Como comunicar riscos tecnológicos a pessoas sem conhecimento técnico

Ajudando as empresas a entender resultados fracos

Frequentemente, profissionais de tecnologia bem-intencionados tentam explicar os riscos para suas empresas e não conseguem atingir os objetivos. Esses profissionais entendem completamente o estado do ambiente de computação e a importância de protegê-lo. Eles podem até ter uma confirmação de terceiros relevantes de suas crenças através do Instituto Nacional de Padrões e Tecnologia dos EUA (NIST), da Organização Internacional de Padronização (ISO), COBIT® ou outros padrões e estruturas. No entanto, eles não conseguem motivar seus colegas sem conhecimento técnico a reconhecer a importância do que estão tentando comunicar.

Falhas na comunicação foram estudadas exaustivamente e estão incluídas em qualquer curso introdutório sobre o assunto. Para identificar as razões da falha na comunicação do risco da tecnologia, em particular, o conhecimento relacionado à segurança cibernética deve ser temporariamente deixado de lado para explorar o que faz a comunicação em geral funcionar bem e o que faz com que ela falhe.

Jack Freund, Ph.D., CISA, CRISC, CISM, CISSP
É a principal voz em medição e gerenciamento de riscos cibernéticos. Ele é co-autor de um premiado livro sobre quantificação de riscos cibernéticos e possui doutorado em sistemas de informação. Freund é um membro da Associação Internacional de Profissionais de Privacidade (IAPP) e parceiro de privacidade de informações do Instituto FAIR. Em 2018, ele recebeu o Prêmio de Corpo de Conhecimento Comum John W. Lainhart IV da ISACA e o Prêmio de Especialista FAIR do Instituto FAIR.

Modelos de comunicação

Nenhuma pesquisa de comunicação seria completa sem a revisão do modelo seminal proposto por Aristóteles.[1] Esse modelo possui três partes: o remetente, a mensagem e o destinatário. O mais importante é o destinatário, que finalmente determina se a comunicação ocorreu. Este modelo simples identifica pelo menos uma parte da falha na comunicação de riscos tecnológicos. Na ausência da recepção da mensagem pela equipe executiva, a comunicação não pode acontecer, quaisquer que sejam as intenções.

No contexto da tecnologia da informação, é apropriado considerar o modelo clássico de teoria da informação de Claude Shannon, publicado em 1948.[2] Shannon aplicou a teoria matemática às comunicações, levando a conceitos como a razão sinal-ruído. De fato, a parte de ruído do modelo pode ajudar a explicar problemas na comunicação de riscos tecnológicos. Os executivos de negócios têm tantas prioridades conflitantes que muitas vezes é difícil para os profissionais de tecnologia superar o ruído e expressar sua opinião. O gerenciamento de negócios é basicamente o gerenciamento de riscos; portanto, para que uma mensagem relacionada à segurança tenha efeito com os tomadores de decisões, ela precisa competir com risco de mercado, risco de crédito, risco competitivo, risco regulatório, risco regulatório, risco de conduta, risco de reputação e todas as outras formas de risco operacional . Numerosos relatórios indicam que os executivos consideram a segurança cibernética uma prioridade, portanto, claramente, eles não a ignoram.[3,4,5] No entanto, o grande número de coisas ruins rotineiramente trazidas à atenção dos profissionais de TI ofusca suas experiências. Na verdade, quando os executivos avaliam essas calamidades em potencial contra incidentes reais, muitos deles concluem que os profissionais de TI são

propensos ao detalhamento ou prognóstico que nunca acontece (medo, incerteza e dúvida [FUD] em outras palavras).[6,7,8]

> "A MENSAGEM SE DISPERSA QUANDO DIVERSOS ASSUNTOS CONSIDERADOS CRÍTICOS SÃO COMUNICADOS, MAS RARAMENTE RESULTAM EM PROBLEMAS OU INCIDENTES REAIS."

