Editor-Chefe: Guilherme Kolling
guilhermekolling@jornaldocomercio.com.br
Editora de Economia: Fernanda Crancio
fernanda.crancio@jornaldocomercio.com.br
Editora-assistente: Cristine Pires
cristine.pires@jornaldocomercio.com.br
Diagramação: Gustavo Van Ondheusden e Ingrid Muller

Opinião

Quanto vale para uma companhia uma informação de negócio trazida da área de TI?

Paulo Alonso
COO da Delfia

Temos um cliente, gigante do varejo, que com nossas informações de TI transformadas em dados de negócios, conseguiu salvar uma média diária de R$ 6 milhões em vendas que poderiam ser canceladas. Hoje, esse tipo de informação é muito útil para o varejo, principalmente em e-commerce e outras plataformas de venda, já que é a forma mais rápida de mostrar a eficiência desse serviço: são vendas que passam por múltiplas plataformas e com nossa expertise, enxergamos toda sua jornada.

Para continuar apurando dados de forma preditiva, é preciso investimento para aumentar a operação e traduzir esses dados em KPIs e aproximação de negócios. As companhias percebem a importância da informação que a TI traz e começam a enxergar essa área com outros olhos e a entender como ajudar e a investir, para acelerar toda a cadeia de negócios.

Exemplos que acontecem nas vendas on-line do varejo, como uma interrupção em algum canal que ficou parado por três minutos e isso gerou uma rentabilidade menor para o negócio, é o tipo de situação que não pode mais acontecer.

Sabemos que o SLA (Service Level Agreement) indica as boas práticas e o tempo de atendimento na contratação dos serviços oferecidos em TI, e que o ITIL otimiza a operação e gerencia o nível de serviço entregue ao cliente de forma eficiente. A experiência do usuário também é importante e assim, o mercado criou um KPI chamado XLA, no qual as empresas medem a satisfação do cliente com o atendimento que lhe é prestado. ITIL e XLA são reconhecidos como essenciais para manter o bom funcionamento das operações.

No entanto, é importante que o consumidor esteja satisfeito, é o mínimo que sua expectativa seja superada positivamente, pois não basta somente atendê-lo no prazo determinado, é preciso atendê-lo bem. É algo óbvio, mas muitas empresas ainda pecam nessa questão. Com uma boa gestão de processos de TI para que a operação continue girando, comecei uma movimentação na organização onde sou COO para mudar o conceito de serviços oferecidos ao cliente. Não queremos apenas oferecer serviços, mas sim, informações de negócio, que são verdadeiramente úteis, relevantes e influentes, que podem alavancar ou salvar vendas em diversas áreas. Transformamos dados em insights essenciais para que os clientes possam utilizá-los internamente, resultando em mais investimentos na área de TI.

Redesenhamos as operações em serviços gerenciados, fortalecemos a área de Governança para padronizar e reunir os dados que são processados, para então tratarmos o que é importante e assim selecionarmos e transformá-los em KPI de negócio. Acompanhamos toda a jornada das operações padrões junto aos profissionais de observabilidade, que monitoram os ambientes digitais e nos trazem essas informações. Nosso DNA em observabilidade nos ajuda na entrega desse serviço como um diferencial para o mercado, além de ser atrativo.

Trouxemos uma profissional de Experiência & Operações de Tecnologia para que hoje e lá na frente - ainda há um grande investimento a ser feito –, essa área possa ser um diferencial para qualquer cliente. Além da operação de TI usual, ele passa a ter informações valiosas de negócios.

Como uma empresa de curadoria de jornadas digitais, sabemos o que temos de praticar dentro de qualquer operação, o básico bem-feito. Para todos os serviços que oferecemos, procuramos sempre agregar ao cliente sem que ele nos peça. E para o mercado, não basta mais fazer muito bem a mesma coisa durante muito tempo, é preciso fazer muito bem, mas, inovar constantemente. A ideia é não ofertar mais uma operação, mas sim, uma informação precisa para escalar negócios e trazer investimentos também. Em algum momento, vão entender que isso é importante para o mercado.


