Segurança da Informação: Visão

Risco Inerente

Negócios são suportados por processos que mantêm uma relação de dependência de ativos físicos, tecnológicos e humanos, que possuem falhas de segurança. Estas por sua vez, são potencialmente exploradas por ameaças que, se são bem-sucedidas na investida, geram impactos de primeiro nível nos ativos, estendendo-os aos processos até que, finalmente, atingem os negócios. Possuir uma visão integrada dos riscos é fundamental para as empresas que buscam o desenvolvimento e a continuidade do negócio, e ainda dependem de uma infra-estrutura operacional sob risco controlado.

Fator Motivacional

Proteger as informações que subsidiam o funcionamento dos processos de negócio da empresa. Reduzir e administrar os riscos da informação e dos impactos potencialmente provocados por um incidente de vazamento, fraude, sabotagem e indisponibilidade. Esses parecem ser os motivos que levam o executivo e seu conselho consultivo a adotar medidas e realizar investimentos em segurança, mas é um equívoco pensar assim. Poderíamos nos enganar – como muitos o fazem - achando que o corpo executivo decide investir em segurança da informação para seguir uma tendência de mercado, para ser reconhecido como um visionário, para estar à frente da concorrência, para não ficar atrás da concorrência, para evitar prejuízos que já ocorreram com os outros, para evitar a repetição de prejuízos que já sofreu, para fortalecer sua imagem de credibilidade através do marketing, ou ainda, para respeitar regulamentações setoriais ou leis. Quando na verdade, pensam – de maneira objetiva – precisam preservar os atributos de confidencialidade, integridade e disponibilidade das informações com base em três únicos motivos ou fatores motivacionais: ganhar dinheiro, não perder dinheiro e não ser responsabilizado.

Gestão de Riscos

O comportamento das pessoas diante de medidas e contramedidas de segurança faz toda a diferença. A perenidade dos seres humanos é certa e, apesar da tendência apontar para um cenário de integração cada vez menor, eles sempre estarão por trás das decisões, das tecnologias, dos controles e das armas. Essas sim, tendem a mudar muito rapidamente. Desta forma, não seria nada inteligente montar uma estratégia de segurança exclusivamente baseada na variável da equação, na porção mais imprevisível, quando a peça chave e felizmente, aquela que já se conhece há tempos, continua sendo o homem.

The Global Risk Management Process (FERMA)

Decision
Árvore de Decisão de Risco

1. Rejeitar: esta opção deve ser considerada quando o risco não está sendo considerado pela estratégia do negócio, uma vez que o custo do controle, ou da contramedida, é superior ao risco ou ao bem a ser protegido.

2. Aceitar: esta opção deve ser considerada quando o risco é inerente à natureza e ao modelo de negócio, fazendo parte das operações normais e, portanto, tendo sido previsto na estratégia. A escolha dessa opção gera um outro nível de análise:

a. Evitar: esta decisão se baseia na vontade e viabilidade de se eliminar totalmente a fonte de um risco específico.

b. Transferir: esta decisão se baseia na relação custo-benefício e na viabilidade (disposição e capacidade financeira) de terceiros, para assumir o risco.

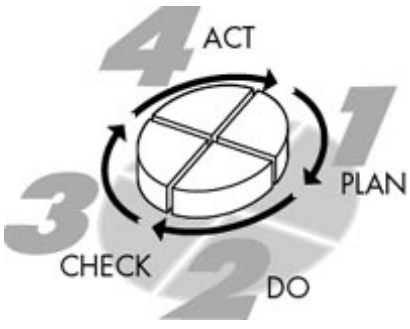
c. Explorar: esta decisão se baseia no interesse e na possibilidade de se obter vantagens competitivas pelo aumento da exposição e do grau de risco.

d. Reter: esta decisão se baseia no interesse do negócio, considerados custo e tolerância, de garantir a manutenção da exposição e do grau de risco.

e. Mitigar: esta decisão se baseia na necessidade do negócio, considerados custo e tolerância, de diversificar, controlar e reduzir os riscos.