Raramente alguém diz claramente aos profissionais de TI que eles não são levados a sério. Em vez disso, esses profissionais precisam interpretar o feedback que recebem. Assim, o modelo de comunicação moderno difere do modelo de Shannon, pois contém um loop de feedback explícito (**figura 1**).[9]

Os executivos de negócios empregam profissionais de tecnologia para identificar problemas e levantar questões importantes. Se todos os problemas de tecnologia forem tratados como críticos, o resultado pode ser apatia. A mensagem se dispersa quando diversos assuntos considerados críticos são comunicados, mas raramente resultam em problemas ou incidentes reais. Os executivos certamente sabem que coisas ruins podem acontecer e podem até ter colegas de outras organizações ou setores que tiveram tais resultados, mas provavelmente têm pouca experiência pessoal. Os executivos querem melhores informações sobre o risco cibernético, mas geralmente assumem que o problema é tão complexo que mesmo as pessoas que contratam para lidar com ele são incapazes de melhorar o cenário.

Os executivos tendem a entender os sistemas que precisam estar on-line para atender seus clientes e os sistemas que causam transtornos aos reguladores. No entanto, a experiência diz que, mesmo que ignorem as coisas críticas que estão fora do lugar, nada de ruim acontecerá.

Muitas vezes, as mensagens sutis e não tão sutis dos executivos são mal recebidas pelos profissionais de tecnologia. Em vez de mudar a mensagem para garantir que o destinatário a entenda melhor (transmitindo a mensagem em termos de interesse), os profissionais de tecnologia podem se tornar arrogantes e secretamente desejar um incidente de segurança para provar que estão certos. Esse dilema pode obrigar os profissionais de TI a enviar aos tomadores de decisão artigos sobre coisas ruins que aconteceram em outros lugares.

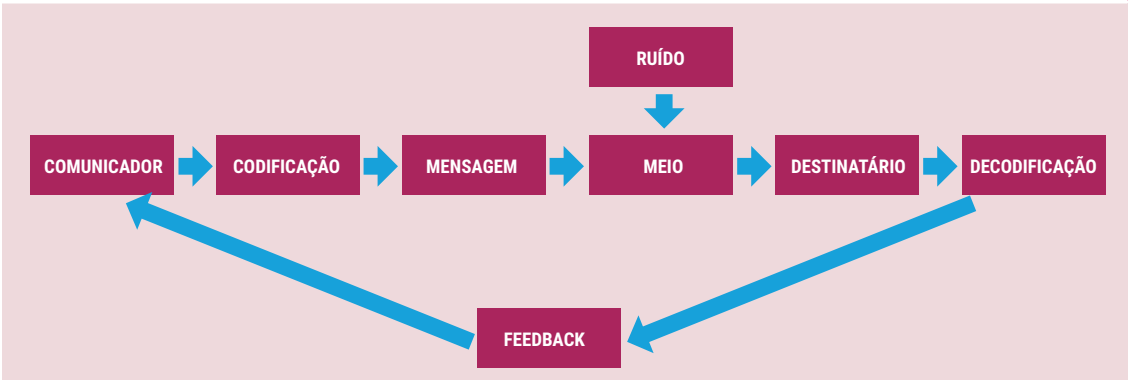
A retificação dessas falhas de comunicação envolve analisar como os riscos são comunicados e como a segurança cibernética pode se tornar relevante para os executivos, começando com a forma como os riscos em potencial são comunicados a eles.

Listas de risco x cenários de risco

Frequentemente, os profissionais de tecnologia usam terminologia confusa para falar de riscos. Como consequência, uma avaliação de risco geralmente parece uma combinação de coisas que não estão funcionando; grupos de pessoas que poderiam causar danos; e noções abstratas, esotéricas ou mesmo existenciais de consequências.[10] Essa lista de fatores de risco pode ser assim:

- Insiders com informações privilegiadas
- Reputação
- Processo de recuperação do sistema não testado

Figura 1-Modelo de comunicação moderno



> AO COMUNICAR O RISCO, É IMPORTANTE LEMBRAR QUE A MAIORIA DAS PESSOAS TEM UMA COMPREENSÃO INCOMPLETA DAS ESTATÍSTICAS, PORTANTO, NÃO SE PODE PRESUMIR O ENTENDIMENTO ESTATÍSTICO.

- Compartilhamento de dados na nuvem com dados sigilosos
- Senhas curtas
- Criminosos cibernéticos

É fácil perceber que cada item da lista é algo que pode causar preocupação. No entanto, os profissionais de tecnologia usam uma espécie de abreviação ao se comunicar com outros profissionais igualmente treinados e afins, enquanto os executivos de negócios são forçados a preencher os espaços em branco com imaginação (pautados pela experiência). Em uma declaração de risco totalmente qualificada, essas partes faltantes são articuladas para serem facilmente compreendidas por indivíduos que não estão familiarizados com os atalhos da profissão.

