Integração da gestão de riscos cibernéticos nas três linhas de defesa

Sergio Kogan e Henrique Quaresma (*)

É fato que a preocupação em relação aos riscos cibernéticos ganhou a atenção da Alta Administração de muitas empresas e dos governos, especialmente com a grande cobertura que a mídia tem dado para o assunto, como por exemplo o caso do WannaCry ocorrido em maio de 2017

De acordo com relatório "The Global Risks Report 20181", desenvolvido anualmente pelo Fórum Econômico Mundial, Ataques Cibernéticos é o 3º risco em termos de probabilidade, seguido por Roubo ou Fraude de Dados (4ª posição) que também tem relação direta com a segurança cibernética. Em 2016 o risco de ataques cibernéticos não constava no Top 10.

Adicionalmente, os órgãos reguladores no mundo todo têm promulgado leis, regulamentos e orientações que endereçam essa preocupação em relação ao tema segurança cibernética. Como exemplo, o Banco Central do Brasil (BACEN) publicou no último dia 26 de abril a resolução 4.658 que determina que as Instituições Financeiras brasileiras devem definir e implementar uma política e medidas de proteção cibernética, além de monitorar e gerenciar os incidentes cibernéticos.

Desafio de gerenciar os riscos cibernéticos

Em diversas organizações no Brasil o tema segurança cibernética é delegado à área de Tecnologia da Informação (TI), uma vez que o componente tecnológico é visto como o principal mecanismo de proteção a ser implementado e gerenciado. Outro fator que contribui para o foco tecnológico da gestão dos riscos cibernéticos é o desconhecimento dos executivos da organização em relação aos riscos envolvidos e seu real impacto no negócio.

O que algumas empresas não levam em consideração é que quando ocorrem incidentes, a organização pode ser impactada de diversas maneiras. Por esse motivo, os riscos cibernéticos devem ser gerenciados como um risco de negócio, com o mesmo nível de atenção e diligência dos outros riscos corporativos.

Integrando riscos cibernéticos nas três linhas de defesa

Estabelecendo como uma premissa fundamental que risco cibernético é um risco de negócio, faria sentido utilizarmos as estruturas, metodologias, práticas e ferramentas de Gestão de Riscos Corporativos para identificar, classificar, analisar, tratar e monitorar os riscos cibernéticos?

A resposta é sim. E uma vez que a forma de gestão, e principalmente de apresentação e comunicação, dos riscos corporativos é conhecida pela Alta Administração, se torna um pré-requisito a tradução do linguajar técnico, comumente utilizado para comunicar os riscos cibernéticos, para riscos de fácil entendimento de profissionais que não possuem o conhecimento técnico em segurança cibernética, porém conhecem profundamente do negócio da organização, e como riscos podem impactar no atingimento dos objetivos estratégicos ou operacionais.

Do ponto de vista de governança de riscos, a estrutura das Três Linhas de Defesa2 (3LoD – Line of Defense) está sendo amplamente divulgada e implementada pelas organizações.

Como adotar essa estrutura para gerenciar os riscos cibernéticos de uma forma holística e integrada?

Em primeiro lugar, é importante determinar as atribuições de cada linha de defesa para que não haja sobreposição e retrabalho, especialmente no cenário atual de busca constante de otimização de custos nas empresas brasileiras.

Primeira linha de defesa

A 1ª linha de defesa é responsável por implementar e operacionalizar os controles para mitigar os riscos cibernéticos. A tradicional função de segurança de TI se enquadra nesse papel, uma vez que geralmente é responsável por implementar e gerenciar processos e soluções tecnológicas relevantes para a segurança cibernética, tais como desenvolvimento de software seguro, gestão de acessos, gestão de vulnerabilidades e atualização de software, monitoração de eventos de segurança, entre outras.

