Sem cultura, não há segurança.

Os exeutivos de TI vivem espremidos no dilema entre disponibilizar e proteger a informação. Entre fazer a informação fluir, para melhorar o rendimento dos negócios, e impor restrições, para evitar danos à produtividade ou à reputação da empresa. Para atingir o equilíbrio ideal entre essas duas posturas, sabem que precisam criar nas corporações a cultura da vigilância sobre todo o ciclo de vida das informações. Não importa se para esse trabalho devam contar com o auxílio de equipes internas ou de terceiros. Para alguns, o modelo ideal seria tirar a área de segurança da informação de dentro da TI e fazê-la se reportar diretamente ao CEO. Mas todos concordam que a manutenção da segurança depende essencialmente da revisão de processos, mas, acima de tudo, do treinamento das pessoas. É o que revelam nesta mesa-redonda, coordenada pelo diretor de redação do Informática Hoje, e da qual participaram: Ariovaldo (**Ari**) Simielli Branco, gerente de TI da Expresso Jundiaí, empresa especializada em transporte e logística; **Carlos** Alberto Barros Alves, gerente de tecnologia da Wickbold Alimentos; **Dario** Almeida, gerente de arquitetura de sistemas da Câmara de Comercialização de Energia Elétrica (CCEE); **Douglas** Borges de Oliveira, diretor de TI da Epay Brasil, empresa de transações eletrônicas, de pré-pagos e cartões de recarga de celular; **Fábio** Luiz Mazelli, diretor de TI da América Latina da Penske Logistics; **Fernando** Martins, gerente de tecnologia do Banco Cacique, do grupo Societé Generale; Luiz Alberto **Villaça** Leão, diretor e CIO da Check Express; Marco **Astorga**, gerente de tecnologia da Abyara Brasil Brokers, empresa de venda de imóveis; **Marcos** Roberto Pasin, CIO da Bueno Netto Incorporadora e Construtora; **Moacyr** Conte Junior, global datacenter manager da Cargill Agrícola; **Rogério** Pires, diretor corporativo do Grupo TV1; **Sérgio** Rosa, infrastructure manager Latin America, da Goodyear; e **William** Rocha, CIO do Grupo D'Avó Supermercados.

IH – Vamos fazer um exercício de abstração: se não tivessem nenhuma restrição orçamentária, o que vocês gostariam de fazer para garantir a segurança do ciclo de vida das informações nas empresas de vocês?

Moacyr – Talvez a minha visão de segurança da informação seja um pouco diferente da maioria: eu vejo a informação também no aspecto físico, até pela característica da área em que eu trabalho, que é a de datacenters. Nós somos os fiéis depositários da informação enquanto ela existe na companhia, dentro ou fora dos datacenters. O que eu gostaria é que o pessoal de TI tivesse mais disciplina ao definir o ciclo de vida da informação, desde o momento em que ela é criada, enquanto é armazenada nos meios eletrônicos e depois fisicamente, quando é guardada em algum local externo. A gente perde essa conexão e isso gera custos astronômicos para a corporação. É caríssimo manter essa informação online, real time, e isso nem sempre é necessário. Algumas informações ficam no offsite storage eternamente, porque todo mundo tem medo de se desfazer delas e a gente não vê ninguém tirando as informações de lá.

IH – Então a solução nem depende tanto de orçamento, é acima de tudo uma questão cultural?

Moacyr – É cultural, mas mais do que isso é uma falta de visão das pessoas que criam os métodos de coleta das informações, sem se preocupar com o ciclo de vida dessas informações. Se a gente não tivesse restrição de orçamento e de tempo, investir mais na conscientização das pessoas é o que faria a grande diferença. Tudo passa no final por você entender os procedimentos, entender por que as coisas são importantes, onde está o valor daquilo, para você aplicar as políticas que são criadas.

Sérgio – A gente precisa mesmo falar da questão cultural. Meu sonho era que fosse ensinada nas escolas a questão do ciclo de criação, guarda e depois de destruição da informação. A questão da segurança da informação é eminentemente

atalho

Desafiados a pensar no que fariam para preservar a segurança da informação nas empresas, se não tivessem restrições orçamentárias, os participantes desta mesa-redonda não hesitaram em apontar para uma solução: conscientização. Eles deixaram claro que se defrontam no dia a dia com a dificuldade essencial de fazer as pessoas entenderem o ciclo de vida das informações. Do momento em que são produzidas, até o momento final do armazenamento ou do descarte, as informações costumam ser negligenciadas por pura falta de cultura de quem lida com elas. Investir na conscientização das pessoas certamente aliviaria a carga de tensão dos CIOs, confrontados com a necessidade de preservar a segurança das informações.

cultural. Não há tecnologia que resolva o problema cultural: todos nós somos treinados a usar a informação e depois ignorá-la.