É importante comunicar claramente ao público-alvo quais itens da lista são ameaças, ativos e controles (por mais fracos que sejam). Os executivos devem entender como a combinação dessas categorias de coisas pode ser manipulada para causar danos à empresa.

O primeiro passo para melhorar a comunicação de riscos é garantir que haja um cenário de risco totalmente definido ao qual uma fórmula de risco possa ser aplicada.[11] Cada declaração de cenário de risco deve contar uma história que seja instantaneamente acessível a pessoas sem conhecimento técnico. Por exemplo, esse cenário pode ser: "Insiders privilegiados usam as credenciais legitimamente concedidas para roubar dados de aplicativos críticos." Ele especifica quem está fazendo algo ruim, quais métodos estão sendo empregados para fazê-lo e como a organização será afetada quando terminar. Um cenário de risco adequado precisa ser voltado para o futuro. Deve descrever uma série de coisas ruins que podem acontecer, não necessariamente algo que está acontecendo atualmente. Uma boa declaração de risco também é relativamente perpétua; se um item pode ser removido do registro de riscos após a correção de algo, é uma deficiência de controle, não um risco real.

A fórmula clássica de riscos

A fórmula clássica de riscos (probabilidade multiplicada pelo impacto) pode ser confusa para aqueles que recebem comunicações de risco de tecnologia. Considere o problema combinado associado à determinação da probabilidade e do impacto de pessoas privilegiadas (do cenário de amostra anterior). Pedir aos executivos que entendam a probabilidade de insiders como 0,45 não faz absolutamente nada para melhorar a comunicação. A probabilidade do quê, exatamente? Esta declaração não ajuda o destinatário a entender o problema.

Ao comunicar o risco, é importante lembrar que a maioria das pessoas tem uma compreensão incompleta das estatísticas, portanto, não se pode presumir o entendimento estatístico. Como resultado, o uso de conceitos como a fórmula básica de risco pode levar a cálculos incorretos, juntamente com a comunicação falha. O primeiro problema é que os termos "possibilidade" e "probabilidade" são usados de forma intercambiável ao falar e escrever. Isso não ajuda em nada para aumentar a compreensão mútua.

Em seguida, a probabilidade não é temporalmente limitada.[12] É inútil dizer aos executivos que a probabilidade (ou possibilidade) é de 40%. Ao lado da pergunta "probabilidade de quê?" mencionada anteriormente, está a pergunta óbvia de quando. É 40% provável que o evento ocorra hoje? Esta semana? Este ano? Esta década? O tempo importa e, por si só, esse valor não comunica efetivamente o que os executivos precisam saber sobre a probabilidade ou possibilidade de realização de riscos.

Para superar esse problema, muitas pessoas aplicam cronogramas fixos às suas estimativas. Eles descrevem esses valores como representando probabilidades anualizadas. Infelizmente, há um problema matemático fundamental com esses tipos de avaliação: E se o evento pudesse acontecer mais de uma vez por período? É matematicamente incorreto afirmar que algo tem 200% de probabilidade de acontecer no próximo ano, pois a probabilidade é um valor entre 0 e 1. E esse valor não é inclusivo: A probabilidade nunca pode ser 0 ou 1, porque um evento futuro nunca pode ser descartado ou descartado com 100% de certeza.

As questões anteriores podem ser superadas utilizando a frequência no lugar da probabilidade na equação.[13] Isso alcança vários objetivos. Primeiro, a frequência é um conceito muito mais acessível para representar eventos

futuros. Para aqueles que não se sentem à vontade em falar de estatísticas, é melhor perguntar com que frequência algo pode acontecer, em vez da probabilidade de isso acontecer. Segundo, essa variável é mais capaz de capturar eventos que ocorrem mais de uma vez por ano (ou período). É fácil compreender uma frequência de dois por ano, enquanto uma probabilidade de 200% não é apenas matematicamente incorreta, mas também difícil de entender na prática. Além disso, valores de probabilidade inferiores a 1 (por exemplo, 0,5) são mais facilmente reconhecíveis como valores de frequência e podem ser comunicados em linguagem simples (por exemplo, uma vez a cada dois anos).