Entretanto, outras áreas da organização também possuem um papel importante na gestão de riscos cibernéticos:

- Recursos Humanos: Geralmente, os colaboradores de uma organização são o elo mais fraco para assegurar uma adequada segurança cibernética, e deve-se dar o devido nível de atenção do momento da contratação até o desligamento do colaborador. Para que isso ocorra, o departamento de Recursos Humanos deve estar alinhado e conhecer o seu papel na gestão de riscos cibernéticos;
- Suprimentos/Compras: Durante a contratação de um fornecedor, diversas atividades devem ser coordenadas pela área, em conjunto com a área contratante e com o apoio da Segurança da Informação Corporativa (2ª linha de defesa que discutiremos logo a seguir neste artigo), para assegurar que os devidos cuidados foram tomados em relação à seleção do terceiro. Uma adequada gestão de riscos de segurança da informação em terceiros (fornecedores e parceiros) deve ser definida e implementada pela organização. Você tem conforto e confiança de que os seus fornecedores e parceiros tratam a sua informação com o mesmo nível de diligência que a sua organização?

Outras áreas também possuem um papel fundamental nessa gestão de riscos cibernéticos corporativos como Segurança Patrimonial/Física, áreas de negócio e de Inovação e Digital.

Entretanto, como atuar de forma integrada e organizada?

A resposta é a 2ª linha de defesa.

Segunda linha de defesa

É responsável por definir as diretrizes e monitorar o cumprimento pela 1ª linha de defesa.

Na gestão de riscos cibernéticos, a proposição é a existência de uma função de Segurança da Informação Corporativa independente.

Cabe a essa área a responsabilidade por:

- Definir a visão, missão e estratégia para gestão dos riscos cibernéticos na organização alinhada à estratégia do negócio e apetite ao risco;
- Definir as diretrizes e suportar a 1ª linha de defesa na implementação das políticas, normas e procedimentos considerando seus papéis e responsabilidades;
- Realizar o treinamento e conscientização dos colaboradores da organização fomentando uma cultura de segurança cibernética;
- Identificar, classificar, analisar, tratar e monitorar os riscos cibernéticos;
- Apoiar na gestão de riscos em terceiros (fornecedores e parceiros) durante a seleção do terceiro e durante todo o ciclo de vida do relacionamento da organização com esse terceiro.
- Atuar na resiliência e continuidade de negócios (Plano de Continuidade Operacional, Plano de Recuperação de Desastres de TI e Gestão de Crises);
- Realizar o monitoramento dos indicadores e da conformidade da organização e dos terceiros.

Terceira linha de defesa

Por fim, a Auditoria Interna necessita de profissionais capacitados e com conhecimento técnico para realizar avaliações independentes que permeiam o ciclo completo de gestão de riscos cibernéticos. É preciso considerar os riscos cibernéticos em todas as auditorias de estratégia, governança e processos da organização e não somente das áreas de TI e Segurança.

O risco cibernético é um risco de negócio e sua efetiva gestão permeia as diversas áreas da organização. O conceito de três linhas de defesa auxilia na estruturação e definição clara dos papéis e responsabilidades de forma que a atuação seja integrada.

Não espere sua organização ser impactada por um incidente cibernético para agir. Entenda como os riscos cibernéticos estão evoluindo e afetam a sua organização, mantenha-se à frente das novas regulamentações, integre uma adequada estratégia e cultura de segurança cibernética dentro da organização, trabalhe integradamente junto aos terceiros para proteger todo o ecossistema do negócio focando nos ativos críticos que não podem ser comprometidos.

(*) Sergio Kogan é Líder em Cybersecurity da EY Brasil e Henrique Quaresma é Gerente sênior especialista em gestão de riscos cibernéticos da EY Brasil

Como a Internet das Coisas colabora para o consumo, prática e negócios do esporte

A tecnologia tem possibilitado uma infinidade de mudanças e melhorias nos esportes

Augusto Panachão (*)

Elas vão desde câmeras que conseguem captar melhor cada movimento até sensores modernos em roupas e equipamentos. Se antes um treinador precisava fazer anotações sobre as jogadas para avaliar o desempenho dos atletas, hoje, vários dados estão facilmente disponíveis para uma análise detalhada.