IH – Mas, considerando que as pessoas estão lá e já vieram sem essa formação, como se faz para acabar com esse apego às informações produzidas e armazenadas?

Sérgio – O que a gente fez na Goodyear é o que a maioria das empresas faz: as campanhas de conscientização. Por exemplo, para os estagiários que chegam na empresa, nós fazemos uma doutrinação de como tratar a informação, principalmente porque eles vêm do mercado usando as redes sociais, onde a exposição de informação não tem limite e tudo está na nuvem. O que eu faria, se não houvesse restrição orçamentária, seria mais campanhas e mais treinamento para todos da empresa o tempo todo.

Fábio – Eu teria um time totalmente dedicado a esse trabalho, até para se criar a cultura, para que esse time pudesse efetivamente atuar em todas as fases do desenvolvimento das aplicações e dos projetos. Quem tem alguma cultura de segurança da informação acaba às vezes pensando nisso ao final do projeto, quando na verdade isso deveria acontecer desde o início de qualquer desenvolvimento. A gente está numa época de informações descartáveis. As pessoas começam a confundir o que é informação corporativa com o que é informação pessoal e isso gera uma grande confusão. O treinamento é importante, mas a realidade é que essa nova geração já vem com o DNA da informação descartável, superficial. Por isso, eu gostaria de ter um time dedicado a discutir, analisar e avaliar todas essas questões.

Fernando – Se eu tivesse dinheiro para usar à vontade, aumentaria a área de segurança da informação com pessoas e investiria em mais ferramentas.

IH – Você tem uma equipe dedicada só à segurança da informação?

Fernando – Tenho, mas é uma equipe restrita. São quatro pessoas. Aumentaria a equipe para que as pessoas pudessem ter um envolvimento maior em todas as áreas, em todos os projetos. Isso tem que ser uma cultura, passa pelo treinamento. E também aumentaria os investimentos em mecanismos de tecnologia para garantir a segurança da informação desde a captura nas agências até transporte, armazenagem e o descarte.

Douglas – Eu tenho um exemplo clássico, que não se refere ao armazenamento digital. Na sala de reuniões, utilizada para reuniões internas e externas, um quadro branco continha informações confidenciais e alguém escreveu "favor não apagar". A faxineira limpou a sala, e, na reunião seguinte, de pessoas de fora da empresa, a informação continuava lá, exposta. A pessoa talvez tenha pensado em continuar a reunião, mas não avaliou o risco de aquela sala ser utilizada na sequência por pessoas que eram de fora da empresa. Por acaso, aquela informação não era relevante especificamente para quem participou da reunião seguinte, mas o episódio nos inspirou a criar uma nova regra: a encarregada de preparar as salas para as reuniões tem o dever de não respeitar nenhuma recomendação daquelas.

Villaça – Acho que a gente está muito bem em segurança da informação lá na Check Express. A gente presta serviço para muitos bancos, com centenas de milhões de transações financeiras por mês. Mas, se não houvesse limitação de orçamento, eu queria ter uma equipe de verificação de segurança da informação, meus hackers/auditores internos, olhando não só os aspectos técnicos, mas também os não técnicos, processuais, da totalidade do ciclo. Uma coisa que me deixa muito preocupado é o fato de a gente trancar portas e janelas e esquecer aquele balcão francês que fica ali em cima da árvore. Nós não costumamos pensar no fato de que, durante uma reunião, muita gente simplesmente fotografa aquele quadro branco de que o Douglas falou. O que a gente faz com as fotos? A gente sincroniza em casa. Duvido que qualquer um de nós tenha fechado essa porta. Com a tendência do bring-your-on-device, fica tudo mais difícil.

fotos hamilton pena

"Não há tecnologia que resolva o problema cultural: todos nós somos treinados a usar a informação e depois ignorá-la."

Sérgio, da Goodyear

IH – Quando você fala que queria ter a sua equipe de hackers/auditores para fazer esse trabalho, necessariamente teria que ser uma equipe interna ou você contrataria uma empresa externa para fazer isso?