Por último, e mais importante, a fórmula de risco simples não contém orientações sobre exatamente o que se deve avaliar a probabilidade e o impacto. Saber o que medir é tão importante quanto saber como medir. O risco tem a ver com perda, portanto, o que estiver sendo medido deve ser uma declaração completa de perda relevante para a empresa. A lista de riscos relacionados à tecnologia apresentada anteriormente é um exemplo clássico de coisas que não são fatores de risco de negócios porque não expressam um cenário de perda completo.

Mapeamento de processos de negócios

Algumas empresas podem não estar familiarizadas com o mapeamento de processos de negócios. No entanto, as equipes de continuidade de negócios já podem ter alguma versão do conceito. Nesse caso, seus mapeamentos e inventários de processos são um bom ponto de partida, exigindo menos recursos e suportando uma única fonte de informações sobre processos na empresa. Para iniciar o mapeamento de processos de negócios do zero, a abordagem de amostragem deve ser seguida, e os principais produtos e serviços e os processos críticos para cada um devem ser o foco. No primeiro ano, um tamanho de amostra viável precisa ser escolhido e um plano para aumentar o número de amostras a cada ano e determinar os recursos necessários.

O mapeamento de processos de negócios é a primeira etapa na criação de um cenário de risco totalmente qualificado. Isso exige entender como as empresas operam e ligar a tecnologia às ofertas de negócios. Também exige uma lista dos produtos e serviços que a empresa oferece (ou agrupamentos razoáveis deles). Essa lista geralmente pode ser compilada levando em conta o que é oferecido em cada linha de negócios ou em alguma outra categoria em grandes empresas (como localização geográfica). Em seguida, as partes da empresa que ajudam a fornecer cada produto ou serviço são ligadas. Considerar os processos de negócios que permitem cada parte da empresa é útil. Por fim, é feita uma conexão entre esses processos de negócios e a tecnologia que os permite. O resultado se parece com a **figura 2**.

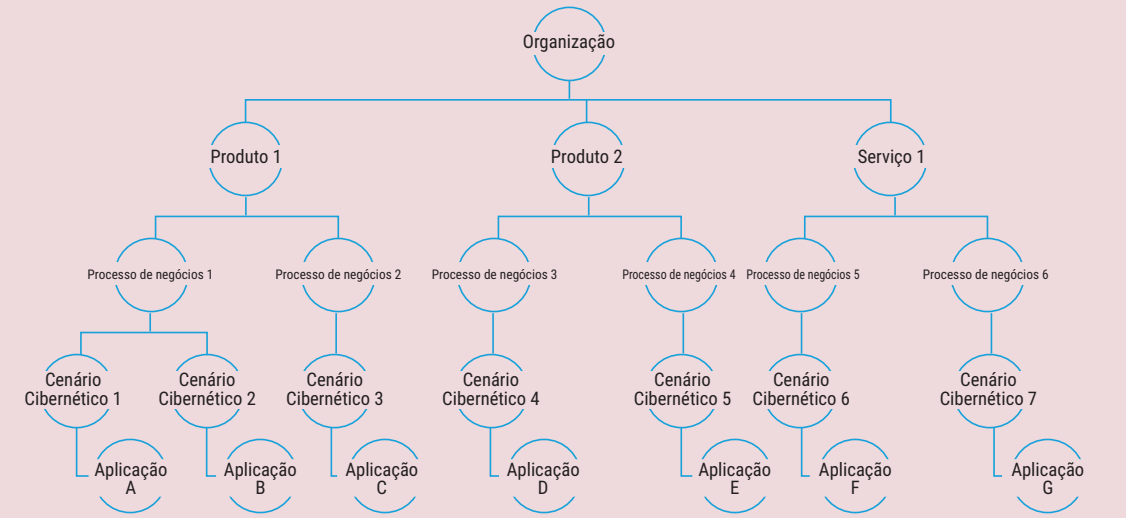
> "O MAPEAMENTO DE PROCESSOS DE NEGÓCIOS É A PRIMEIRA ETAPA NA CRIAÇÃO DE UM CENÁRIO DE RISCO TOTALMENTE QUALIFICADO."

