ANBIMA

Debate

Cydersecurity no mundo das assets

ANBIMA

Sumário

Apresentação

Os riscos trazidos pelo mundo conectado são cada vez mais complexos. E não são apenas as perdas financeiras que estão em jogo. Os riscos reputacionais também podem causar prejuízos consideráveis. As empresas do mercado financeiro, pela riqueza e pela importância das informações com as quais trabalham, são atraentes alvos para os cibercriminosos. Não estão expostos apenas os grandes bancos, que transacionam bilhões de reais. As assets também correm riscos e precisam ter a cibersegurança como prioridade.

Para auxiliar essas instituições de pequeno e médio portes a identificar o que é essencial no gerenciamento de riscos, a cibersegurança foi tema de uma edição do ANBIMA Debate, série de eventos exclusivos para associados criada para discutir assuntos de interesse do mercado. O encontro, que foi assistido por 140 pessoas, entre público presencial e online, aconteceu em São Paulo.

Este relatório consolida os principais pontos da mesa-redonda.

Participante
Rodrigo Fusco, gerente de Tecnologia da M Square Brasil

Participante
Jorge Vaz, superintendente de TI do Banco Máxima

Participante
Álvaro Teófilo, head de Produtos de Identidade Digital da Tempest

Moderação
Ricardo Döllinger, presidente do Comitê de Compliance e chief operating officer de Compliance do BNP Paribas para a América Latina

Por que me preocupar com cibersegurança?

Cuidados com cibersegurança são necessários independentemente do tamanho da asset. Mesmo sem plataformas transacionais, essas instituições correm risco de ataques. Custo não é desculpa para a não adoção de medidas de segurança. O que falta, na maioria das vezes, é cultura.

O assunto é desafiador, mas não pode ser minimizado. Uma gestora pequena pode avaliar que, por trabalhar com estrutura simplificada e poucos funcionários, não tem os recursos necessários para montar um sistema de segurança cibernética, ou que, por não ter plataformas transacionais, não está tão sujeita a risco de ataques. Esse é um paradigma que precisa ser quebrado.

"Quando a instituição é grande, ela aguenta um ataque cibernético: pode até balançar, mas não quebra; se é de pequeno porte, uma pancada pode bastar para ela cair."