"A gente está numa época de informações descartáveis. As pessoas começam a confundir o que é informação corporativa com o que é informação pessoal e isso gera uma grande confusão."

Fábio, da Penske

fotos hamilton pena

> “Um dia virei a página de um bloquinho e não acreditei no que vi: informações confidenciais que jamais poderiam estar lá, que deveriam ter sido trituradas.”
>
> Villaça, da Check Express

Villaça – Provavelmente seria uma empresa externa. Quando falo em minha equipe quero dizer uma equipe sob a minha responsabilidade, não de um auditor de um cliente ou de um auditor de uma entidade externa reguladora. Numa outra empresa em que eu trabalhei, havia uma experiência fantástica de aproveitamento máximo de papel: todas aquelas sobras de papel de impressoras viravam bloquinhos. Um dia virei a página de um bloquinho e não acreditei no que vi: informações confidenciais que jamais poderiam estar lá, que deveriam ter sido trituradas. Por isso, cultura é essencial,

Marcos – Desde o ano passado a gente passou a contratar empresas especializadas para cada tipo de segurança. Então eu quero uma equipe especialista naqueles check points, naquele firewall, naquele ambiente. Hoje eu tenho uma pessoa que cuida das empresas de segurança, cobrando SLA, melhorias. Porém a gente chega sempre à conclusão de que não adianta ter tudo isso se os usuários não cuidam da segurança. Por isso, começamos neste ano um trabalho interno de conscientização de todos os usuários, começamos a fazer eventos internos nos quais contamos histórias que acontecem no mundo inteiro em grandes, pequenas e médias empresas. Então a regra lá é essa, todo mundo é dono da informação e todo mundo tem que zelar pela informação. A informação não é da TI, é da empresa.

Villaça – Uma coisa que ainda ninguém falou é que ter os cuidados adequados com a migração da informação ao longo dos diferentes estágios, de forma a que essa informação não se perca ou seja adulterada, também é segurança da informação. Não adianta nada aquele nosso sistema que faz a limpeza da base online e joga na base de segundo nível, se ele não foi adequadamente homologado. Na verdade, o que está gerando é lixo, que ninguém vai conseguir ler daqui a alguns anos. Quem de nós já não tentou recuperar uma informação de offsite e não conseguiu? Às vezes é porque ela simplesmente não foi gravada.

IH – É preciso disciplina na organização dos processos e do fluxo das informações, certo?

Villaça – Disciplina e qualidade. Às vezes a gente não aplica para a guarda da informação no back office a mesma qualidade que a gente aplica para o sistema online que está interagindo com os usuários.

Ari – Quando pensa em segurança da informação, a primeira coisa que vem à cabeça do gestor de TI é continuidade do negócio, e o primordial aí é um processo estruturado. Quando cria um processo estruturado, você mexe com pessoas, com o ciclo da informação e também com treinamento. Não adianta mexer com sistemas sem antes mexer com processos, não adianta mexer com processos sem antes falar em cultura e para falar em cultura tem que falar de treinamento. Outro aspecto importante é que estamos vivendo a era da mobilidade. Quando a gente está com um veículo em trânsito, por exemplo, eu estou pegando informação de um rastreador, que está passando pela Internet e pode ser captada por alguém. A melhor forma de proteger essa informação é conscientizando as pessoas.

IH – Além do trabalho de conscientização, quem cuida de fazer essa vigilância?

Ari – São processos subdivididos. TI cuida de tudo que envolva comunicação e telecomunicações, celular, dispositivos móveis, Internet. Mas existe a parte de controle de risco da empresa, que tem equipes voltadas para a segurança não só da informação mas também da mercadoria e dos itens que estão dentro da empresa, como câmeras, dispositivos de controle de acesso até o caminhão. O que tem aconteido é que o mercado está cada vez mais reativo: a cada vez que você cria métodos para se proteger, aparecem outros métodos para furar essa proteção. Por exemplo, quando você coloca um dispositivo de segurança dentro de um veículo, essa informação é confidencial: ninguém pode saber onde está colocado e de que forma esse dispositivo vai atuar. Essa informação fica restrita a poucas pessoas dentro da empresa, através de um documento, mas na hora de uma revisão o veículo tem que ser desbloqueado e isso acaba tendo que ser divulgado. Imagine a cada manutenção ter que mudar o dispositivo de lugar. Por isso a gente tem que ter dentro e fora da empresa equipes e fornecedores envolvidos no processo de segurança.