Depois que houver uma conexão entre a tecnologia (elementos de tecnologia) e os produtos e serviços (elementos de negócios), é hora de elaborar os cenários de risco que afetam cada um. Isso ajuda a decompor o mapa do processo em cenários mais detalhados. Em geral, os aplicativos são a interface principal entre as empresas e suas tecnologias e, como tal, servem como o nexo que liga os elementos de tecnologia aos elementos de negócios. Alguns processos de negócios são baseados em aplicativos simples, como e-mail. Nesse caso, a infraestrutura de suporte que possibilita o e-mail também está alinhada com o processo de negócios e, por fim, com os produtos e serviços que o processo possibilita. Isso fornece uma noção de que tipo de problemas relacionados à tecnologia podem surgir e como eles podem afetar a empresa e suas ofertas. Aliás, esse modelo funciona para empresas com e sem fins lucrativos e para os setores público e privado. Em todos os casos, existe uma empresa para oferecer algo e a tecnologia está alinhada com essas ofertas para possibilitá-las. Em alguns casos (como o exemplo do e-mail), a tecnologia está alinhada com vários processos de negócios e produtos e serviços correspondentes. Após a conclusão desse mapeamento de ofertas e tecnologia, é possível elaborar cenários de risco.

Desenvolvimento de cenários de risco totalmente qualificados

Há diferentes níveis de cenários, dependendo de onde no mapa do processo de negócios o cenário existe. Por exemplo, no nível mais alto (por exemplo, relatórios do conselho), é provável que haja apenas alguns cenários agregados. Os cenários nas partes intermediárias da empresa (por exemplo, gerência sênior, chefes de várias linhas de negócios) incluirão desdobramentos adicionais dos cenários agregados que estão vinculados a produtos

Figura 2 - Mapeamento de processos de negócios que liga produtos e serviços a tecnologias



e serviços específicos. No final, haverá muitas versões de cenários cibernéticos que desencadeiam cenários de nível superior.[14] Um exemplo desse tipo de decomposição é apresentado na **figura 3**.

Ao elaborar categorias de risco de primeira linha, é importante considerar os negócios específicos nos quais a empresa está envolvida. No entanto, é possível começar com as seguintes categorias de eventos de Base II, mesmo para empresas que não estão envolvidas em serviços financeiros:[15]

1. Fraude interna
2. Fraude externa
3. Práticas de emprego e segurança no trabalho
4. Clientes, produtos e prática comercial
5. Danos a bens físicos
6. Interrupção nos negócios e falhas de sistema
7. Execução, entrega e gestão de processos

A maioria das empresas possui uma versão das categorias 1, 2, 5, 6 e 7 que aborda seus riscos tecnológicos. Um exemplo de categorias de risco aplicáveis (com base na **figura 3**) seria o seguinte:

1. Perda e furto de dados
2. Confiabilidade dos dados
3. Disponibilidade do sistema
4. Fraude

Essas quatro categorias de risco são adequadas para reportes em nível de diretoria. Elas podem ser desdobradas em versões específicas de produtos e serviços que refletem cenários em uma linha de negócios

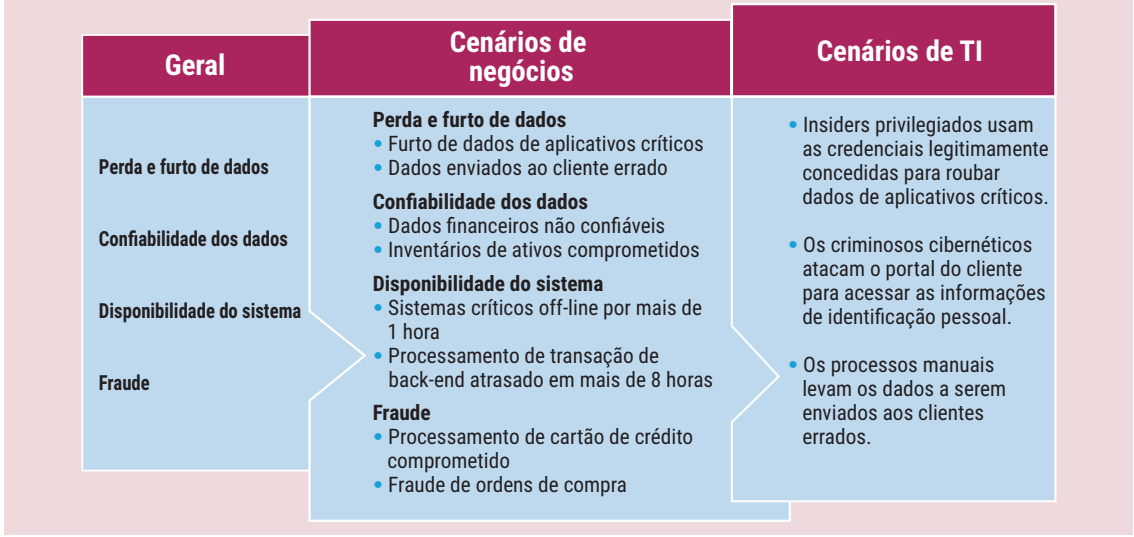
> "AO ELABORAR CATEGORIAS DE RISCO DE PRIMEIRA LINHA, É IMPORTANTE CONSIDERAR OS NEGÓCIOS ESPECÍFICOS NOS QUAIS A EMPRESA ESTÁ ENVOLVIDA."