O fator de Tolerância é determinante para que se definam investimentos compatíveis com o bem a ser protegido e principalmente, para que o nível de risco residual esteja dentro da zona de conforto e compativel com a natureza de cada negocio.

O que não se conhece não se pode controlar.
O que não se controla não se pode mensurar.
O que não se mensura não se pode gerenciar.
O que não se gerencia não se pode aprimorar.



Conceitualmente, atingiremos a maturidade adequada da gestão de riscos quando ela não for perceptível. Quando os processos estiverem bem definidos e documentados, orientando os agentes humanos e prontos para suportar mudanças corriqueiras nos ativos físicos, tecnológicos e humanos, sem que isso represente uma bruta e não planejada oscilação no nível de risco.

Mas se os processos estão emperrados, os usuários insatisfeitos por terem de trocar muitas senhas e o CEO se questionando porque apesar de todos os investimentos em segurança ele ainda continua a receber mais spams do que e-mails confiáveis, certamente algo está muito, muito errado.

Principais Certificações Profissionais

CISM Certified Information Security Management (www.isaca.org)
CISSP Certified Information Systems Security Professional (www.isc2.org)
CISA Certified Information Systems Auditor (www.isaca.org)
BS7799 Lead Auditor (www.bsi-global.com)
SSCP Systems Security Certified Practitioner (www.isc2.org)
GIAC Global Information Assurance Certification (www.sans.org)
CSP RSA Certified Security Professional (www.rsa.com)
CBCP Certified Business Continuity Professional (www.drii.org)
ABCP Associate Business Continuity Professional (www.drii.org)
MBCP Master Business Continuity Professional (www.drii.org)
CCSA Certification in Control Self-Assessment (www.theiia.org)
CIA Certified Internal Auditor (www.theiia.org)
CFE Certified Fraud Examiner (www.cfenet.com)
CPP Certified Protection Professional (www.asisonline.org)

CISM - Certified Information Security Manager

Certified Information Security Manager, é a nova certificação da ISACA especialmente desenhada para profissionais experientes em segurança da informação. A CISM é orientada para o negócio e focada em gestão de risco da informação, quando trata *conceitualmente* questões de segurança, sejam elas gerenciais, de desenho ou técnicas. Ela destina-se a indivíduos que precisam manter uma visão "global" ao gerenciar, desenhar, supervisionar e avaliar a segurança da informação da empresa.

Primeira Habilitação em Segurança de Informações
(Fonte: site do ISACA www.isaca.org.br)

ROLLING MEADOWS, Illinois, 20 de agosto — Enquanto as empresas se deparam com complicadas ameaças com segurança em TI, os executivos devem ter a certeza de que seus gerentes em segurança de TI tenham a perícia necessária para reduzir os riscos e proteger a organização. Para satisfazer esta necessidade, a Associação de Auditoria e Controle de Sistemas de Informação (Information Systems Audit and Control Association - ISACA) introduziu a nova designação de Gerente Habilitado em Segurança de Informações (Certified Information Security Manager™-CISM™.

O foco da designação CISM em nível gerencial diferencia-se de outras habilitações em segurança de TI que se concentram em aptidões baseadas em especialista.
A habilitação CISM está projetada para oferecer aos executivos seniores a segurança de que aqueles que estejam habilitados, tenham a perícia para oferecer um gerenciamento e consultoria eficiente de segurança. Trata-se de uma designação orientada em negócios para profissionais que gerenciam a segurança das informações de uma organização e possuem o conhecimento e a experiência para instalar, implementar e dirigir a estrutura de segurança para gerenciar risco com eficácia.

