Blog Minuto da Segurança

CPO e CSO: Unidos pelas novas regulamentações!

Kleber Melo

CPO e CSO Unidos pela Lei!

CPO e CSO: Unidos pelas novas regulamentações! Duas das principais funções dentro das empresas estão cada vez mais sendo analisadas quanto à aplicabilidade dentro dos diversos requisitos de proteção de dados. O ***Chief Privacy Officer (CPO)*** e o ***Chief Security Officer (CSO)*** - ou um funcionário com responsabilidades semelhantes - são responsáveis pelo que poderia ser visto como responsabilidades mutuamente exclusivas, mas não mais.

Seus papéis e responsabilidades parecem se sobrepor e colidir.

"***Chief***" não significa necessariamente o status de nível C. Quando se trata de funções de conformidade em geral, "***Chief***" geralmente significa a pessoa principal na função, não uma designação de nível-C.

Com mudanças no atual ambiente regulatório, dentre os quais os mais proeminentes no momento, podemos citar:

- Lei de Privacidade brasileira (LGPD)
- Regulamentação 4658 do Banco Central do Brasil
- General Data Protection Regulation (GDPR)
- Lei Cibernética Chinesa
- Lei de Privacidade da Califórnia

As funções do CPO e do CSO estão se tornando mais reconhecidas, mais necessárias e mais colaborativas - não como funções isoladas em uma organização, mas como parceiros.

Apara efeitos deste artigo, vamos generalizar a função do ***Security Officer*** com o nome de CSO, mas também podemos vê-lo definido como CISO, sendo esta definição uma questão de semântica e reporte hierárquico. O CISO tende a trabalhar mais relacionado a tecnologia da informação, reportando-se ao ***CIO - Chief Information Officer***, ou Diretor de Tecnologia, e o CSO de forma mais ampla nas questão de informações, incluindo as questões de tecnologia.

Visão geral das funções

O papel do CISO e do CPO diferem na estrutura de relatórios, no escopo e na autoridade.

O **CPO** é responsável pela visão, estratégia e programa em relação ao uso de informações pessoais.

O **CSO** é responsável pela visão, estratégia e programa para garantir a proteção dos ativos de informação e tecnologias.

Do ponto de vista de reporte hierárquico, o CPO costuma se reportar a um conselho geral, diretor de conformidade e pode ter uma linha pontilhada para um conselho de administração. Em contraste, o CSO pode se reportar tanto ao diretor de tecnologia, diretor de informações (CIO) ou a qualquer outra diretoria (já vi reportes para Diretor de Risco, Diretor de Segurança Física e Fraudes, Diretor de RH, Diretor Financeiro, e vários outros), e talvez reportar-se a um CEO diretamente e também pode ter uma linha pontilhada para o conselho.

Em muitos casos, o CPO pode ter crescido no papel de dentro da organização, proveniente de TI, conformidade ou RH. Antes de sua proeminência recente, a privacidade era considerada uma função de meio expediente anexada às responsabilidades existentes de alguma outra função, onde as organizações pediam que as pessoas se ofereçam para assumir esse papel para preencher uma lacuna.

Com o tempo, o agente de privacidade ganhou experiência por necessidade ou é um advogado que pode ter se transformado no papel. O CSO, no entanto, geralmente vem de dentro de uma função de TI (infraestrutura de rede, desenvolvimento de software etc.) ou pode ter sido um ex-engenheiro que continuou a acompanhar as mudanças de tecnologias.

Privacidade e Segurança não é muito diferente em um ambiente de negócios em relação à informação. A segurança fornece proteção para todos os tipos de informações, de qualquer forma, para que a confidencialidade, integridade e disponibilidade das informações sejam mantidas. A privacidade garante que as informações pessoais (e às vezes informações confidenciais da empresa também) sejam coletadas, processadas (usadas), protegidas e destruídas legal e justamente.

É impossível implementar um programa de privacidade bem-sucedido sem o suporte de um programa de segurança.

Assim como as cortinas de uma janela podem ser consideradas uma proteção de segurança que também protege a privacidade, um programa de segurança da informação fornece os controles para proteger as informações pessoais.

Os controles de segurança limitam o acesso a informações pessoais e protegem contra seu uso e aquisição não autorizados. É impossível implementar um programa de privacidade bem-sucedido sem o suporte de um programa de segurança.

Assim como as barras de uma janela ajudam a impedir que intrusos entrem em sua casa, permitindo que as pessoas olhem para dentro, um programa de segurança pode implementar controles sem considerar a privacidade. Por exemplo, um programa de segurança pode exigir credenciais para acessar uma rede sem restringir o acesso a informações pessoais. Você teria segurança, mas não privacidade, pois qualquer pessoa com credenciais válidas pode ver todas as informações pessoais que sua organização possui.