específica, como mostra a **figura 3**.

Embora esses rótulos sejam úteis para o agrupamento de riscos, essas categorias precisam ser detalhadas em mais um nível para obter um cenário de risco totalmente qualificado que forneça um maior grau de precisão na avaliação de riscos. Por exemplo, "Furto de dados de aplicativos críticos" é uma categoria útil, mas não fornece detalhes suficientes sobre o que está acontecendo, quem o está fazendo e como avaliar os fatores de risco e a eficácia dos controles. Um cenário de risco totalmente qualificado pode ser: "Insiders privilegiados usam as credenciais legitimamente concedidas para furtar dados de aplicativos críticos."

Esta afirmação revela várias situações críticas. Primeiro, ela afirma quem está tomando a ação. Em seguida, afirma como eles estão conseguindo. Nesse caso, a empresa já concedeu a esses indivíduos as ferramentas

Figura 3 - Decomposição de categorias de risco em cenários



necessárias para cometer atos ilícitos, que também são claramente identificados como furto de dados de aplicativos críticos. O mais importante é que a afirmação conte uma história, e esse tipo de narrativa garante que a comunicação seja clara e completa. Como categoria de cenário de perda, a "perda de dados" é um exemplo útil, mas a frase pode conjurar imagens diferentes para pessoas diferentes. Um cenário de risco totalmente elaborado articula a maneira específica pela qual a perda de dados ocorre.

O próximo passo é conectar os cenários de perda aos ativos de tecnologia relevantes. Para isso, é necessário identificar os atributos inerentes aos ativos que os conectam ao cenário. Por exemplo, o cenário de exemplo anterior exigiria apenas um único atributo: usuários com permissão para ver dados confidenciais. É semelhante à maneira como as empresas de seguros usam informações demográficas para determinar os prêmios. Aqui, esses atributos inerentes vinculam os cenários de risco corretos aos ativos que poderiam causá-los. Além disso, como os cenários de risco são elaborados de forma que a fórmula de risco possa ser aplicada com precisão, os ativos de tecnologia podem ser vinculados, por meio de seus dados demográficos, a classificações de risco que representam como a perda pode ocorrer nesse sistema. O cenário conta uma narrativa específica dos elementos de tecnologia e que pode ser alinhada às categorias de risco relatadas na empresa.

Avaliações de risco de descendente x ascendente

As avaliações de risco de ascendentes geralmente são reconhecidas como muito mais completas do que as descendentes. No entanto, como as avaliações ascendentes exigem a coleta de grandes quantidades de informações de várias tecnologias e indivíduos, a maioria das empresas as considera excessivamente demoradas, possivelmente resultando em uma avaliação incompleta antes da data de vencimento dos relatórios.

As avaliações de risco descendentes, por outro lado, têm a reputação de serem rápidas e fáceis. Eles exigem menos recursos para serem realizados e podem fornecer resultados significativos. No entanto, estão sujeitas ao viés das pessoas de alto nível hierárquico que os conduzem, e geralmente são desconectadas dos problemas do dia-a-dia e dos cenários de risco que são bem conhecidos dos que estão em nível mais operacional.

