Agosto 2006

Trajetória Profissional: Mercado Internacional

1) Como você descobriu a segurança da informação? Onde mais você atuou com segurança?

Minha trajetória profissional é um tanto atípica, pois antes mesmo de ingressar na faculdade, já havia iniciado a operação de uma pequena empresa de treinamento, desenvolvimento de software e arquitetura de soluções de automação comercial. Desde então, programando sistemas de informação e provendo também a infra-estrutura de redes, como base para a operação e controle de empresas de varejo, tomei consciência dos primeiros aspectos de seguranca da informação ligados à proteção de software, controle de acesso, virus, integridade e continuidade. Durante os nove anos de operação da empresa, algumas mudanças de posicionamento ocorreram como reflexo do mercado e de meus próprios interesses profissionais, levando-a a focar em serviços de consultoria de tecnologia da informação adicionando componentes de segurança. Foi quando então decidi me aproximar definitivamente do mercado de consultoria e descobri a Modulo Security em destaque no mercado brasileiro, dedicada ao segmento de segurança da informação, e oferecendo um terreno fértil para ampliar minhas habilidades, alinhar minha carreira e aprofundar os estudos no campo da seguranca da informação. Foi certamente uma das passagens profissionais mais ricas que experimentei pelo fato de ter encontrado estudiosos, entusiastas e visionários dedicados a seguranca da informação e com disposição para desenvolver produtos e serviços inovadores. Desde então me dedico ao campo da Seguranca da Informação, agora mais voltado à Gestão de Negócios, tendo prestado consultoria para inúmeras empresas nacionais e internacionais, gerenciado grandes projetos e conduzido o desenvolvimento de produtos e serviços profissionais. Tudo isso acompanhado de pesquisa contínua, o contato com outros especialistas do setor, a publicação de artigos, livros, ministrando palestras e lecionando em cursos de MBA e em treinamentos executivos. Nos últimos anos tenho me concentrado no gerenciamento de negócios de consultoria em empresas multinacionais, inicialmente na Schlumberger e Atos Origin Brasil, e desde 2005 na Atos Consulting, Inglaterra.

2) Qual a sua formação?

Minha formação é fundamentalmente em TI com especializações voltadas para a área de negócio. Cronologicamente falando, sou formado como Bacharel em Ciência da Computação, Pós Graduado em Redes, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Internacionalmente certificado CISM - Certified Information Security Manager e BS7799 Lead Auditor e concluindo especialização em Negociação e Estratégia pela London School.

3) Qual foi o caminho para que você se tornasse um profissional de segurança fora do Brasil? Por que essa escolha?

O caminho do mercado exterior surgiu naturalmente por força da necessidade pessoal de manter a carreira em crescimento e a percepção de momentânea saturação do mercado Brasileiro em decorrência da minha última ocupação como Gerente da Divisão de Consultoria de Segurança da Informação da Atos Origin para a América Latina. Após montar a operação da nova unidade de negócios no Brasil, formar a equipe de consultores, especialistas e entregar com sucesso grandes projetos de consultoria a clientes globais pela América do Sul por dois anos consecutivos, tal resultado gerou a exposição internacional que resultou em um convite irrecusável vindo da Atos Origin UK. A decisão de aceitar o convite não requereu muito esforço visto que muitos fatores relevantes, tanto pessoais e profissionais, estavam alinhados.

4) Você consegue identificar diferenças no mercado de segurança do Brasil e da Itália, ou da Europa?

As diferenças existem. Algumas mais perceptíveis que outras, mas em geral, os problemas de segurança são comuns, diferindo consideravelmente na forma como são enxergados, qualificados e tratados. A tolerância aos riscos da informação varia de setor para setor e de país para país. Mais conservadores, os Ingleses investem mais tempo em testes, validações e documentações, enquanto que os Italianos preferem ver tudo funcionando antes de iniciar uma depuração mais elaborada. São apenas alguns sinais, mas que não podem ser usados para generalizar, considerando que esses comportamentos tendem a oscilar entre setores de um mesmo país. De qualquer forma, comparando o comportamento Europeu com o Brasileiro, percebe-se a nítida valorização das pesquisas e dos processos de segurança da informação, estes mais elaborados, alinhados com padrões mundiais e amparados por farta e detalhada documentação, enquanto que nós Brasileiros preferimos a resposta rápida e o *time-to-market*. Na prática, o comportamento médio Europeu pode ser traduzido pelo trinômio: pesquisa, planejamento e teste, enquanto o Latino médio pode ser representado pelo trinômio: experiência, ação e customização. Estas diferenças não representam necessariamente inferioridade ou simplesmente irresponsabilidade do Latino, mas no meu ponto de vista, ousadia para quebrar paradigmas e buscar o mesmo através de novos caminhos.

5) Com relação à atuação da segurança da informação fora do Brasil, quais são as principais diferenças na postura e nos desafios do CSO? Qual a sua expectativa com relação à sua profissão?

