54 – Janeiro de 2004

Governança corporativa responsável e as certificações profissionais de segurança

Estar diante de um desafio profissional e não se sentir preparado para vencê-lo é certamente uma situação de tirar o sono. Comumente a sensação de incapacidade pode se originar da carência de instrução formal, da baixa estima e falta de autoconfiança ou ainda da noção clara e transparente de que não reúne todas as competências necessárias e um volume suficiente de experiências acumuladas que o permita atirar a única flecha e acertar da primeira vez no centro do alvo.

Este tem sido o problema de muitos profissionais à frente da responsabilidade de gerir a informação das empresas e zelar por sua confidencialidade, integridade e disponibilidade. Garantir que os segredos de negócio estejam bem protegidos, que sejam alcançados e mantidos os altos índices de acessibilidade e conectividade e ainda, que a empresa esteja assistida pelas melhores práticas de mercado e cercada por controles de segurança que viabilizem a gestão de riscos e o suporte à governança corporativa responsável é o que atormenta a vida dos Gerentes de Segurança.
A pressão está cada vez maior e assim, a expectativa de resultados dos executivos e investidores. O assunto antes limitado aos fóruns técnicos escalou vertiginosamente a hierarquia e alcançou o alto escalão, tornando-o interessado e comprometido – espontaneamente ou não – com a gestão de riscos. Não somente os riscos de primeiro nível, atribuídos às falhas operacionais de ativos físicos, tecnológicos e humanos, mas principalmente os riscos relacionados aos demais níveis e que podem atingir processos de negócio, provocar danos à imagem da empresa em seu mercado e até mesmo gerar responsabilização legal.
Recentes casos internacionais relacionados a fraudes financeiras, manipulação de resultados e maquiagem de documentos, trouxeram à tona muitos dos aspectos de segurança antes invisíveis aos olhos dos executivos. Talvez por esses escândalos tenhamos visto a divulgação em massa da lei americana Sarbanes-Oxley que ampliou as atribuições do CEO (Chief Executive Office) e demais executivos no sentido de responsabilizá-los legalmente pela qualidade dos processos de divulgação de informações da companhia, pela preparação de relatórios, por investigações contábeis independentes, pela revisão de documentos e demonstrações financeiras preparados pelo CFO (Chief Financial Office), por limitações de atuação das auditorias independentes como prestar serviços de implementação de sistemas financeiros e muitos outros novos controles de risco que nunca estiveram em suas agendas.

Diante desse novo cenário de controles internos, compreender que o topo da pirâmide onde potencialmente ocorre a falência da empresa, o desgaste da imagem ou o prejuízo financeiro é apenas a camada onde o efeito final do processo de insegurança e descontrole corporativo é visível, é fundamental. Pense no seu corpo, mais especificamente na derme. Até que uma inflamação ou infecção se insinue sob a forma de um rubor, nódulo ou irritação visível, como uma espinha, outras camadas subcutâneas e elementos estruturais da

pele terão de ter sido previamente afetadas, gerando um efeito cascata cumulativo que culminará na percepção da irritação. Assim, preocupar-se com identificação dos problemas estruturais de segurança antes que alcancem a parte mais visível (o negócio), passou a ser também responsabilidade do alto executivo, que por sua vez conta com o apoio direto do CSO – Chief Security Office.
Esse desdobramento nos faz concluir que os já complexos e abrangentes desafios de gerir os riscos de segurança da informação se intensificaram. As expectativas de resultado foram maximizadas e agora são aguardadas ansiosamente pelo CEO e CIO a cada nova reunião do comitê executivo. As mudanças legais, estruturais e funcionais que incidem agora no topo da pirâmide, precisamente na faixa executiva, irão influenciar diretamente as faixas tática e operacional, demandando ações sinérgicas e integradas, voltadas à redução do risco.
Desta forma, o profissional de segurança que corporativamente planeja, desenha, implementa e administra as ações tem que estar preparado. Agora, mais do que nunca, é para valer e ele tem que estar seguro de que está apto e de que é possível atingir os resultados. De que é factível administrar o orçamento limitado priorizando e postergando ações. De que é necessário justificar os investimentos e medir, quase que em tempo real, o retorno proporcionado por cada um deles. De que está inteiramente alinhado à estratégia e aos interesses do negócio e que toda e qualquer iniciativa terá partido de uma necessidade fundamentalmente de negócio.

Parece que estamos falando de um super homem, dotado de visão aguçada de administrador de empresas, acompanhada de uma eficaz habilidade em gerenciar mudanças e se relacionar com pessoas, carregando ainda uma forte veia financeira que dá racionalidade às suas ações, mais um passado técnico que lhe permite compreender de forma integrada o papel da tecnologia na sustentação da operação do negócio e principalmente, com uma base conceitual de gestão de segurança da informação acumulada em treinamentos, preparações profissionais e amplas experiências práticas.