Na prática, aqueles que executam funções de auditoria normalmente não sofrem cenários hipotéticos. Eles reconhecem que não podem avaliar tudo e selecionam amostras na parte inferior para as categorias na parte superior nas quais desejam reportar. Essa abordagem de amostragem pode ser muito útil para empresas que tentam preencher a lacuna entre as avaliações de risco ascendentes e descendentes. A amostragem, em conjunto com a decomposição do cenário de risco descrita anteriormente, oferece as ferramentas necessárias para gerar relatórios confiáveis sobre o estado de risco em uma empresa.

A abordagem de amostragem para avaliação de riscos

Para usar o método de amostragem:

Gostou do artigo?

- *Leia Atravessando a lacuna de risco digital. www.isaca.org/Bridging-the-Digital-Risk-Gap*
- Saiba mais, discuta e colabore sobre o gerenciamento de riscos nos fóruns on-line da ISACA. *https://engage.isaca.org/onlineforums*

1. Selecione algumas amostras do nível mais baixo para pautar cada categoria de risco de nível superior e intermediário. Por exemplo, na categoria perda e furto de dados, correlacione várias declarações de risco de nível intermediário de cada unidade de negócios (por exemplo, furto de dados em aplicativos críticos).
2. Selecione os cenários cibernéticos e os elementos de tecnologia vinculadas a eles. Isso resulta em vários elementos específicos de recursos de baixo nível para avaliar. Essas podem se tornar as classificações de risco usadas para justificar as classificações aplicadas a outros níveis.

Essa abordagem permite uma avaliação de risco ascendente com o benefício de avaliar o risco na parte inferior para validar essas classificações.

Inicialmente, tais amostras devem abordar aplicativos e infraestrutura críticos e importantes, mas, com o passar do tempo, uma empresa pode experimentar a maior parte de seu ambiente de tecnologia. Por exemplo, ela pode testar os principais aplicativos no primeiro ano, seguidos pelos aplicativos de segundo e terceiro níveis nos anos seguintes. As avaliações de risco resultantes devem incluir uma declaração de âmbito, indicando que a classificação é baseada em uma amostra (por exemplo, 15%) de aplicativos e infraestrutura críticos. Esse âmbito também pode ser incluído nos planos estratégicos anuais, e qualquer amostragem adicional solicitada por uma empresa pode ajudar os líderes de segurança e risco a preparar melhores orçamentos para recursos para apoiar essas solicitações.

Abordando falhas

Com muita frequência, as listas de falhas chegam aos registros de riscos organizacionais. Uma boa regra básica é que, se um item no registro puder ser verificado, removido ou concluído com a alteração correta na configuração, implementação de tecnologia ou processo, provavelmente não é um cenário de risco e não pertence ao registro de risco. No entanto, essas listas de falhas são muito importantes para a capacidade geral de gerenciamento de riscos de uma empresa. Ao lado de cada nível na hierarquia do cenário de risco, deve haver uma lista correspondente de itens defeituosos, em níveis crescentes de detalhes à medida que alguém desce a lista.

Por exemplo, uma lista de patches ausentes ou servidores configurados incorretamente não deve estar no registro de riscos. Em vez disso, eles devem residir em sua própria lista de problemas que exigem atenção, como um registro de gerenciamento de problemas ou um registro de interrupção/correção. Esses itens individuais podem ser categorizados em um nível agregado de forma a permitir que eles sejam vinculados a cenários cibernéticos. Por exemplo, vários usuários podem ter privilégios demais no acesso a aplicativos críticos. Isso pode ser classificado como permissões desnecessárias ou excesso de privilégios. Essa categoria pode ser alinhada, por exemplo, com o cenário cibernético de "insiders privilegiados usando indevidamente permissões concedidas legitimamente". Em um nível superior, essas falhas podem ser agrupadas em uma categoria chamada "gerenciamento de identidade e acesso".

Responsabilidade pelo risco

É uma noção popular de que uma entidade comercial "possui" risco. O que isso significa, na prática, é que todos os itens no registro de riscos devem estar alinhados com um proprietário que não esteja na TI, no gerenciamento de riscos, segurança cibernética e assim por diante. O risco deve estar alinhado com alguém

> "AS AVALIAÇÕES DE RISCO DE ASCENDENTES GERALMENTE SÃO RECONHECIDAS COMO MUITO MAIS COMPLETAS DO QUE AS DESCENDENTES."