Se os negócios são fundamentalmente suportados por processos, pessoas e tecnologias em qualquer parte do mundo, podemos supor que todas as empresas estão praticamente suscetíveis as mesmas falhas, ameaças e impactos. Diante disso, o que efetivamente difere é o contexto. Seja por conta das particularidades da cultura local, da legislação, de tratados internacionais ou regulamentações setoriais, há sempre uma aderência natural do comportamento dos gestores, executivos e *C-Level* ao contexto. O mesmo ocorre com o CSO ou CISO – Chief Information Security Officer, como é comumente conhecido na Europa. Considerando este aspecto, as principais diferenças entre o CISO Brasileiro e o

CISO Britânico estão no planejamento de longo prazo, na preocupação com a conformidade, integridades e auditabilidade dos processos e na maturidade do sistema de gerenciamento de riscos, inerentes ao pensamento Europeu. Enquanto que o CISO Brasileiro precisa reagir com rapidez e eficiência no curto prazo e cuidar fundamentalmente da operação de hoje para poder ter a chance de pensar no amanhã. Este é sem dúvida um reflexo do imediatismo nativo de empresas brasileiras que querem primeiro sobreviver. De empresas que não enxergam ou não conseguem materializar o valor do investimento de longo prazo em segurança ou ainda, de empresas internacionais que precisam mostrar crescimento e resultado nos primeiros anos de operação para justificar sua permanência. Sob a ótima do profissional de segurança da informação, esse é um sinal positivo, pois mostra uma oportunidade de curto e médio prazo à medida que a maturidade de segurança do executivo brasileiro acompanhar a consciência internacional e à medida que novas regulamentações e leis forem criadas para proteger a economia e as relações comerciais. Minha expectativa é de que surjam oportunidades para uma nova geração de CISOs preparados e orientados a agir como um verdadeiro CHIEF e não como COLLABORATOR, reagindo ao hoje sem deixar de planejar o amanhã de forma consistente e alinhada aos interesses e estratégias do negócio.

6) Como a função de CSO é vista no exterior? Ela já está consolidada? Está submetida à área de TI?

Em geral o CSO ou CISO é um executivo com participação colaborativa no comitê *C-LEVEL* provendo orientação sob os riscos do negócio e ao mesmo tempo, recebendo diretrizes estratégias para manter o planejamento de segurança da informação alinhado aos interesses e à natureza da empresa. Assim como as áreas de auditoria, inspetoria e controle, o CISO oferece aconselhamento e se posiciona como tal em relação ao *board*. É uma posição consolidada, mas o escopo de suas atividades ainda varia de acordo com o porte e a maturidade da empresa no tratamento dos riscos da informação. Um indicador interessante é ver que em uma reunião de CISOs, muitos deles já ostentam cabelos brancos e experiência suficiente para transcender os aspectos técnicos da segurança. O reflexo dessa maturidade é ver, que em geral, estão ligados às áreas de auditoria e conformidade, suportado as decisões de negócio, e não ligados diretamente à área de TI.

7) O CSO já compõe uma classe profissional, ou a função ainda não está precisamente consolidada?

Decididamente a precisão não existe ainda, mesmo porque além de ser uma atividade nova, seu nível de responsabilidade, envolvimento com o negócio e importância vem mudando muito rapidamente, o que sugere a adoção de novos acrônimos para melhor descrever o novo perfil. Curiosamente, a primeira expressão que me lembro ter sido usada no Brasil, Security Officer, no exterior não representa um profissional de Infosec, mas profissionais de segurança física e patrimonial, o que indica que tudo ainda está em transformação. Por conta dessas variações que confundem empregados, empregadores e clientes, algumas entidades de classe têm se estabelecido internacionalmente para colaborar na elaboração de expressões e termos comuns além de prover base conceitual e suporte para os profissionais do setor. Podemos citar como exemplos o ISSA – Information System Security Association com capítulos por todo o mundo, e mais recentemente o IISP ou Institute of Information

Security Professionals de Londres, fundado em 2006 através de fusão de iniciativas dos setores privado e acadêmico, do qual faço parte como membro fundador.

8) Em sua opinião, qual o futuro da segurança da informação?

É arriscado demais tentar prever o futuro, pois o caminho que a segurança deve seguir será influenciado e praticamente determinado pelas futuras transformações nas relações comerciais, na legislação, no nível de maturidade de compradores, vendedores e usuários de serviços e produtos em geral, e principalmente, pela decisão do risco tido como tolerável para cada negócio. Porém, generalizando, posso arriscar o palpite de que cada vez mais as decisões de negócio estarão vinculadas aos aspectos de segurança associados, e estes por sua vez, estarão igualmente vinculados aos requisitos do negócio. A segurança da informação tenderá a ser mais uma caixa do organograma gerando *outputs* para orientar o negócio e recebendo dele *inputs* para o realinhamento do planejamento. *Business Plan* and Planos de InfoSec se suportarão mutuamente. O efeito desse novo estágio de maturidade poderá revelar surpresas, como a percepção de que em uma atividade específica, menos segurança pode representar mais para o negócio.