A integridade e a confiabilidade da informação e dos sistemas TI são cruciais para o sucesso de uma empresa, portanto os executivos precisam estar seguros de que os profissionais encarregados da segurança da empresa sejam habilitados e capazes, disse Marios Damianides, CISA, CPA, CA, presidente do conselho do Grupo de Trabalho Organizado para A Habilitação da ISACA (Credentialing Task Force) e sócio na Ernst & Young em Nova York, Nova York, EUA. A habilitação CISM é para gerentes responsáveis pelo entendimento do relacionamento entre as necessidades dos negócios e a segurança de TI.

Para obterem a designação CISM, os profissionais devem concluir com sucesso o exame CISM (a ser oferecido em 2003), aderirem a um código de ética e submeterem evidência verificável de cinco anos de experiência relacionada com trabalho de segurança de informações.

A ISACA é a organização ideal para administrar esta habilitação pioneira em segurança de informações em nível gerencial, disse Robert Roussey, CPA, Presidente da ISACA International e Professor de Contabilidade na University of Southern Califórnia em Los Angeles, Califórnia, EUA. Desde 1978, a ISACA tem oferecido a habilitação CISA(®) Auditor Habilitado em Sistemas de Informação (Certified Information Systems Auditor™), a qual tem se desenvolvido e se tornado o padrão aceito globalmente de perícia em auditoria de TI.

Contate a ISACA através do telefone +1-847-253-1545, ramal 471, ou por email: certification@isaca.org.

Com 26.000 membros em 160 divisões em 100 países, a Information Systems Audit and Control Association® (ISACA™) (www.isaca.org) é líder reconhecida globalmente na direção, controle e segurança de TI. Fundada em 1969, a ISACA patrocina conferências internacionais, publica o Jornal Information Systems Control, desenvolve padrões de auditoria e de controle de sistemas de informações aplicáveis globalmente, e administra a habilitação respeitada globalmente CISA® (Certified Information Systems Auditor™) e a nova habilitação Certified Information Security Manager™ - CISM™.

CISA - Certified Information Systems Auditor

Certified Information Systems Auditor, é a certificação principal da ISACA. Desde 1978, o exame CISA mensura a excelência nas areas de auditoria, controle e segurança de TI. A CISA cresceu ao ponto de ser reconhecida globalmente e adotada por todo o mundo como símbolo de sucesso. Existem mais de 29,000 CISAs ao redor do mundo, e mais de 10,000 profissionais passaram pelo exame CISA, somente em 2002.

Nota: Para obter informações detalhadas das certificações do ISACA, envie um e-mail com a sua solicitação para: educar@isaca.org.br. Acompanhe ainda a iniciativa de abertura do capítulo Rio de Janeiro do ISACA que junto com o capítulo São Paulo fomentará o apoio aos profissionais brasileiros de auditoria e segurança da informação.

Bibliografia Especializada

• NBR/ISO/IEC 17799. Tecnologia da Informação: Código de prática para a gestão da segurança da informação. ABNT, 2002. 56p

• SEMOLA, Marcos: Gestão de Segurança da Informação – uma visão executiva. Editora Campus 2003. 184p.

• PELTIER, Thomas R.: Information Security Policies and Procedures – a practitioner's reference. Auerbach Publications. 373p.

• DOU. Decreto nº3.505, que institui Política de Segurança na Administração Federal.13 Jun 2000.

• DOU. Decreto 3.587. Estabelece a composição de ICP do governo. 5 de setembro de 2000.

• PARKER, Donn. Fighting Computer Crime: a new framework for protecting information. New York: Willey. 1998. 512p.

• GIL, Antonio de Loureiro. Segurança em Informática. 2 ed.. São Paulo: Atlas, 1998. 193p.

• HUTT, Arthur E. et al. Computer Security Handbook. 3rd Edition. New York: John Wiley & Sons, Inc. 1995.

• RUSSEL, Deborah e GANGEMI, G.T. Computer Security Basics. California, O'Reilly & Associates, Inc. 1991. 441p.