responsável pelos produtos e serviços articulados no mapa do processo de negócios. Isso representa uma mudança de cultura significativa para a maioria das empresas. Para muitos, é uma heresia pensar que um profissional de TI não "possui" um risco de perda de dados e furto. Mais especificamente, a TI pode se responsabilizar por uma série do que os profissionais de risco operacional chamam de gatilhos de risco ou uma taxonomia causal, como as "permissões desnecessárias" mencionadas anteriormente. Por fim, a perda é creditada aos responsáveis pelos produtos e serviços afetados. Um efeito colateral importante da alocação de propriedade de risco dessa maneira é que a avaliação de um cenário de risco varia de uma unidade de negócios para a próxima. É provável que a quantidade de perda associada aos clientes varie significativamente de um produto para outro. Assim, uma declaração de risco pode aparecer em vários registros de risco internos, provavelmente com

classificações de risco distintas. Para todos esses fatores de risco alinhados com unidades de negócios, é importante designar um contato para atuar como uma ponte entre a TI e a unidade de negócios para ajudar na comunicação e tradução da terminologia de TI e para auxiliar nas decisões de tratamento de riscos, incluindo o acompanhamento de consertar falhas alinhadas com essas declarações de risco.

Conclusão

Por fim, há programas de tecnologia para que as empresas possam fornecer os produtos e serviços para os quais são planejados. Com raras exceções, os líderes empresariais não são especialistas em fornecer soluções de tecnologia. Toda profissão tem sua própria linguagem, jargões e abreviações que permitem que os profissionais se comuniquem rapidamente. No entanto, a TI é uma profissão que existe para atender a um objetivo organizacional e, como tal, precisa ajustar suas comunicações para ajudar a liderança organizacional a atingir seus objetivos.

Estar mais bem alinhado com a empresa permite melhor criação de valor, facilita a percepção de competência e alivia disputas internas que distraem o cumprimento das expectativas dos clientes. Reorganizar os relatórios de risco de TI para melhor alinhar-se ao entendimento da empresa sobre seus propósitos e prioridades melhora a comunicação e fornece aos tomadores de decisão as informações necessárias para serem melhores gerentes.

Notas de rodapé

1 Griffin, E.; *A First Look at Communication Theory, 6th Edition*, McGraw-Hill, USA, 2006
2 Shannon, C. E.; "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, edição 3, 1948, p. 379–423, 623–656
3 ISACA®, *State of Cybersecurity 2019*, *www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf*
4 Risk.Net, "Top 10 Operational Risks for 2019," 14 de março de 2019, *https://www.risk.net/risk-management/6470126/top-10-op-risks-2019*
5 Marsh & McLennan, Microsoft, "2019 Global Cyber Risk Perception Survey," setembro de 2019, *https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf*
6 *Ibid*.

> "UMA DECLARAÇÃO DE RISCO PODE APARECER EM VÁRIOS REGISTROS DE RISCO INTERNOS, PROVAVELMENTE COM CLASSIFICAÇÕES DE RISCO DISTINTAS."

7 Copeland, J.; "No Time to Talk Cyber Risk, Senior Executives Say," Fair Institute Blog, 19 de setembro de 2019, *https://www.fairinstitute.org/blog/no-time-to-talk-cyber-risk-senior-executives-say*
8 Jones, J.; "Jack Jones: Quit Blaming Executives for Cybersecurity Problems," Fair Institute Blog, 19 de agosto de 2019, *https://www.fairinstitute.org/blog/quit-blaming-executives-for-cybersecurity-problems*
9 Laws, S. M.; "Corporate Communication: Identity, Image and Reputation," *International Journal of Business Competition and Growth*, vol. 3, edição 4, 2014, p. 344–349
10 Freund, J.; J. Jones; *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann, USA, 2014
11 Maurice, D. R.; J. Rathod (ed.); "Cybersecurity and Technology Risk," *Operational Risk Perspectives: Cyber, Big Data, and Emerging Risks*, Risk Books, Reino Unido, 2016
12 *Op cit* Freund, Jones
13 *Ibid*.
14 Freund, J.; "Keep It Simple: How to Avoid Drowning in Cyber Risk Information," Risk.net, 2017, *www.risk.net/risk-management/3938516/keep-it-simple-how-to-avoid-drowning-in-cyber-risk-information*
15 Bank for International Settlements; " QIS 2–Operational Risk Loss Data," 2001, *https://www.bis.org/bcbs/qisoprisknote.pdf*