Além de possibilitar a avaliação dos treinadores após a competição e ajudar no parecer dos juízes durante os jogos, a tecnologia influencia na maneira que o esporte é praticado pelos atletas. Informações de saúde, como batimentos cardíacos, além da visualização dos pontos fortes e fracos do competidor podem ajudar a moldar seu treino e definir suas metas.

O uso da Internet das Coisas (IoT, na sigla em inglês) - ou dispositivos conectados por uma rede - traz diversos avanços. Na natação, por exemplo, o contador de voltas passou a ter um display embaixo d'água para facilitar a contagem em certas provas. Quando o nadador toca o touchpad na parede ao fazer sua virada, o sistema automaticamente muda o número de voltas que ainda faltam. Assim, o atleta pode se concentrar somente no nado, sem precisar levantar a cabeça para ver as placas de plástico de contagem.

No futebol, atletas estão usando um top com um dispositivo GPS acoplado, capaz de monitorar o jogador em treinos e partidas, coletando dados como distância percorrida, velocidade média e frequência cardíaca. Com essas informações, é possível saber o rendimento do jogador e, com outras informações médicas, saber quando ele tem um desempenho melhor e quando está suscetível a um desgaste ou lesão.

Na Copa do Mundo de 2014, foi inaugurado um sistema de câmeras para comprovar quando a bola cruzava a linha do gol. Os estádios foram equipados com 14 câmeras de alta velocidade focadas em capturar imagens de todos os pontos dos gols. Assim que a bola cruzava a linha, o sistema enviava a confirmação do gol imediatamente a um relógio que o árbitro usava.

A experiência de visualização das competições também atingiu outros níveis com a tecnologia. Nos Jogos Olímpicos de Inverno de 2018, por exemplo, a Intel disponibilizou mais de 50 horas de cobertura para serem vistas em realidade virtual (VR). Através de um aplicativo, era possível vivenciar, por exemplo, a velocidade e a altura das manobras de snowboard com óculos VR ou mesmo em celulares iPhone e Android.

Outro exemplo é o Tour de France, maior competição de ciclismo do mundo, que, por meio de dispositivos GPS instalados embaixo do selim de cada bicicleta, coleta dados e os combina com informações históricas e condições climáticas. A partir da análise dessas informações, gera insights em tempo real sobre a competição, como velocidade média de cada ciclista, distância entre corredores e previsões da corrida. Todas essas informações alimentam plataformas digitais para melhorar a visualização e experiência do Tour pelos fãs.

Quando se fala em assistir as competições nos locais, a IoT também muda a experiência dos espectadores. Redes Wi-Fi, sensores que incluem alarmes de segurança, termostatos, medidores inteligentes e sistemas de tickets eletrônicos tornam o prédio mais inteligente. Isso ajuda na segurança pública, no compartilhamento das experiências das pessoas nos meios digitais, nas informações recebidas pelas emissoras de televisão, e até em um consumo mais inteligente de energia do prédio, reduzindo custos.

Segundo uma pesquisa da Harbor Research, nos últimos anos, a indústria esportiva tem sido uma das principais em termos de desenvolvimento de aplicações da Internet das Coisas, e a receita gerada por essa tecnologia tende a aumentar em 2018.

Os dispositivos conectados da IoT geram mais informações disponíveis, que significam mais precisão e decisões justas nas competições, mais segurança para os espectadores, melhores treinos para os atletas e um melhor acompanhamento da sua saúde, além de experiências de compra e visualização mais satisfatórias e interessantes para os consumidores. Seja para um atleta profissional melhorar seu desempenho, para um atleta amador se motivar com seu progresso, ou para treinadores, espectadores e empresas, a evolução dessa tecnologia está mudando a prática, consumo e negócios dos esportes.

(*) É Diretor de Soluções e Tecnologia da Dimension Data, empresa global de soluções e serviços de tecnologia da informação.