No entanto, no que se refere a políticas, gerenciamento de fornecedores, violações de dados e relatórios para o conselho de administração, tanto o CSO quanto o CPO desempenham um papel integral e às vezes sobreposto para proteger a marca e a reputação de uma organização. Seus papéis como colaboradores e parceiros tornaram-se cada vez mais importantes.

Neste artigo, vemos os papéis como posições separadas, mas há um movimento em que os papéis são combinados. Quando combinada, a única função geralmente se encaixa em uma das duas fórmulas:

A CPO aceita as duas e tem uma pessoa forte de segurança da informação para confiar, não como um subordinado direto, mas como um parceiro. O diretor de privacidade e segurança pode gerenciar as políticas, enquanto a segurança da informação gerencia a implementação técnica.

O CISO assume a privacidade, tende a haver um escopo de expertise bem menos definido. O ***chief data protection officer*** (ou algum título semelhante) pode ou não ter um escritório de privacidade separado para tratar este assunto, em vez disso, enviar pessoal técnico para treinamento de privacidade.

Nenhuma segurança é infalível e nenhuma privacidade é absoluta!

Nenhuma das duas opções parece ser ideal em todos os sentidos, a empresa deve decidir o que funciona melhor para sua situação regulatória, prioridades e cultura. Em essência, nenhuma segurança é infalível e nenhuma privacidade é absoluta.

Quais informações um programa de privacidade protege?

Um programa de segurança protege todos os ativos informativos que uma organização coleta e mantém. Um programa de privacidade se concentra nas informações pessoais que uma organização coleta e mantém.

O que é uma informação pessoal? Esta é uma pergunta para a equipe de privacidade responder.

Uma maneira de definir informações pessoais é observar as leis e regulamentações aplicáveis. Muitas vezes, os estatutos e regulamentos definem informações pessoais como primeiro nome ou iniciais, juntamente com um número de identificação emitido pelo governo, informações de contas financeiras ou informações de saúde. Embora a proteção desse tipo de informação forneça proteção direta contra roubo de identidade, roubo de fundos e atos discriminatórios, essa definição é abrangente?

Considere um endereço de email. Para muitos sites da Web, um endereço de e-mail é metade das credenciais necessárias para fazer login. Além disso, se um endereço de e-mail de um indivíduo for obtido de uma determinada empresa, é fácil criar uma campanha de ***phishing*** confiável fornecendo uma comunicação desse tipo. o negócio.

Segundo a Lei de Privacidade brasileira, temos as seguintes definições em seu Art 5º:

> I - *dado pessoal*: informação relacionada a pessoa natural identificada ou identificável;
> II - *dado pessoal sensível*: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - ***dado anonimizado***: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Se uma definição legal para informações pessoais for usada, o endereço de e-mail pode não ser protegido adequadamente contra acesso não autorizado, nem as pessoas serão notificadas se o endereço de e-mail for perdido em uma violação de dados.

Um programa de privacidade precisa pelo menos considerar ir além da definição legal de informações pessoais para atender às expectativas das partes interessadas de sua organização. Uma definição mais ampla de informações pessoais é "***qualquer informação relacionada a um indivíduo identificado ou identificável***". Um programa de privacidade precisa, para sua organização, encontrar o equilíbrio entre a definição legal e a definição ampla de informações pessoais.

Protegendo informações pessoais

Dada a definição organizacional de informações pessoais como base, um programa de privacidade precisa definir os requisitos de processamento e proteção de informações pessoais. Os requisitos de proteção incluem itens como: quais funções organizacionais têm acesso às informações, quando e como as informações podem ser compartilhadas interna e externamente e quando e como as informações devem ser destruídas. Esses requisitos devem estar relacionados a informações pessoais em qualquer mídia, não apenas armazenadas eletronicamente.

Esses e outros requisitos relacionados à privacidade são fornecidos ao programa de segurança para implementar proteções e controles apropriados. Não cabe a um programa de privacidade declarar a tecnologia ou os processos a serem usados para proteger as informações pessoais (embora a equipe de privacidade possa ter opiniões valiosas); cabe aos especialistas em segurança fazer essa determinação.

Portanto, um programa de privacidade depende de um programa de segurança. Isso cria a necessidade de estabelecer um relacionamento cooperativo e interdependente entre as equipes (e o CPO e o CSO), ou mesmo combinar as duas funções em uma única diretoria, neste caso poderíamos propor a criação da função *Chief Security and Data Privacy Officer (CSDPO),* ou algo similar.

Políticas

O CPO é normalmente responsável pelas políticas a seguir, ou, se não, deve contribuir significativamente para a política final:

- Política de privacidade do site;
- Políticas de privacidade internas (por exemplo, política de privacidade do funcionário, política do escudo de privacidade do código de conduta - se aplicável);
- Padrões de classificação de dados;
- Padrões de solicitação de acesso a dados;
- Política de mídia social.