Rodrigo Fusco

Custo não é desculpa

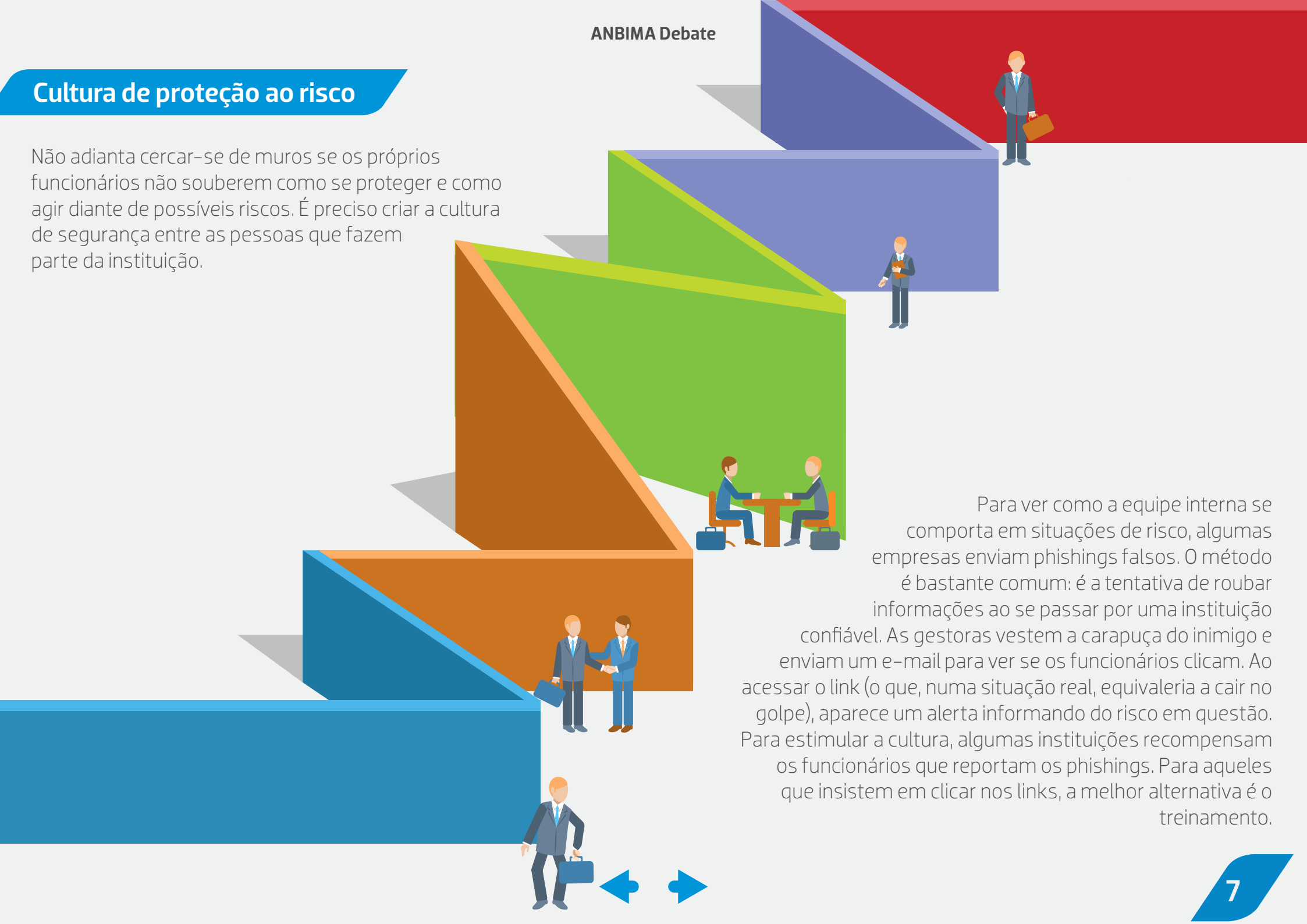
Não são só os riscos reputacionais e operacionais de ficar com o sistema fora do ar por causa de um vírus ou de algum tipo de ataque ou invasão. Há também um risco muito grande para o negócio, decorrente da indisponibilidade de dados e sistemas.

Os cuidados a serem tomados são muitos, mas existem ações muito básicas que já garantem um alicerce mínimo para a segurança. Custo ou pessoal não podem ser desculpas: há soluções de código aberto que não exigem investimentos vultuosos; é possível terceirizar, dispensando a necessidade de equipe interna especializada no assunto; e várias das práticas de cibersegurança podem ser aplicadas tanto por grandes instituições como por assets de pequeno porte.

Os gestores precisam dar ao tema de segurança a mesma atenção que dão para aspectos legais, por exemplo. Toda asset conta com uma assessoria jurídica, mas o mesmo não acontece com a área de tecnologia. É preciso mudar essa cultura. Não dá para a instituição achar que está segura fazendo uso de produtos disponíveis em supermercados ou atribuindo a responsabilidade pela segurança ao profissional responsável pela manutenção das máquinas. É essencial escolher produtos de qualidade e trabalhar com pessoal especializado.

Cultura de proteção ao risco

Não adianta cercar-se de muros se os próprios funcionários não souberem como se proteger e como agir diante de possíveis riscos. É preciso criar a cultura de segurança entre as pessoas que fazem parte da instituição.



Para ver como a equipe interna se comporta em situações de risco, algumas empresas enviam phishings falsos. O método é bastante comum: é a tentativa de roubar informações ao se passar por uma instituição confiável. As gestoras vestem a carapuça do inimigo e enviam um e-mail para ver se os funcionários clicam. Ao acessar o link (o que, numa situação real, equivaleria a cair no golpe), aparece um alerta informando do risco em questão. Para estimular a cultura, algumas instituições recompensam os funcionários que reportam os phishings. Para aqueles que insistem em clicar nos links, a melhor alternativa é o treinamento.