• KRAUSE TIPON, Handbook of Information Security Management 1999, Editora Auerback

• VALLABHANENI, S.Rao. CISSP Examination Texbooks. Vol1: Theory. SRV Professional Publications, Illinois. 2000. 519p.

• ISO/IEC JTC 1/SC 27. Glossary of IT Security Terminology. Information technology - security techniques. 1998.

• SCHNEIER, Bruce. Segurança.com – Segredos e mentiras sobre a proteção na vida digital. Editora Campus.

• DIAS, Claudia, Segurança e Auditoria da Tecnologia da Informação, Axcel Books, 2000.

• BRASILIANO, Antônio Celso Ribeiro, A (In)segurança nas Redes Empresariais, Editora Sicurezza 2002.

• MACHADO, André e FREIRE, Alexandre, Como Blindar seu PC, Editora Campus 2006

Links

Colaborações Profissionais

Augusto Quadros Paes de Barros, CISSP www.paesdebarros.com.br
André Fucs, CISSP www.cfsec.com.br e http://www.fucs.org/portugues/
André Machado Blog O Globo Online - http://oglobo.globo.com/blogs/andremachado/
Edson Fontes, CISA, CISM www.edison.fontes.blog.uol.com.br/
Giordani Rodrigues www.infoguerra.com.br
Gilberto Martins de Almeida gmalmeida@all.com.br
Luis Rabello, CISSP, BS7799LA – Coluna PEOPLEWARE www.idgnow.com.br
Marcos Machado www.istf.com.br
Márcio D'Avila www.mhavila.com.br
Marcus Rarum www.ranum.com
Marcos Henrique www.marcoshenrique.com.br
Marcos Sêmola, CISM, BS7799LA – Coluna FIREWALL www.idgnow.com.br
Nelson Correia, CISSP http://globalesecurebr.blogspot.com/
Nicolas Laufer http://www.cripto.info/
Patrícia Peck www.patriciapeck.com.br
Renato Opice Blum www.opiceblum.com.br
Renata Cicilini Teixeira www.cicilini.com.br
Segio Dias, MVP, CISSP - http://sdias.spaces.live.com/
Schneier www.schneier.com
Crypto-Gram BR por Eduardo Never e Francisco Milagres http://download.cissp.com.br/cryptogrambr

Centros de Pesquisa

FERMA - Federation on European Risk Management Associations www.ferma-asso.org/
AIRMIC - The Association of Insurance and Risk Managers www.airmic.com
ALARM - The National Forum for Risk Management in the PSector www.alarm-uk.com
IRM - The Institute od Risk Management www.theirm.org
UNICAMP - Equipe de Segurança em Sistemas de Rede www.security.unicamp.br
NIC BR www.nic.br
CERT - Computer Emergency Response Team www.cert.org
CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes Brasil www.cert.br
ISA - Internet Security Alliance www.isalliance.org
FIRST - Forum of Incident Response and Security Teams www.first.org
RNP CAIS - Centro de Atendimento a Incidentes de Segurança www.rnp.br/cais
ISO/IEC 17799:2000 Information Security Management – www.iso.org
SANS Institute - System Administration, Networking, and Security www.sans.org
US-CERT - United States Computer Emergency Readiness Team www.us-cert.gov
CSRC - Computer Security Resource Center, NIST – http://crsc.ncsl.nist.gov
CSI - Computer Security Institute www.gocsi.com
MICROSOFT Centro de Segurança - http://www.microsoft.com/brasil/security/default.mspx