O CISO deve ser responsável pelo seguinte:

- Normas e requisitos de segurança;
- Política de Utilização Aceitável;
- Software de prevenção de perda de dados;
- Inventário de dispositivos;
- Controle de mídia removível; e,
- Controle de acesso, provisionamento, logs e outras relacionadas às questões técnicas de proteção da informação.

No entanto, dentro de cada uma das políticas acima, as funções devem colaborar e provavelmente envolver outros departamentos, conforme aplicável. Existem algumas políticas em que as duas diretorias precisam colaborar para ter um conjunto abrangente de políticas e abordagens. por exemplo:

- Diretrizes de gerenciamento de fornecedores, padrões de fornecedores e due diligence;
- Política de uso aceitável (também BYOD, Monitoramento, etc.);
- Violação de dados, política de resposta a incidentes e procedimentos;
- Treinamento de funcionários;
- Classificação e gerenciamento de dados.

E há políticas que não parecem pertencer a nenhuma destas diretorias, mas tanto o CPO quanto o CISO têm uma responsabilidade em relação a essas políticas, por exemplo:

- Políticas de retenção de dados;
- Política de desligamento de funcionários;
- Política de backups;
- Política de continuidade de negócios e contingência.

Vendor management ou Gestão de fornecedores

Com muitas regulamentações exigindo a devida diligência, a supervisão e o controle sobre os fornecedores (considere, o GDPR, o LGPD e a regulamentação 4658 do Bacen), o gerenciamento do fornecedor é um risco e uma vulnerabilidade importantes para as organizações. Como há uma falta geral de confiança no relacionamento do fornecedor, faça as seguintes perguntas antes de trabalhar com o fornecedor:

- O fornecedor divulgou alguma informação sensível ou você pode confirmar se um fornecedor teve uma violação de dados ou um ataque cibernético envolvendo informações confidenciais confidenciais?
- Você pode determinar o número de fornecedores com acesso a suas informações confidenciais e quantos desses fornecedores estão compartilhando esses dados com um ou mais de seus fornecedores?
- Esses fornecedores têm salvaguardas de dados, políticas de segurança e procedimentos equivalentes aos que você tem atualmente?
- Sua postura de segurança é suficiente para responder a uma violação de dados ou ataque cibernético?

Apesar dessa falta de confiança e apesar dos requisitos para exercer o controle, as empresas raramente conduzem revisões iniciais ou contínuas dos fornecedores de políticas e programas de gerenciamento de fornecedores para garantir que eles lidem com o risco do fornecedor. A falta de recursos dificulta que as organizações tenham um robusto programa de gerenciamento de fornecedores. As empresas dependem de obrigações contratuais, em vez de auditorias e avaliações, para avaliar as práticas de segurança e privacidade dos fornecedores.

A exigência desta supervisão tende a cair nas mãos do CPO ou do CSO, porque os executivos e os conselhos de administração raramente estão envolvidos no gerenciamento de risco do fornecedor. Vale a pena notar, no entanto, no caso de um incidente, como uma violação grave de dados ou violação de segurança, é o CSO e, talvez, o CEO que são responsabilizados diretamente mesmo que o fornecedor esteja em falta.

Para lidar com a supervisão do fornecedor, o CPO e o CSO devem trabalhar juntos para realizar a devida diligência e exercer supervisão contínua em combinação com a unidade jurídica e de negócios que se beneficia dos serviços e produtos.

As ferramentas disponíveis incluem ***due diligence*** inicial, relatórios de auditoria de fornecedores independentes, como um relatório de controles de organização de serviços e o desenvolvimento de padrões de verificação em torno dos cinco princípios do serviço de confiança:

1. ***Segurança***: O sistema está protegido contra acesso, uso ou modificação não autorizados.
2. *Disponibilidade*: O sistema está disponível para operação e uso conforme comprometido ou acordado.
3. *Integridade de processamento*: o processamento do sistema é completo, válido, preciso, oportuno e autorizado.
4. *Confidencialidade*: As informações designadas como confidenciais são protegidas como comprometidas ou acordadas.
5. ***Privacidade***: A coleta, uso, retenção, divulgação e descarte de informações pessoais do sistema estão em conformidade com os compromissos no aviso de privacidade da organização prestadora de serviços e com os critérios estabelecidos nas regulamentações nacionais e internacionais em vigor.

As entidades tendem a querer manter suas políticas em segredo, mas o cliente tem um requisito legal para exercer a devida diligência. Seja você o CPO / CSO do lado do cliente ou do fornecedor, você deve estar preparado para compartilhar políticas para atender aos requisitos de supervisão. Estas incluem todas as políticas listadas acima, juntamente com a prova de que as políticas são seguidas.