9) Existe algum desafio em trabalhar como CSO no exterior? E as vantagens?

Muitos são os desafios em trabalhar no exterior na área de segurança da informação e gestão de negócios, a começar pela língua, pela cultura, os hábitos locais e ainda pelo prejulgamento que fazem de seu país quanto ao potencial de oferecer profissionais de alto nível. Além de existir uma percepção de valor diferente oferecido pela segurança da informação, dado o grau de maturidade dos gestores, ainda existem as particularidades de comportamento que podem fazer uma iniciativa de *awareness* (conscientização de usuários), por exemplo, fracassar. Na verdade, estamos todos falando das mesmas coisas: *risk management, compliance, information security management system* etc, mas a forma de fazê-lo deve se adequar para garantir a efetividade. Vencidas estas barreiras, surgem as vantagens que não são poucas. A primeira delas é a chance de conhecer novas formas de pensar, além de se relacionar com culturas diferentes. De conhecer novos métodos para avaliar a qualidade e o valor dos produtos e serviços, pela oportunidade de herdar antigas e ricas experiências, e especialmente pela chance de mudar sua própria percepção sobre o mundo e o mercado de trabalho. Outras vantagens obvias estão associadas à maturidade do cargo que reflete diretamente no orçamento do cargo, nos investimentos em treinamento, além da oportunidade de aprimoramento de idiomas e o nítido aumento de visibilidade internacional, o que o torna um profissional suscetível a trabalhar praticamente em qualquer parte do mundo.

10) Há alguma pretensão em voltar a atuar no Brasil?

Sim. O retorno ao Brasil faz parte de meus planos originais por razoes pessoais, mas ainda depende de algumas mudanças no mercado brasileiro e o surgimento de oportunidades que maximizem esta experiência internacional, tanto no setor acadêmico quando no setor comercial privado. Acredito que ainda há muito a se fazer no mercado Brasileiro no campo da Segurança da Informação e Gerenciamento de Negócios de uma maneira geral, o que pessoalmente me atrai a retornar e pôr em pratica novos métodos e modelos de negocio.

Definitivamente os Europeus não tem a solução para tudo, nem tão pouco podem se colocar apenas na posição de mestres. O aprendizado e bidirecional e os Brasileiros do setor de tecnologia, particularmente os de seguranca da informação, se destacam pela extensão de seu conhecimento e pela postura flexível e criativa. Assim, um dos grandes valores desta passagem pela Europa está na chance de conhecer os erros e acertos de inúmeras iniciativas do passado a fim de evitar enganos futuros e aproveitar para aprimorar as iniciativas bem sucedidas no retorno ao Brasil.

11) Fale-me um pouco do trabalho que você desempenha na empresa?

Como *Head of Operations* da Atos Origin UK, meu desafio core é promover o aprimoramento do gerenciamento de projetos globais, fomentar o desenvolvimento de novos negócios e gerenciar a entrega de soluções de consultoria que transformem os riscos da informação em valor para os nossos clientes. Em linhas gerais, procuramos maximizar os resultados e suportar o desenvolvimento do negocio dos clientes através do gerenciamento de riscos, da viabilização de novas aplicações e da garantia de conformidade legal e regulatória. Além da responsabilidade sobre a estratégia da oferta de consultoria para o setor, acumulo a responsabilidade sobre os negócios de consultoria de InfoSec Offshore contando com recursos globais da companhia localizados especialmente na Itália, Índia e no Brasil.

About Atos Origin:
Atos Origin is an international information technology services company. Its business is turning client vision into results through the application of consulting, systems integration and managed operations. The company's annual revenues are EUR 5.5 billion and it employs over 47,000 people in 40 countries. Atos Origin is the Worldwide Information Technology Partner for the Olympic Games and has a client base of international blue-chip companies across all sectors. Atos Origin is quoted on the Paris Eurolist Market and trades as Atos Origin, Atos Euronext Market Solutions, Atos Worldline and Atos Consulting. For more information, please visit the company's web site at http://www.atosorigin.com.

Marcos Sêmola *é Head of Operations and Consulting Business Development da multinacional Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, profissional certificado CISM – Certified Information Security Manager pelo ISACA, BS7799 Lead Auditor pelo BSI, Membro da ISACA, ISSA, IBGC, CSI e membro fundador do IISP – Institute of Information Security Professionals of London. Professor da FGV – Fundação Getúlio Vargas, Pós Graduando em Negociação e Estratégia pela London School, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed. Campus, autor de outras duas obras ligadas à gestão da informação pelas editoras Saraiva e Pearsons e premiado pela ISSA como SecMaster®, Profissional de Segurança da Informação de 2003 Setor Privado e 2004 Desenvolvimento de Mercado, sendo membro da comissão julgadora em 2005. Visite www.semola.com.br ou contate marcos@semola.com.br*