Institutos de Pesquisa e Desenvolvimento Profissional

ISACA – Information System Security & Control Association www.isaca.org
ISC2 - International Information Systems Security Certification Consortium www.isc2.org
ISSA - Information System Security Professionals www.issa.org http://www.issabrasil.org
BSI – British Stantard Institution www.bsi-global.com
DRI - Disaster Recovery Institute www.drii.org
SANS Institute www.sans.org
CompTIA www.comptia.org
BCI - Business Continuity Institute www.thebci.ogr
CISSPs www.cissps.com
RSA www.rsa.com
ASIS www.asisonline.org
CFENET www.cfenet.com - Intitute of Information Security Professionals (UK)
IISP Institute of Information Security Professionals (UK) www.instisp.com
Information Security Management Maturity Model (ISM3) http://www.ism3.com
ABRAIC http://www.abraic.org.br
Brazilian Information Security http://www.brassec.com.br/

Comunidades e Guias

ISMS International User Group www.xisec.com/
Comunidade ISMS PT http://ismspt.blogspot.com/
IFTF Info Security Task Force http://www.istf.com.br/vb/index.php
Blog CISSP http://www.cissp-certification.info/
Guia Sobre Sites http://www.sobresites.com/segurancadainformacao/index.htm
Microsoft Security http://www.microsoft.com/brasil/athome/security/default.mspx
Cartilha de Segurança na Internet http://cartilha.cert.brNavegue Seguro - http://www.navegueprotegido.org
Internet Segura - http://www.internetsegura.org
Guide to CISSP Blog por Leandro Bennaton http://www.guidetocissp.com/

Stantards

BSI BS25999-1: DRAFT DPC http://www.bsi-global.com/Risk/BusinessContinuity/bs25999.xalter
BSI BS7799-2:2002, http://www.bsi-global.com/
BSI BS ISO/IEC 27001:2005, http://www.bsi-global.com/
BSISEI CMMI, http://www.sei.cmu.edu/cmmi/
ISACA COBIT, http://www.isaca.org/
EA 7/03, http://www.european-accreditation.org
ISO 13335, http://www.iso.org/
ISO 19011:2002, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=31169
ITSM, ITIL, http://www.itil-itsm-world.com/
ISSA GAISP, http://www.issa.org/gaisp/_pdfs/v30.pdf
IETF RFC2119, http://rfc.net/rfc2119.html
NIST SP800-53, http://csrc.nist.gov/publications/nistpubs/
NIST SP800-55, http://csrc.nist.gov/publications/nistpubs/
ISO 9001:2000, http://www.iso.org
ISO/IEC 17799:2000, http://www.bsi-global.com/
ISO 18044, ISO 15228, http://www.iso.org/
ISO 15408, http://www.iso.org/
ISO 12207, http://www.iso.org/

E-Books

Content Central http://cc.realtimepublishers.com

Geral

ICP-Brasil: Infra Estrutura de Chaves Públicas Brasileira www.icpbrasil.gov.br
Medida Provisória nº 2.200-2, de 24 de agosto de 2001 www.planalto.gov.br
CG - Comitê Gestor www.cg.org.br
SecurityFocus Online http://online.securityfocus.com
IDG Now! Segurança www.idgnow.com.br
InfoGuerra www.infoguerra.com.br
Módulo Security Solutions www.modulo.com.br
SecForum www.secforum.com.br
Security Review www.modulo.com.br
TotalSecurity www.totalsecurity.com.br
CSO Online www.csoonline.com
InfoSecurity Magazine www.informationsecurity.techtarget.com
ISTF Info Security Task Force www.istf.com.br
Xforce ISS www.xforce.iss.net
Symantec www.symantec.com
SECINF. Glossary of Terms Network Security http://secinf.net/info/misc/glossary.html
WEBOPEDIA. Security http://webopedia.internet.com/Networks/Security
Banco Bradesco - Politica http://www.bradesco.com.br/seguranca_informacao/
Computer Museum - http://www.computerhistory.org/

Nota: participe da atualização desta página enviando sugestões e informações.

A união entre profissionais de auditoria e segurança, bem como de estudiosos e interessados no tema é fundamental para o aprimoramento das práticas de auditoria e gestão de riscos e para a manutenção do processo de desenvolvimento contínuo. Ajude a manter o ciclo em movimento constante.