Além disso, o CSO precisa estabelecer uma abordagem baseada em riscos para testar as medidas de segurança dos fornecedores e estar preparado para que os clientes testem os seus próprios controles.

Compliance

Embora não seja o escopo deste artigo, falta-nos mencionar uma outra área que cada vez mais toma importância e relevância no cenário explorado acima e que direta ou indiretamente se relaciona e possui interdependência com ambas as diretorias, CPO e CSO. Esta área é Compliance !

Conforme definido por Robert Roach, vice-presidente e diretor global de conformidade da New York University, “***Conformidade é uma abordagem sistemática à governança projetada para***

garantir que uma instituição cumpra suas obrigações sob leis, regulamentos, melhores práticas e padrões aplicáveis, obrigações contratuais e políticas institucionais." Em outras palavras, ***"Compliance busca alcançar responsabilidade e transparência em todas as operações institucionais*** ".

Nesse sentido, ***Compliance*** é muitas vezes vista simplesmente como "cumprindo a lei" e, embora isso seja verdade em muitos aspectos, os profissionais de ***Compliance*** argumentariam que os programas de conformidade devem procurar dar um passo adiante. Profissionais de conformidade, especialmente aqueles com maior responsabilidade ética, muitas vezes procuram comunicar a conformidade como um "***compromisso de fazer a coisa certa***". Fazer com que os funcionários entendam que estar comprometido em fazer a coisa certa acabará resultando no cumprimento da lei. Objetivo principal de uma função de conformidade.

Os elementos geralmente aceitos de uma função de ***Compliance*** eficaz são vistos como as ferramentas que um profissional de conformidade pode usar para realizar essa missão. Os exemplos incluem o desenvolvimento de políticas e procedimentos para que os indivíduos tenham as informações necessárias para tomar as decisões corretas, bem como treinamento e educação para que os funcionários entendam as políticas e os procedimentos e apliquem suas responsabilidades diárias.

Como sabemos, em um setor altamente regulamentado, como o Financeiro, existe uma miríade de leis, regulamentos e orientação de agência com os quais as instituições devem obedecer. Mas, como os profissionais de conformidade costumam afirmar, a conformidade com esses requisitos é uma função comercial e não de responsabilidade do departamento de ***Compliance***. O escritório de ***Compliance*** suporta a conformidade operacional atuando como um gerenciador de portfólio da matriz regulatória, aproveitando o programa de conformidade para garantir que todas as obrigações da instituição sejam atendidas pelos especialistas no assunto no nível operacional.

Devido ao exposto a área de ***Compliance*** deve se integrar cada vez mais as áreas de Privacidade e Segurança da Informação, participando das definições de políticas e controles e garantindo a conformidade com todos os requisitos legais que estas outras duas áreas necessitam atender.

Conclusão

Há uma série de propostas de leis de privacidade atualmente em vigor e consideradas nacional e internacionalmente existem dezenas de leis de privacidade que estão em vigor, ou estão à beira de serem implementadas . A maioria, senão todas, inclui requisitos de segurança para garantir privacidade.

E sim, segurança e privacidade não são as mesmas coisas, mas são inextricavelmente relacionados. Eles são como uma casa, sem uma boa base (segurança), você não terá uma residência estável (privacidade). O pedreiro deve estar em comunicação constante e eficaz com o arquiteto para que você não acabe morando em um castelo de cartas.

Não adianta possuir excelente políticas de privacidade se não houver a adequada proteção e monitoração de dados implementada, política sem controle implementados não resolve o problema da organização.

As funções de CPO e CSO estão cada vez mais interligadas e , por força da lei, ganham agora a atenção definitivas dos conselhos administrativos das empresas. Talvez fosse esta a oportunidade que os profissionais das áreas de Privacidade e Segurança estivessem esperando para ganhar atenção e investimentos, oportunizando crescimento de carreira e uma evolução significativa na maturidade de proteção da informação. E por fim, "O Cliente Agradece!"

Textos Referências:
Lexology & CSO & Educause Review

Por:
Kleber Melo (kleber.melo@mindsec.com.br)
Sócio Diretor da MindSec Segurança e Tecnologia da Informação

---

MindSec

Empresa de consultoria especializada em Segurança da Informação, conta com consultores experientes e capacitados para auxiliar a sua empresa nos desafios diários trazidos pelas novas regulamentações e por novas vulnerabilidades. A MindSec oferece a seus clientes soluções diferenciadas para proteção avançada da informação, proteção de privacidade e informações sensíveis de negócio, de clientes, acionistas e colaboradores.

Consulte um especialista MindSec contato@mindsec.com.br

Representante Oficial: