IT'S TIME TO TALK ABOUT da itSMF sobre gestão da proteção de dados como fator de competitividade by design

A 26 de maio a itSMF realizou mais uma edição do IT'S TIME TO TALK ABOUT, desta vez sobre gestão da proteção de dados como fator de competitividade by design.

Filipe Pereira, Head of Digital Lead & Protection na LCG Consulting, foi o convidado desta sessão onde privacidade e segurança by design foram considerados os maiores e mais fortes níveis de competitividade e que acompanham as equipas de segurança de informação e desenvolvimento. A questão que se coloca é até que ponto as organizações estarão preparadas para responder aos desafios e o porquê da competitividade surgir como prioritária neste momento.

Toda a componente de TI de mobilidade e o que o 5G trará, vem alterar completamente a forma como estamos habituados a trabalhar, com reflexo inclusivamente na legislação que está a acompanhar estes desenvolvimentos já com o foco na inteligência artificial.

No entanto, na generalidade dos casos, Filipe Pereira considera que há uma preocupação do que a inovação possa vir a ser e não damos espaço à inovação porque queremos colocar restrições na forma como tudo isto tem impacto na sociedade. “É a velha dicotomia, a velha discussão de que o progresso está aí, não vai parar, temos que o permitir e, por outro lado, temos que ter muito cuidado com o impacto que o progresso possa implicar”, afirma.

Exemplo deste receio é, não só a gestão das cidades do futuro, mas também a recolha de dados biométricos para efeitos laborais cuja utilização se exige que apresente benefícios concretos para os cidadãos.

Assim, concluímos que, efetivamente, **as organizações não têm confiança para implementar todas essas transformações que são necessárias a médio e longo prazo.**

Para dar esse passo em frente, Filipe Pereira considera que é necessário potenciar uma governação corporativa que identifique os riscos ao invés de correr atrás do prejuízo, facilitando trocas de informação e comunicação interna entre departamentos. Há muitos valores humanos nas organizações que não têm espaço para fazer valer a sua voz - opiniões concretas e ideias, mas, por outro lado, as empresas também têm receio de perder os seus colaboradores e não devem tê-lo.

A taxa de conversão de clientes ou índice de fidelidade são indicadores de competitividade, mas que têm necessariamente que ser integrados desde o início dos processos. **Para haver uma boa infraestrutura técnica, abrangente e eficiente, a instituição tem de ter estabilidade económica e uma boa base de formação dos seus colaboradores.**

O tamanho do mercado é essencial para a componente competitiva e a sofisticação da cadeia de abastecimento também é um fator de diferenciação muito importante na hora de escolher ou reter uma determinada relação profissional de prestação de serviços. E **se não somos transparentes na forma como tratamos os dados dos nossos clientes, muitas vezes perdemos essa confiança, pelo que a proteção de dados não deve ser vista como uma camada extra, mas sim uma dimensão estratégica para garantia de competitividade.**

Por outro lado, o risco de ser vítima de um ataque de hackers ainda é muito ignorado pelas organizações por desinformação ou desconhecimento do investimento que deve ser feito. Sensibilização e informação sobre estas questões são quase nulas ou inexistentes.

Conformidade à força

Conformidade a longo prazo passa por: diagnóstico e implementação de sistemas de conformidade, avaliações, auditorias e análise a longo prazo.

Contudo, muitas empresas têm poucos recursos para praticar este ciclo de garantia da segurança de informação. Filipe Pereira, pela experiência em trabalhar com estas questões, acredita que “só quando se fala em multa é que as organizações ponderam disponibilizar verba para fazer face às questões levantadas na manutenção de segurança de dados. As limitações orçamentais são uma barreira concreta à forma como as organizações se preparam”.

Conformidade não é apenas cumprir um conjunto de pontos, fazer um novo requisito de avaliação de conformidade e esperar mais um ano; implica uma definição e visão estratégica sobre operações de risco e cibersegurança na experiência do cliente.

“Soluções de segurança digital implicam custos, mas são bastante importantes. Um plano estratégico de segurança na organização tem sempre de existir”, sublinha Filipe Pereira.

Portanto, **a gestão de segurança da informação ou um sistema de gestão de proteção de dados tem que contemplar soluções de segurança digital.**

Para haver um planeamento estratégico num nível mais básico de maturidade, é necessário começar a apostar na formação e sensibilização. As implementações de base de segurança muitas vezes não existem, mas são essenciais na gestão de dados - não apenas os dados pessoais, mas os dados trocados entre a organização e os seus clientes. Uma organização competitiva é a que processa estes dados com segurança e que dá condições aos seus colaboradores para tratarem devidamente os seus dados.