TeamCulture lança plataforma

– A TeamCulture irá apresentar pela primeira vez durante a 44ª edição do CONARH, que acontece entre os dias 14 e 16 de agosto na São Paulo Expo. A plataforma é uma metodologia ágil para a gestão e engajamento de clima e cultura organizacional, baseada em 10 métricas de satisfação: Relacionamento com a equipe, Vestir a camisa, Felicidade, Crescimento Pessoal, Bem estar, Feedback, Relacionamento com o gestor, Reconhecimento, Satisfação e Alinhamento. Com mais de 120 perguntas em seu banco de dados, a ferramenta permite uma avaliação contínua de equipes, o que viabiliza a antecipação de cenários e garante agilidade para resolução de problemas.

A ferramenta é gratuita para análise de uma equipe de até 10 pessoas e possui 5 formatos de perguntas, desde múltiplas escolhas até matriz dentro de uma escala.

De acordo com Rafael Bueno, CEO da TeamCulture, a nova solução surge como uma forma de imprimir velocidade da tomada de decisão baseada em evidência. "Em uma era de Big Data, mais do que informações, as companhias precisam de soluções inteligentes que facilitem a mudança de rota ou antecipe cenários para uma movimentação, tornando-as mais competitivas e ágeis. O produto da TeamCulture tem o objetivo de questionar os colaboradores e levantar informações para agir e evoluir, por meio de métricas mundialmente reconhecidas", pondera (www.teamculture.com.br.).

News @TI

TCU disponibiliza nova ferramenta para consulta à lista de contas irregulares

@O Tribunal de Contas da União (TCU) criou e disponibilizou no Twitter um robô com inteligência artificial que interage com o cidadão por meio de mensagens de texto, prestando informações sobre a atuação da Corte de Contas. A solução é uma iniciativa pioneira no âmbito da administração pública federal. O objetivo é utilizar a tecnologia para facilitar o acesso à lista, de forma prática, rápida e simples, e oferecer ao eleitor mais uma maneira de obter informações necessárias para o pleno exercício da cidadania (@TCUoficial).

QuickBooks Online

@A Intuit, multinacional de soluções para gestão financeira de pequenas empresas e profissionais autônomos, confirma a comercialização da versão brasileira do QuickBooks Online, a solução mundialmente reconhecida como líder para a gestão financeira de pequenas empresas. O sistema oferece funcionalidades gerenciais e contábeis para que os empreendedores façam a gestão das finanças dos seus negócios de maneira mais prática e de acordo com a conformidade fiscal. Um dos principais atrativos deste novo produto é o controle de estoque, que ajuda na avaliação de estoque mostrando quais produtos estão em falta e quais estão no estado de alerta sugerindo, assim, novas compras. Durante a gestão, ainda é possível separar os itens que são para venda e outros que são para escritório, por exemplo, que não necessitam de novas aquisições em curto prazo, mas que precisam ser classificados como custos do mês na empresa. O cadastro de produtos é feito por um de código para cada SKUs ou por kits (quando tem mais de um produto dentro de um item) (www.quickbooks.intuit.com/br.).

MicroStrategy Symposium 2018

@A MicroStrategy® Incorporated, líder mundial no fornecimento de plataformas analíticas e software de mobilidade, traz mais uma vez para Brasil o MicroStrategy Symposium, que acontece anualmente em mais de 20 cidades em todo mundo. Em duas edições, no dias 21 de agosto, em São Paulo e 30 de agosto, em Brasília, o evento tem por objetivo mostrar como as inovações digitais e tecnologias móveis ajudam a enriquecer os insights por toda a organização. Neste ano, o viés de negócios do São Paulo Microstrategy Symposium será reforçado com a presença do economista e apresentador da Globo News, Samy Dana. Com o tema "Econodata: a ciência além dos dados", o palestrante, além de apresentar perspectivas e tendências do cenário político-econômico do Brasil, procurará desmistificar a ideia de que os dados por si só bastam e a importância de estudá-los e bem entendê-los (https://www.microstrategy.com/us).