Carlos – Não podemos esquecer que, quando se fala em segurança da informação, a área jurídica é essencial, e nem sempre ela é consultada. Existem informações que têm que ser armazenadas por cinco, dez, 15 anos, e eu vejo que muitas vezes as áreas que estão em volta da TI não têm esse conhecimento. Nós temos uma enorme variedade de equipamentos móveis na rua, como os coletores de dados, que têm dentro deles todas as informações da companhia. Se eu tivesse orçamento, ampliaria essa área, para fazer todo o mapeamento desses equipamentos.

William – Nós não temos uma área específica de segurança e não temos uma política de segurança de informação formal implantada. Se eu não tivesse restrição orçamentária, eu implantaria a política de segurança da informação na empresa com

uma equipe específica, não necessariamente interna, mas não abriria mão de ter uma equipe de auditoria participando, sempre em sintonia com a área jurídica. E seria fundamental fazer a segregação de responsabilidades, para evitar de ter só a equipe técnica tenha acesso a tudo, o que não é correto. Seria importante também ter uma equipe para validação de códigos, porque temos sistemas desenvolvidos internamente. Outro ponto é uma atenção especial com relação a arquivamento de informações. Por mais tempo que passe, uma hora você vai desativar um sistema cujo backup você fez numa mídia A, B ou C e quando você precisar restaurar isso, depois de três, quatro anos, não tem mais aquele sistema, não tem mais aquela mídia. Às vezes você pode até ter como recuperar a mídia, mas não tem todo o aparato de hardware para reprocessar alguma informação.

Rogério – O Grupo TV1 tem seis unidades de negócio. Os nossos colaboradores são muito jovens, com média de idade entre 25 e 28 anos, e essa geração está vindo com outra cabeça, com outras necessidades. Nós temos uma política formal de segurança da informação. Quando criamos essa política, nós chegamos para o presidente da empresa e perguntamos para ele o seguinte: qual é o nível de segurança que você quer ter na empresa? E avaliamos duas vertentes: o risco do negócio e a estratégia de negócio da empresa. Numa empresa como a TV1, que é de comunicação e marketing, se eu tiver uma política muito restritiva, vou parar as unidades de negócio. Quando você faz uma política de segurança, tem que levar em consideração qual é a estratégia de cada uma das áreas de negócio, para que essa política não prejudique essas áreas. Embora eu tenha uma política de controle do ciclo de vida da informação, esse é um grande desafio. Se eu tivesse que investir em alguma coisa, buscaria ter mais tempo para a conscientização das pessoas: esse é o fator essencial. Hoje eu não tenho restrição de orçamento com relação à segurança, em termos de tecnologia. Tenho auditoria externa, feita por uma empresa que mensalmente me envia um relatório de vulnerabilidades. Nós fazemos testes de vulnerabilidade uma vez por ano, eu contrato uma empresa para fazer um teste de invasão, para saber até onde ela vai chegar.

Villaça – É técnico, não é?

Rogério – Essa pessoa não sabe nada da empresa, eu não dou nenhuma informação para ela e ela tenta chegar até os meus servidores, por exemplo. Hoje um grande problema é o volume de dados. Nós temos uma política de que a cada seis meses, quando o arquivo não é utilizado, é jogado para uma área e depois dessa área é feito o backup. Muitas vezes dizem que precisam dessa informação de volta. Então, se eu tivesse mais tempo, gostaria de conscientizar as pessoas de que nem toda informação precisa ser guardada.

IH – E que tipo de incidente é constatado com mais frequencia nessas auditorias?

Rogério – Normalmente são vulnerabilidades em patches de atualização.

Astorga – Meu sonho era de fato ter orçamento para ter uma equipe de segurança dedicada. Mas eu não acredito numa área de segurança que seja da TI, porque, pela minha experiência, é muito comum o CIO dar um jeitinho. Na minha opinião, a área de segurança tem que responder direto para o CEO e ponto final. Pode ser uma opinião polêmica, mas em geral é assim: segregação de papéis para mim é fundamental nesse ponto.

Moacyr – Nesse ponto, eu vivi uma situação estranha: tinha que me reportar ao CEO aqui no Brasil e tinha um chefe na França, que cuidava de todas as unidades. Um queria liberar e o outro queria trancar. Era extremamente complicado, porque um falava que segurança é a nossa preocupação, aí o outro falava que precisava fazer negócio.

"A regra lá é essa: todo mundo é dono da informação e todo mundo tem que zelar pela informação. A informação não é da TI, é da empresa."

Marcos, da Bueno Netto

IH – O francês era um CIO, um CTO ou um executivo de negócios?

Moacyr – Era o CSO do grupo, cuidava de toda a segurança de informação do grupo nos 28 países. Então o que ele falava de certa forma tinha muito peso no board.

Astorga – Tinha auditoria interna também separada ou não?

"Não adianta mexer com sistemas sem antes mexer com processos, não adianta mexer com processos sem antes falar em cultura e para falar em cultura tem que falar de treinamento."

Ari, da Expresso Jundiaí

mesa-redonda

fotos Guilherme Ko Freitag

“Não podemos esquecer que, quando se fala em segurança da informação, a área jurídica é essencial, e nem sempre ela é consultada.”

Carlos, da Wickbold

Moacyr – Nós tínhamos uma área de controle interno do grupo. Basicamente ele vinha para verificar como andavam os processos de controle e segurança.

Dario – Na minha empresa nós passamos por esse processo. No passado, toda a parte de segurança da informação ficava dentro da TI e posteriormente foi criada uma área de compliance e gestão de risco, com toda a questão das políticas e da auditoria. Ela está segregada, respondendo direto para o presidente e a parte mais operacional e técnica de implantação e administração de tecnologias permanece dentro da TI. Então, as normas são definidas externamente e nós temos que garantir que os sistemas respondam àquelas normas.

Douglas – Nós tínhamos um cenário que era dentro de TI, antes de a empresa ser adquirida pelo grupo. Uma vez adquirida pelo grupo, o CSO que está na Alemanha nos visita frequentemente. Ele começou um trabalho de troca de cultura, depois entrou com algumas ferramentas e agora faz só a manutenção, que é basicamente auditoria. Então a cultura já está implementada, nós seguimos as melhores práticas que ele envia e ele reporta diretamente ao board. Ele não tem ligação nenhuma com a área de TI.

Ari – Apesar de ser uma empresa familiar, eu tenho uma equipe de risco que é separada de TI, mas ela olha para a TI da seguinte forma: eu tenho que aplicar as ferramentas de proteção e ela me monitora com relação ao uso das ferramentas de proteção.

Douglas – É a mesma coisa.

Ari – O foco da equipe é voltado para a operação, mas ela olha toda a gestão de risco, tanto da informação quanto do negócio. Então ela está sempre com as duas visões.

Carlos – Eu também entendo que a área de segurança da informação não deveria fazer parte do escopo de TI, embora hoje na Wickbold ela faça. Estando fora, ela traz mais credibilidade para a companhia, porque às vezes os departamentos entendem que, como faz parte da TI, a TI não assume aquelas práticas. Então, com uma área de compliance fora da gestão de TI, realmente a credibilidade aumentaria e eu acho que o resultado seria bem melhor.

Fernando – Eu concordo que a área de segurança da informação tem que se reportar ao board, para descaracterizar a intervenção da TI. Informação é TI, então é a TI que está segurando, está burocratizando. Tem que quebrar esse paradigma, ou seja, não é a TI que está impedindo alguma coisa, é a empresa.

Moacyr – Eu concordo que, se a gente consegue ter a área de segurança da informação fora de TI, a visibilidade vai ser outra, não vai ser só de ativos eletrônicos, vai ser a informação como um todo, desde o que vai no papel até o que está guardado num disco. Mas não é só isso que vai resolver o problema. O que faz a diferença em todo o processo são as pessoas. Outra coisa importante é que as regras têm que ser claras e válidas para todos. Isso já fez efeito em níveis muito importantes da companhia, pessoas perderam o emprego porque fizeram coisas fora das políticas. A gente pode gastar o dinheiro que for em tecnologia que não resolve.

Fabio – Na prática eu concordo, acho que hoje na maioria das empresas seria melhor a segurança da informação sair de TI. O que acontece é que depende muito do nível de maturidade de cada empresa.

Astorga — Hoje a nossa preocupação, na Abyara, é ainda maior porque eu trabalho com informações de clientes dos meus clientes. São informações sensíveis, de renda, de investidores, o mercado imobiliário envolve muito dinheiro. Então hoje existe um trabalho na Abyara de valorizar a informação dos nossos clientes. Imagina quanto valeria uma informação sobre o nosso cliente, que em geral é um ivestidor.

IH – O que significa valorizar a informação do cliente? O que vocês fazem na prática para isso?

Astorga – É, por exemplo, conter o entusiasmo de divulgar que determinada celebridade comprou vários imóveis. Então é preciso conter esse impulso de compartilhar essa experiência com os amigos, porque

“Seria fundamental fazer a segregação de responsabilidades, para evitar de ter só a equipe técnica com acesso a tudo, o que não é correto.”

William, do Grupo D’Avó

junto acabam indo os dados confidenciais do cliente. Outra questão importante é a da legalidade da informação. O pessoal sempre fala muito de confiabilidade, integridade e disponibilidade. Mas e a questão da legalidade dessa informação? De onde veio, como ela foi obtida? Veio desviada de uma empresa concorrente? Na rua Santa Ifigênia, no centro de São Paulo, comprei um HD usado que provavelmente devia ser de uma pessoa do financeiro: tinha balancete, várias informações de crédito. Descobri a empresa, entrei em contato com a pessoa e levei o HD para ela. Ela não acreditou. Então, tão importante quanto guardar é descartar corretamente a informação. Mas basicamente eu queria orçamento para ter gente, porque as áreas querem acelerar os processos e por isso mesmo não querem mandar para o pessoal da segurança.

Vllaça – E o que você pensa sobre segurança na nuvem?

Astorga – Controle da nuvem é uma coisa que a gente deveria ter há muito tempo. Quem tem datacenter em outsourcing já deveria ter controle, já deveria auditar periodicamente. Para mim não mudou muita coisa, a única diferença é que saiu do servidor dedicado, que você sabe onde fica.

Villaça – A gente vê histórias escabrosas de vazamento de informação de quem usou backup na nuvem. Ainda acho que é bem diferente armazenar ou processar alguma coisa na nuvem de usar máquina virtual num datacenter.

Moacyr – Acho que aí se trata de um conceito diferente para cada um. Eu tenho o meu, posso enxergar a Cargill como tendo uma nuvem há anos, porque nós temos sistemas rodando espalhados pelo mundo inteiro e a gente acessa de qualquer ponto. É uma nuvem privada, há anos é desse jeito. Acho que tem muita gente rotulando soluções de hosting, de retail colocation, como cloud computing. Para mim é um buzzword. Eu não consigo encontrar uma boa definição de cloud computing.

Douglas – Eu concordo com o Moacyr que é marketing. Para mim, cloud é aquilo que eu tenho certeza de que roda em diversos datacenters de endereços físicos diferentes e que isso é load balance, numa transação ele entra aqui e pode responder por outro que está em outro lugar. Isso é muito difícil de ser feito.

Moacyr – Mas quem tem alguma coisa transacional que funciona assim? Não existe. No nosso mundo, que é o mundo de negócios que tem transações, você já tentou ver o que envolve dois datacenters trabalhando em load balance?

Douglas – Nós temos em load mesmo. Uma divisão da empresa, que faz transação financeira, tem dois datacenters que trabalham em load nos Estados Unidos. Ele não replica transação feita, ele pode responder o que o outro não respondeu. É bem complicado. Tem dois na Europa em outro negócio.

Moacyr – São dois. Imagine tentar fazer isso em grid. Não vale a pena.

Douglas – É um dinheiro incomensurável. Independente de fazer só virtualização ou cloud, não importa o nome que você dê, se você tirar da sua empresa, quando você compra processamento, independente se é on demand ou não, o que a gente percebe é que se você comprar de uma empresa que está fora, desaba o custo. Essa é a grande pressão, o hardware no Brasil é muito mais caro, qualquer coisa para colocar aqui dentro é muito mais cara, eletricidade é muito cara, nós temos um custo nacional.

IH – E que impactos isso gera para para a empresa do ponto de vista da segurança?

Douglas – A partir do momento em que você economiza em máquina, você vai gastar em outra coisa e pode gastar em segurança. É um caminho normal. E você iguala a realidade da sua empresa, a sua realidade brasileira, à realidade mundial. Se você está hospedando fora, literalmente você comprou o espaço e está por trás de uma estrutura de segurança que provavelmente você não teria condição de

> “Quando você faz uma política de segurança, tem que levar em consideração qual é a estratégia de cada uma das áreas de negócio, para que essa política não prejudique essas áreas.”
>
> Rogério, do Grupo TV1

> “Na minha opinião, a área de segurança tem que responder direto para o CEO e ponto final.”
>
> Astorga, da Abyara

mesa-redonda

foto Guilherme Ko Freitag

“Informação é TI, então é a TI que está segurando, está burocratizando. Tem que quebrar esse paradigma, ou seja, não é a TI que está impedindo alguma coisa, é a empresa.”

Fernando, do Banco Cacique

ter.

Dario – Eu acho que essa discussão toda acontece porque é uma quebra de paradigma. Tudo no final das contas depende do aspecto econômico. A nuvem na verdade leva a ganho de escala, especialização e redução de custo. Então a questão é como eu me movo para esse mundo onde tenho otimização econômica e me protejo. Essa é a grande discussão.

Douglas – Quando se fala em assuntos como treinamento, descarte de informações e cultura, acho que tudo se resume a uma coisa só: processos. Se você tem bons processos, você treina melhor, busca a ferramenta melhor. Se você tem bons processos e ferramenta melhor, impacta a cultura de maneira mais decisiva. De tudo que eu vivi até hoje, o meu maior problema no processo de tratar a informação é classificá-la. Se eu classifico bem, sei quando descartar. Se eu tenho uma informação transacional qualquer que está armazenada há 14 anos e devidamente classificada, eu tenho um motivo para ela estar armazenada. Se ela não está mais armazenada e eu já descartei, é porque também ela foi classificada de maneira tal que depois de X anos eu poderia descartá-la. Aí eu evito o que o Moacyr comentou de ter um monte de coisas armazenadas e não recuperar nada, porque eu classifiquei bem a informação. Para classificar informação, nem o PIB dos Estados Unidos seria suficiente, porque informação entra todo dia, sai todo dia e amanhã ela tem que ter uma classificação nova, é um budget eterno. O grande desafio é ter ferramentas que classifiquem automaticamente a sua informação. Antes de classificar, você vai ter que criar o seu método de classificação. Por mais que tenha melhores práticas, ele é seu, é você que sabe se a informação é só dado, se é algo descartável ou se ela é útil. Sendo útil, o quão útil. Se além de útil ela for confidencial, quais os níveis de confidencialidade. Ter um software que automaticamente classifique e diariamente reclassifique as informações para mim é o grande desafio. Hoje o nosso trabalho está ligado a classificar informação, melhorar o processo e adequar.

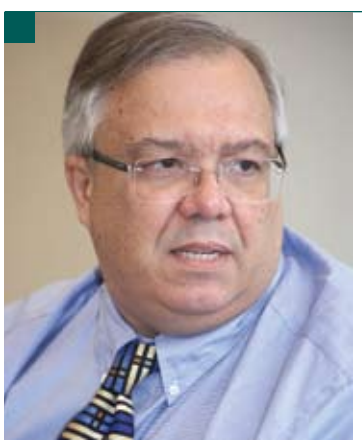
IH – Uma vez que a informação na origem já não foi classificada, como você recupera?

Douglas – É o mais complexo, e o problema não é só se ela não foi classificada na origem, mas também se durante algum período ninguém a reclassificou. Por exemplo, recebi um e-mail que tinha uma informação relevante e sem comentar com ninguém mantive num dispositivo móvel, ela não recebeu classificação, o dispositivo móvel a atualizou em mais algum lugar e pronto, está feito o estrago. Então, se pudesse investir dinheiro hoje investiria em uma ferramenta que ajudasse no meu processo de classificação, que ela atualizasse automaticamente e já me indicasse como tratar cada informação. Além disso, seria ótimo se eu pudesse aumentar a equipe de monitoria.

IH – Como você aborda essa questão da classificação das informações no Big Data, com esse volume incontrolável de informações que são geradas em pontos completamente diferentes?

Douglas – Eu tive contato com algumas ferramentas, que fazem bastante coisa. Uma vertente de uma dessas ferramentas era: uma vez saneado, classificar. Então eu comecei a observar o que eles tinham criado. Realmente é muito flexível, tem que ser baseado no processo que você construiu dentro da sua empresa, baseado no seu negócio. Mas você precisa conseguir que ele seja flexível o suficiente para aceitar todas as regras do seu negócio. É muito difícil, mas eu já vi empresas chegando lá.

Dario – Eu queria tratar o assunto sob outra perspectiva, a perspectiva da gestão do conhecimento. Existe um grande dilema nas empresas entre disponibilizar e proteger a informação. Geralmente os investimentos maciços são feitos na proteção da informação, que é uma obrigação. Proteger a informação confidencial, a informação sensível e a informação privada é uma obrigação; a preocupação com a falta de proteção é tão grande que viabiliza os orçamentos. Mas a gente não vive só de proteção,



“Acho que tem muita gente rotulando soluções de hosting, de retail colocation, como cloud computing. Para mim é um buzzword.”