Filipe Pereira aponta, ainda assim, uma solução ao dispor das organizações que têm menos conhecimento na matéria: "quando não há recursos internos já se verifica muito o CISO as a Service - Chief Information Security Officer. O DPO e o CISO têm pontos de interação muito grandes. Nada disto fará sentido e será apenas a criação de obstáculos em cima de obstáculos se os responsáveis das organizações não o virem como uma mais-valia em termos de crescimento".

No apurar de responsabilidades existem instituições como o Comité Europeu de Proteção de Dados, a autoridade nacional quanto à Proteção de Dados, a CNPD, e ainda existe a tutela ou grupo, no caso da administração pública.

RGPD e Lei de Execução têm que responder às exigências dos controladores e tudo isto emana da legislação. Na componente da proteção de dados há uma sugestão de políticas e processos-tipo que podem ser identificados à partida.

Cabe aos controladores o verificar da lógica de uma recolha de dados com informação sobre o titular. Tem que haver uma garantia de definição de finalidade legítima de retenção e eliminação dos dados pessoais. Tem que haver a consciência do porquê de se manter o mapeamento das atividades e do seu processamento ao abrigo da proteção de dados e segurança de informação.

Maturidade das organizações

As organizações avançam na sua maturidade à medida que vão passando pelos problemas e os vão ultrapassando.

"Numa perspetiva corporativa eu acho que o conceito acaba por ser muito mais facilmente integrado e corresponde precisamente também aquilo que nós estamos a falar em termos de conceito de maturidade. Mas se olharmos para o conceito em termos de psicologia, a maturidade começa quando o drama termina", descreve Filipe Pereira. A melhor forma de fazer análise de riscos é com sabedoria e calma. Primeiro há que fazer uma identificação de quais os riscos e as sanções e coimas são aquilo a que as administrações mais atenção dão. Depois surge a questão do dano reputacional, que é muito importante e que tem tudo a ver com a componente da confiança que os clientes têm.

Tem que existir um reforço da segurança física e digital, uma gestão da mudança comportamental e alteração processos, quando necessário.

A aplicação e manutenção da conformidade deve ser vista como um plano integral de continuidade e não apenas pontual.

O nível de maturidade mais elevado é o da consciência orgânica em que a organização entende, claramente, que tem de haver respeito pelos dados das pessoas. Ter respeito pelos dados do cliente é a melhor forma de identificar o serviço de valor acrescentado que conseguimos transmitir e garantir uma boa relação de confiança.

Assim, fica claro que uma maior maturidade implica também a possibilidade de incidentes ou erros que promovam a melhoria de qualidade no serviço desde que os responsáveis pelas organizações estejam dispostos a aprender com esses erros, bem como a fazer um melhor aproveitamento dos recursos para corresponder a estas lacunas.

Resumindo, conformidade é uma forma de obter diferenciação e confiança dos titulares.

Na fase de perguntas e respostas, António Bento, da Direção do itSMF, começou por perguntar se, na generalidade das organizações, há maior sensibilidade e conhecimento sobre o GDPR.

Filipe Pereira responde que passados três anos da sua aplicação, ainda há um nível de maturidade relativamente baixo, dado o pouco investimento que tem sido feito e a discussão pública ser quase nula (a discussão acontece em pequenos fóruns com pouco mais de meia centena de pessoas).

“Acho que as administrações ainda não estão devidamente sensibilizadas nem têm noção do que terão de fazer. O debate não aconteceu; o que aconteceu foi injeção de informação”, acrescenta.

Na administração pública há profissionais que estão mais sensibilizados e são mais conhecedores do tema do que outros. Já as PMEs só vão sentir na pele esta urgência quando as entidades financeiras começarem a exigir alguns níveis de critério de requisitos de segurança para poderem, por exemplo, ter acesso a linhas de crédito ou poderem candidatar-se a determinados projetos de inovação.

Mas será que as empresas mais inovadoras já bebem deste potencial do que o by design na proteção de dados e na privacidade pode trazer?

Tudo tem a ver com a capacidade e maturidade das pessoas que hoje estão à frente dessas ideias de negócio ou que apoiam e orientam essas ideias de negócio. A privacidade é uma condição sine qua non. As PMEs não têm formação contínua e é necessário garantir que têm essa formação.

Mas se há uma organização que tem uma forte componente de inovação, essa acaba por fazer parte de um dos pilares *core* do seu desenvolvimento.

O próximo encontro do itSMF, online, acontece a 16 de junho.