Faça o básico: cuide das suas senhas

As práticas de segurança começam com iniciativas simples. As pessoas têm o hábito de usar as mesmas senhas para todos os logins – se o invasor descobrir qual é, tem acesso a tudo. Muitos vazamentos de fotos íntimas, por exemplo, acontecem não porque a nuvem na qual as imagens estavam armazenadas foi invadida, mas sim porque a senha utilizada era a mesma de outros cadastros.

Você até pode se arriscar e repetir as senhas, mas é essencial que os códigos utilizados nos e-mails pessoal e profissional sejam diferentes e únicos. Isso porque todos os demais cadastros remetem a uma conta de e-mail.

O sistema de verificação em duas etapas (two factor autentication) também é uma forma simples de garantir segurança. Ele envia um SMS quando há tentativa de login em uma determinada conta – se não for o proprietário, é possível impedir o acesso. A maioria dos serviços de e-mail, mesmo os gratuitos, disponibiliza essa opção, basta ativar.

São princípios básicos para adotar, inclusive na vida pessoal, que evitarão muita dor de cabeça.

Também é comum que fornecedores de serviços de segurança utilizem a mesma senha para todos os clientes. Isso significa que alguém mal-intencionado pode invadir as bases de dados de todos os clientes. Uma alternativa quando se trabalha com fornecedor externo é contratar uma segunda empresa para testar as práticas que foram adotadas pelo provedor contratado.

"Two factor autentication não custa nem um centavo a mais e melhora a segurança em 99%."
Rodrigo Fusco

Regulação

A necessidade de regular as práticas de cibersegurança é uma certeza do mercado. Ainda que a regulação não consiga tratar de todos os riscos e problemas que podem afetar as gestoras, pois é algo muito dinâmico, é possível definir normas gerais. Assim, cada instituição, de acordo com o seu porte e a sua realidade, fará a análise de risco (risk assessment) dela e dos provedores de serviço com os quais se relaciona.

A discussão atualmente gira em torno de como construir essas normas: de forma prescritiva ou baseada em princípios. A primeira descreve detalhadamente os aspectos que devem ser observados nas medidas de segurança, prevendo situações e como agir em cada uma delas. Já as normas fundamentadas em princípios transmitem um conceito mais genérico, que pode ser adaptado a cada situação de acordo com o ambiente da empresa.

"Questões muito complexas são difíceis de regulamentar com muita prescritibilidade."
Dollinger

Nem sempre uma prescrição detalhada será garantia de efetividade. O que atende a um banco de grande porte, que tem milhões de transações, teria um nível de prescrição que não se aplica a uma pequena asset. Da mesma forma que a regulamentação voltada para uma gestora de pequeno porte não atende às necessidades de uma grande instituição.

Como é feito lá fora?

No mercado internacional, alguns aspectos-chave recomendados pelo Comitê de Basileia e pela Iosco (Organização Internacional das Comissões de Valores Mobiliários) são comumente observados, como a adoção de práticas e políticas de segurança cibernética, a definição do que é risco, a aplicação de testes de vulnerabilidade e o reporte de incidentes cibernéticos. Entre outros aspectos, pode-se criar uma discussão sobre a necessidade de uma certificação para os profissionais que atuam nesse setor e aplicar programas de treinamento para que todos os funcionários de uma instituição saibam como mitigar riscos e se proteger deles.

Os padrões do Nist (Instituto Nacional de Padrões e Tecnologia dos Estados Unidos) também têm servido como base para muitos países montarem a própria regulação.

Nossas iniciativas em cibersegurança

Lançamos o **Guia de Cibersegurança** com práticas para orientar as instituições na implementação de um programa de segurança cibernética. Nossa ação segue em linha com o que tem sido feito no mundo todo: o objetivo do guia é servir como referência nas diferentes instituições que fazem parte da Associação e para a educação das equipes.

Acesse »

Análise baseada em risco

Um primeiro passo em direção à segurança cibernética é fazer uma avaliação interna, mapear os riscos, identificar o grau de exposição da empresa e traçar planos de contingência. Significa que a instituição está protegida? Não. Mas significa que ela sabe quais são seus ativos mais críticos, conhece os possíveis impactos de uma ocorrência e tem um plano de resposta em caso de incidente, incluindo como tratar os diversos públicos, como funcionários, clientes e imprensa, entre outros.