Moacyr, da Cargill

também vive de oportunidade e a oportunidade está no uso e na disponibilização da informação. A informação só é útil quando está na cabeça das pessoas, se transformando em conhecimento, e pode ser aplicada na prática para transformar os negócios. Se eu tivesse um orçamento irrestrito, investiria intensamente em processos de gestão do conhecimento. A gestão do conhecimento, ainda mais nos tempos do Big Data, envolve uma série de coisas. Por exemplo, uma das áreas novas é a área da pesquisa de informações não estruturadas, de informações em mídias variadas, que consiste em buscar informação em áudio, em texto, em mídia social, em vídeo e ter uma forma de classificação e de seleção dessa informação. Nós contratamos auditorias independentes para fazer testes de vulnerabilidade todos os anos. Dependendo da dinâmica da entrada de projetos, a gente faz isso mais de uma vez ao ano. Os usuários dos nossos sistemas estão espalhados, estão na rede, os nossos sistemas são web, então nós temos uma preocupação muito grande de proteção ao acesso a esses sistemas e às bases de informação. Por exemplo, para os agentes acessarem nossos sistemas, eles têm um esquema de segurança, autenticação de três fatores: têm que entrar com token, com autenticação digital e com senha. A gente tem essa preocupação muito grande, mas não adianta nada só restringir, porque a informação só se transforma em conhecimento quando é acessível. A gente tem que dar acesso à informação de forma seletiva, buscando aquilo que tem relevância, mas tem que dar acesso. Então, investir em processos e sistemas de gestão do conhecimento é fundamental para transformar o negócio e aumentar o valor da empresa.

Ari – Eu me lembro de quando estava numa reunião da cúpula da outra empresa em que trabalhava e a gente ia mudar a estratégia de negócio. A primeira coisa que se discutiu, antes de apresentar qualquer informação, foi um contrato, que regia a confidencialidade.

Dario – É interessante. Quando o Ari falou sobre o contrato, pegou o papel e olhou para ele. Hoje nós vivemos numa sociedade digital, o contrato não está mais no papel. Antigamente, você tinha um contrato em papel. Como você protegia esse contrato? Botava no cofre. Hoje os contratos são digitais. Embora a gente coloque os servidores na sala-cofre, a informação não está presa no cofre, ela está acessível através da rede. Proteger essa informação é cada vez mais difícil. A minha empresa administra mais de 40 mil contratos, todos em formato digital, todos nos sistemas, todos confidenciais. São arquivos digitais e eles estão na rede de alguma forma. Então, essa complexidade toda de gestão da segurança se multiplicou.

Sérgio – Uma fórmula que me pareceu funcionar muito bem é a criação de uma comunidade de segurança da informação: a pessoa responsável por segurança da informação reporta para o CFO, mas cada departamento é responsável por segurança da informação. Então existem métricas nos departamentos. O departamento de TI tem o security officer, que responde por segurança da informação dentro do departamento de TI. O RH tem o security associate, que responde por segurança da informação dentro do departamento de RH. E todos eles reportam através de métricas claras para o CFO. Isso tem algumas vantagens muito interessantes, como, por exemplo, agilidade, time to market. O RH tem alguém que não é um expert em segurança, mas tem ideia do que a gente está falando ali no RH, então ele reage rápido. Mas isso requer, de novo, cultura da empresa. Leva um tempo para chegar nesse grau de maturidade, mas eu acredito que esse é o modelo que funciona melhor.

IH – Vocês acham que a tendência é de que precisem cada vez mais de apoio externo de empresas especializadas para fazer esse trabalho?

“Para classificar informação, nem o PIB dos Estados Unidos seria suficiente, porque informação entra todo dia, sai todo dia e amanhã ela tem que ter uma classificação nova, é um budget eterno.”

Douglas, da Epay Brasil

“A gente não vive só de proteção, também vive de oportunidade e a oportunidade está no uso e na disponibilização da informação.”

Dario, da CCEE

Villaça – Eu acho interessante usar produtos de terceiros em questões de segurança específica da informação técnica, porque o terceiro nessa situação tem uma coisa que a gente não tem, que é escala e abrangência de experiência. Por maior que seja a minha área interna de segurança da informação, seja ela do CIO ou não, alguém externo me ajuda em economia de escala, ele traz experiências que eu não tenho.