilhões em 2021. “É uma indústria gigantesca e esse é o único canal onde estamos vendo crescimento, cada vez mais digital. Então, essa preocupação com o tratamento de dados perante a lei ou perante a segurança dos clientes vai ser uma constante dentro das seguradoras”, complementou. É nesse cenário que as empresas vão buscar soluções para conviver com a inteligência artificial, entender até onde vão tomar risco e os possíveis impactos para o cliente. “O recado final que eu quero reforçar a todos é que empreendam”, recomendou.

Painel 3 - Responsabilidade Civil e os Danos Causados pelas Enchentes no Rio Grande do Sul

“Em se tratando de responsabilidade civil, como melhor imputar ou não imputar culpa pelos prejuízos causados pelas enchentes, sem precedentes, ocorridas no Rio Grande do Sul? Poderia o caso fortuito ou a força maior serem utilizados como excludente de responsabilidade em todos os cenários de responsabilização, questionou a mediadora do terceiro painel, Dra. Daniela Benes. Para ela, a boa doutrina da responsabilidade civil - que tem suas bases históricas no milenar direito romano e no direito francês, ainda é a mais prudente e correta forma de se reestabelecer com segurança a confiabilidade dos vínculos contratuais e extracontratuais no Estado do rio Grande do Sul. Ajustadas estas relações, o mercado segurador poderá atuar e oferecer coberturas adequadas aos novos tempos e novos riscos. “O nosso painel tem essa característica de ir lá no Rio Grande do Sul, enxergar o que está acontecendo lá e ver de que forma podemos ajudar daqui para frente em termos de responsabilidade civil”, disse a mediadora Dra. Daniela Benes.

O primeiro painelista, o **Professor Carlos Pianovski,** convidou os expectadores a refletir sobre os desafios que a situação trouxe para o âmbito da responsabilidade civil, tanto nas relações contratuais como nas extracontratuais. Pessoas e empresas não puderam pelos mais diversos motivos cumprir contratos, coisas pereceram em mãos de terceiros, adimplementos contratuais foram postergados, outros contratos tiveram que ser extintos/resolvidos por absoluta possibilidade de continuidade. A atividade econômica de forma quase que geral foi aniquilada.

“Quais as respostas que o direito pode oferecer? Focado mais na responsabilidade contratual, o Professor mencionou que há a necessidade de diferenciarmos duas situações que são básicas dentro da teoria do inadimplemento e que tem uma importância prática óbvia. A primeira é aquilo que no juridiquês chamamos de mora, e a segunda aquilo que chamamos de inadimplemento definitivo”, salientou. E dentro deste tema, trouxe a reflexão as causas que afastam o dever do cumprimento contratual, sendo elas o caso fortuito e força maior. Estas duas excludentes podem, perfeitamente, serem invocadas para os casos envolvendo as enchentes do Rio Grande do sul, mas há de se ter certa parcimônia e cuidado, disse o Professor.

O segundo painelista, **Rodrigo Cardona Ueda** trouxe para a o foco da discussão o que viu e o que presenciou quando atuando na regulação dos sinistros que envolveram as enchentes. Ressaltou a

importância das apólices de responsabilidade civil no contexto, e como a partir disso deve o mercado segurador reagir a eventos futuros.

Concluindo o ciclo de painéis, **Silvia Esperanza** foi encarregada de trazer o olhar da indústria de seguros, de mostrar ao público como o mercado segurador está se portando em termos de aceitação de riscos e fixação dos prêmios. “A primeira coisa que fizemos naquele momento foi a criação de um comitê humanitário para tentar suprir e criar situações para que pudessem ajudar nossos irmãos do Sul com toda aquela catástrofe. O mercado segurador de uma certa forma ficou bastante assustado com aquilo, porque aqui no Brasil catástrofes climáticas são incomuns”, analisou.

Foram 478 municípios afetados pelas enchentes e o setor não tem o mapeamento de perdas numa região tão grande. “Quando a gente vai olhar o que tem de fato de perdas em relação a possíveis indenizações o número chega a 3.9 bilhões, o que corresponde a cerca de 30% do valor total do prejuízo. O percentual mostra como a penetração do seguro ainda é baixa em determinadas regiões”, alertou

Na Marsh, especificamente, houve apenas 204 sinistros. Desse total 84 ficaram abaixo da franquia e apenas 08 sinistros são sinistros de responsabilidade civil reclamados até agora. E desses sinistros de RC reclamados, a maior parte deve ter uma exclusão por caso fortuito ou força maior. “O mercado vem reagindo positivamente aos eventos climáticos e globalmente o mercado já está muito preparado para esse tipo de coisa. Em breve teremos uma evolução aqui no Brasil também e isso já começa a aparecer nos nossos relatórios de taxas”, concluiu.

Após o final de cada palestras foi aberto o espaço para as perguntas da plateia e os debates dos palestrantes.

Assista ao VI Encontro Nacional de Seguro de Responsabilidade Civil na íntegra no canal da AIDA Brasil no Youtube:
https://www.youtube.com/watch?v=YAm3H9ZG4Io

Fonte: Oficina do Texto, em 28.11.2024