DELFIA/DIVULGAÇÃO/JC

É importante que o consumidor esteja satisfeito, é o mínimo que sua expectativa seja superada positivamente, pois não basta somente atendê-lo no prazo determinado, é preciso atendê-lo bem

O tripé para vencer a fraude

Carlos Vieira
Fraud Prevention Manager da Topaz

O cenário dos negócios e serviços cada vez mais conectado, ocasionado pela transformação digital e avanço da digitalização no Brasil, mostra às empresas a necessidade de discutir constantemente formas de prevenção de riscos, de estratégias eficazes contra ataques e de proteção para fortalecer a segurança cibernética. O Brasil é considerado um dos mercados mais complexos em relação à prevenção à fraude, mas também é um dos mais avançados e uma referência em inovações e em tecnologias para a cibersegurança. O crescimento das fraudes digitais no país cresceu estratosfericamente, de acordo com o levantamento global sobre Tendências de Fraude Digital Omnichannel realizado pela TransUnion em 2023: as tentativas de fraude digital aumentaram 80% globalmente desde 2019.

O panorama de ataques no Brasil se arrasta desde os anos 2000, quando em 2002, o phishing tornou-se comum para roubar credenciais de usuários e invadir contas de clientes em instituições financeiras, assim como o surgimento de malwares em 2004. De lá para cá, foram anos da ascensão de RATs (Remote Access Trojans) – inclusive nos dispositivos móveis, das "falsas centrais" com o crescimento de relatos de ataque por meio de sistemas de telefonia, até a transformação digital, com milhões de pessoas entrando no sistema financeiro, sua evolução e o lançamento do Pix, a massificação do uso de Inteligência Artificial em técnicas para burlar autenticação facial, a "laranjização" e a lavagem de dinheiro por meio de Bets.

Para toda essa avalanche de ameaças há mecanismos e tecnologias avançadas de prevenção de riscos para identificar e mitigar vulnerabilidades e proteger transações para evitar a manipulação de consumidores. Mas, a prevenção à fraude precisa de três pilares para que a segurança digital de fato aconteça: prevenção, que requer a adoção de tecnologias emergentes para proteções adequadas, como análise em tempo real, análise comportamental de usuários, bloqueio de ligações suspeitas, autenticação adaptativa; conscientização, para educação contínua de usuários sobre prevenção e segurança digital, orientação para denúncias de atividades suspeitas, campanhas em mídias sociais, alertas em tempo real durante e jornada e conscientização sem atritos; e repressão, para reprimir crimes cibernéticos, denúncias com rapidez, colaboração entre instituições financeiras, implementação de leis rígidas e aplicação e cumprimento da lei.

Além dos três pilares, outras iniciativas buscam combater atos ilícitos. No ano passado, a Resolução Conjunta Nº 6 emitida pelo Banco Central é uma inovação que fez com que o mercado financeiro colaborasse entre si rumo a um sistema avançado e mais robusto de segurança. Adicionalmente, a identificação de contas laranja está evoluindo junto às instituições, que usam de análise comportamental e de conexões financeiras para identificação de padrões de contas suspeitas para definição do perfil de laranjas, além de cooperação e compartilhamento de informações.

Também, a combinação de tecnologias de ponta com estratégias eficazes de prevenção de riscos são fatores importantes para combater essas ameaças. O mercado financeiro está repleto de soluções de prevenção à fraude e lavagem de dinheiro, que garantem a proteção necessária em transações e segurança de operações. Em todo tipo de transação que possa ser processada pelo sistema financeiro, por exemplo, há diversos aspectos que são calculados, como o uso de algoritmos de inteligência artificial, para entregar informações de riscos e ameaças em tempo real e permitir que o cliente tome uma decisão, seja de bloquear ou liberar aquele procedimento.

Outras soluções baseadas em inteligência artificial - e que empregam tecnologia sofisticada - garantem a integridade de cada transação e incorporam soluções avançadas antifraude e de combate à lavagem de dinheiro – estes dois conceitos estão intimamente relacionados à fraude. É comum no mercado dizer que 99% das fraudes são seguidas por uma atividade ilícita de lavagem de dinheiro.

A IA é uma ferramenta poderosa para combater atos fraudulentos, com aplicações que se utilizam massivamente de algoritmos de machine learning para empregar identificação de anomalias transacionais, comportamento e de habitualidade dos usuários, além de redes neurais, deep learning e técnicas para validações gerais. Nada é 100% seguro, contudo, estar um passo à frente do cibercrime é o que organizações, governos e grupos continuam fazendo, por meio de um processo robusto de sensibilização, identificação e prevenção de atos ilícitos, cooperando entre si e integrando tecnologias com velocidade para um bem maior: uma sociedade mais segura. Tentativas de fraude devem ser denunciadas, para que nenhum amigo, familiar ou nós mesmos sejamos vítimas de algum crime cibernético.