Pois justo este último fator, representa a maior dificuldade e carência atual dos profissionais candidatos ao cargo de CSO. A atividade de Security Officer, concebida e tratada oficialmente pela estrutura organizacional das empresas, é muito recente. Diferente dos cargos e atividades de administrador de empresas, técnico contábil, programador de computador, analista de sistemas ou ainda consultor de tecnologia da informação, a atribuição focada em gerir os riscos da informação dentro de uma organização acabou de ser inventada. Praticamente não existem cursos de graduação dedicados ao assunto, não existe o tratamento individual como profissão regulamentada, e poucos são os cursos de pós-graduação com a proposta verdadeira de formar profissionais de segurança da informação. No entanto, existem muitas certificações profissionais que compartilham conhecimentos valiosos para preparar o CSO e sua equipe. São normalmente associações internacionais de classe, consórcios, empresas de tecnologia ou centros públicos e privados de excelência que oferecem cursos seguidos de provas de avaliação de conhecimento, possuindo alvos bem definidos, ora puramente técnicos, ora táticos com uma visão operacional dos controles de segurança e felizmente, ora estratégicos.

As certificações técnicas mais cobiçadas e respeitadas do mercado são aquelas que abordam tecnologias específicas e comumente líderes de mercado como a tecnologia Cisco, Checkpoint, Microsoft, RSA, Oracle entre outras. Com o perfil mais tático, exigindo o

mínimo de 3 anos de experiência, misturando conceito e tecnologia, e se baseando em especialidades de um conjunto de domínios chamado CBK (*Common Body of Knowledge*), a certificação CISSP (*Certified Information Systems Security Professional*) é uma das mais respeitadas em todo o mundo. É emitida pelo ISC2 (*International Information Systems Security Certification Consortium*), que já certificou mais de 40 profissionais no Brasil. A associação internacional ISACA (*Information Systems Audit and Control Association*), famosa por sua certificação de auditoria de sistemas CISA (*Certified Information Systems Auditor*), lançou há pouco mais de um ano a certificação de segurança CISM (*Certified Information Security Manager*). Diferente de todas as demais que se concentram em aptidões baseadas em especialidade, a certificação CISM tem o foco no nível gerencial e exige o mínimo de 5 anos de experiência. É orientada aos negócios e destinada aos profissionais que atuam como gerentes responsáveis pela segurança das informações de uma organização e possuem o conhecimento e a experiência para especificar, implementar e dirigir a estrutura de gestão de riscos, além da habilidade de compreender o relacionamento entre as necessidades dos negócios e a segurança de TI. A habilitação CISM está projetada para oferecer aos executivos seniores a garantia de que aqueles que estejam habilitados tenham a perícia para oferecer gerenciamento e consultoria eficiente de segurança. O Brasil possui apenas 10 profissionais certificados contra 29 na América Latina e mais de 1300 em todo o mundo.

Principais certificações:

ABCP Associate Business Continuity Professional
BS7799 Leader Auditor
CBCP Certified Business Continuity Professional
CCIE Cisco Certified Internetwork Expert
CCNA Cisco Certified Network Associate
CCSA Checkpoint Certified Security Architecture
CCSA Certification in Control Self-Assessment
CCSE Checkpoint Certified Security Engineering
CFE Certified Fraud Examiner
CIA Certified Internal Auditor
CISA Certified Information Systems Auditor
CISM Certified Information Security Management
CISSP Certified Information Systems Security Professional
CPP Certified Protection Professional
CSP RSA Certified Security Professional
GCIA Certified Intrusion Analyst
GCFW Certified Firewall Analyst GIAC Global Information Assurance Certification
GSEC Global Information Security
MBCP Master Business Continuity Professional
MCSA Microsoft Certified System Architecture
MCSE Microsoft Certified System Engineering
MCDBA Microsoft Certified Data Base Administrator
OCP Oracle Certified Professional
SSCP Systems Security Certified Practitioner
entre outras.

O reconhecimento de valor dessas certificações nunca esteve simplesmente atrelado à sua existência, mas vem ocorrendo gradativamente e espontaneamente pelo mercado a partir da demonstração de competência dos profissionais certificados e também pela rigidez seletiva com que os certificadores conduzem o processo de avaliação e proteção de seu selo. Nos dias de hoje, praticamente todas são reconhecidas mundialmente e assim, conseguem nivelar o conhecimento e adotar uma linguagem única que possibilite ao profissional certificado ser classificado como apto para determinada atividade no Brasil, na França, na China ou em qualquer parte do mundo. Esses profissionais concentrados ao redor de uma certificação ou tema único potencializam ainda a troca global de experiências, métodos e ferramentas, fomentam uma base de conhecimento coletivo, que por sua vez, realimenta o próprio processo de aprendizado e valorização da certificação. Em tempo, é importante lembrar que a ausência do reconhecimento público de competência através do selo não desqualifica um profissional que, de alguma forma, conseguiu reunir conceito, técnica e prática. Para estes, o único obstáculo provavelmente será a maior dificuldade em conseguir uma oportunidade de mostrar suas competências, pois talvez os executivos - agora responsáveis diretos pela gestão dos riscos - não queiram se expor já no processo de seleção do profissional responsável por garantir seu sono.

Marcos Sêmola *é Security Practice Manager da multinacional Atos Origin, Consultor Sênior em Gestão de Segurança da Informação, CISM – Certified Information Security Manager, Professor de Segurança da Informação da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação e autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus 2003.*
marcos@semola.com.br