Do ponto de vista regulatório, isso pode servir como atenuante, pois mostra que a empresa foi diligente, ainda que, do ponto de vista do negócio, possa haver perdas.

Serei atacado. O que fazer?

Atualmente, a questão não é se a empresa será atacada, mas quando. A Finra (instituição que regula o mercado financeiro nos Estados Unidos) recomenda que as instituições devem partir sempre do princípio de que serão invadidas e, por isso, precisam estar preparadas para quando isso acontecer.

"Estar preparado para responder a um ataque é tão importante quanto trabalhar na prevenção."
Jorge Vaz

Como você vai reagir? Qual será seu posicionamento perante os clientes? O que dirá para a imprensa? Para quem vai ligar pedindo socorro? Na hora da crise, é difícil definir tudo isso e ainda tentar reduzir o impacto do incidente. Por isso é importante pensar em tudo antes e estruturar um plano de ação com as responsabilidades de cada um frente ao ataque.

"É pouco comum encontrar planos de crise que incluam questões de segurança de informações."
Álvaro Teófilo

Compartilhamento de inteligência

Outra forma de se fortalecer perante os riscos é compartilhando conhecimento. O mercado discute, inclusive, a criação de um fórum ou organismo para troca de informações sobre inteligência cibernética entre as instituições financeiras. Em alguns países, os reguladores oferecem plataformas para fóruns online, por meio dos quais os profissionais trocam informações e até relatam ocorrências.

Assim, se uma instituição for atacada, ela pode compartilhar os endereços que fizeram parte do incidente para que outras coloquem esses IPs sob suspeita. É recomendável que esses ambientes permitam depoimentos anônimos, pois há instituições que preferem não se expor.

"Se os próprios atacantes compartilham informação, por que nós, que somos pró-mercado, não estamos preocupados com isso?"

Jorge Vaz

Em 2012, no auge dos ataques aos caixas eletrônicos no Brasil, os grandes bancos se reuniram para discutir práticas de segurança e estabeleceram requisitos mínimos que estes equipamentos deveriam cumprir. Foi uma rica troca de informações, que aumentou o padrão de excelência das normas já adotadas. Esse tipo de experiência, entretanto, ainda é incomum.

Dificuldades de compartilhar

Ambientes de colaboração coletiva, como fóruns, enfrentam alguns desafios, como participantes que não contribuem para o debate e apenas usufruem do que é publicado ou dito pelos demais, ou pessoas mal-intencionadas que se inserem apenas para colher informações e jogar contra.

Uma forma de evitar isso é "gameficar" a plataforma. Quem não participa pode ter seu acesso à informação limitado e começa a cair numa escala de pontos, podendo inclusive ser banido do grupo. Ainda que o integrante não tenha informações relevantes para compartilhar, ele pode contribuir com pesquisas, levantamento de boas práticas e identificação de tendências que podem ajudar outros participantes do fórum. Não é simples, mas há caminhos.

"É complexo, mas compartilhar informação de forma sistemática é um princípio que todo mundo deveria seguir."
Álvaro Teófilo

Saiba mais

Quer saber ainda mais? Assista ao ANBIMA Debate sobre cibersegurança no mundo das assets na íntegra: youtu.be/h-ThFiVkeSI

Clique aqui e confira a apresentação de Ricardo Döllinger, que mediou o debate.

Comece a implementar boas práticas de segurança cibernética na sua gestora: baixe o nosso: **Guia de Cibersegurança**

ANBIMA Debate

Cybersecurity no mundo das assets

Comunicação e Marketing
Marcelo Billi

Coordenação de Comunicação
Marineide Marques

Redação
Flávia Nosralla

Projeto Gráfico/Diagramação
José Carlos Oliveira

Rio de Janeiro
Av. República do Chile, 230 – 13° andar – CEP 20031-170
Tel: (21) 3814-3800

São Paulo
Av. das Nações Unidas, 8501 – 21° andar – CEP 05425-070
Tel: (11) 3471-4200

ANBIMA