ISSN 0080-2107

Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras

Igor Siqueira Cortez
Confederação Nacional da Indústria – Brasília/DF, Brasil

Luis Claudio Kubota
Instituto de Pesquisa Econômica Aplicada – Brasília/DF, Brasil

Recebido em 29/setembro/2011
Aprovado em 10/abril/2012

Sistema de Avaliação: *Double Blind Review*
Editor Científico: Nicolau Reinhard

DOI: 10.5700/rausp1119

Os autores informam que este estudo foi realizado no âmbito de cooperação entre o Instituto de Pesquisa Econômica Aplicada e o Comitê Gestor de Informática.

RESUMO

Recentemente, uma série de ataques cibernéticos a empresas e governos no Brasil e no exterior tornou público o potencial impacto econômico desse tipo de atividade, do ponto de vista tanto privado quanto público. Existe extensa literatura econômica — teórica e empírica — que avalia os incentivos para que as empresas adotem ou não medidas de segurança da informação. No presente estudo foi desenvolvida uma avaliação empírica desse fenômeno no Brasil. Modelos *logit* e *probit* ordenado foram desenvolvidos como forma de avaliar os efeitos sobre a probabilidade de ocorrência de problemas de segurança da informação, levando-se em conta as características das firmas, inclusive as medidas de segurança de informação. Os resultados apontam para uma relação positiva entre as medidas de segurança da informação e a probabilidade de identificar a ocorrência de problemas cibernéticos, sugerindo que a sofisticação dessas medidas de proteção aumenta a probabilidade de identificação dos problemas.

Palavras-chave: *internet*, segurança da informação, ataques cibernéticos, econometria.

INTRODUÇÃO

Recentemente, uma série de ataques cibernéticos a organizações como Fundo Monetário Internacional (FMI), Lockheed Martin (principal fornecedor de armamento das Forças Armadas dos Estados Unidos da América), Google, Sony, Playstation, Hyundai, Credicard, entre outras, levantou a discussão sobre a relevância de investimentos na área de segurança da informação como forma de

Igor Siqueira Cortez, Graduado em Ciências Econômicas pela Universidade de Brasília, Mestre em Economia pela Universidade de São Paulo, é Economista da Confederação Nacional da Indústria (CEP 70040-903 – Brasília/DF, Brasil).
E-mail: igor.cortez@cni.org.br; igorcortez@gmail.com
Endereço:
Confederação Nacional da Indústria
SBN, Bloco C, Edifício Roberto Simonsen
70040-903 – Brasilia – DF

Luis Claudio Kubota, Graduado em Economia, Mestre e Doutor em Administração pela Universidade Federal do Rio de Janeiro, é Técnico de Planejamento e Pesquisa do Instituto de Pesquisa Econômica Aplicada (CEP 70076-900 – Brasília/DF, Brasil).
E-mail: luis.kubota@ipea.gov.br

proteger informações sigilosas, evitar prejuízos às corporações e prover a manutenção do bem-estar da sociedade.

No Brasil, esse fato também vem ganhando importância após uma série de intrusões e ataques cibernéticos a bancos e a sistemas de órgãos do Governo Federal. Esses ataques revelaram ao grande público a existência de ameaças que têm o potencial de comprometer o pleno funcionamento de infraestruturas críticas.

Apesar de ser um assunto que tem chamado a atenção apenas recentemente, há grande quantidade de estudos que utilizam a teoria econômica para abordar o problema de segurança da informação. Por algum tempo, os problemas associados a esse campo foram tratados como problemas técnicos que seriam resolvidos apenas por engenheiros e cientistas computacionais utilizando a linguagem computacional. No entanto, a teoria econômica revelou que muitos dos problemas abordados nesse campo também estão ligados a incentivos econômicos.

Neste trabalho, teve-se como objetivo analisar a relação empírica entre as medidas associadas aos investimentos em segurança da informação e a ocorrência de problemas de segurança da informação[1] para uma amostra representativa de firmas com mais de dez funcionários no Brasil.

Modelos *logit* e *probit* ordenado foram desenvolvidos como forma de analisar a relação entre segurança da informação e problemas de segurança da informação levando-se em conta os efeitos de características das firmas. No presente estudo utilizaram-se micro dados da Pesquisa sobre o uso das tecnologias da informação e comunicação no Brasil: TIC Domicílios e TIC Empresas 2009, do Comitê Gestor de Informática (CGI), procurando responder a duas questões:

- Quais os determinantes da probabilidade das firmas identificarem ou não problemas de segurança da informação?
- Quais os determinantes da probabilidade das firmas identificarem um ou mais problemas de segurança da informação?

A TIC Empresas 2009 é uma pesquisa conduzida anualmente e que segue padrões metodológicos da Organização para Cooperação Econômica e Desenvolvimento (OECD) e do Departamento Estatístico da União Europeia (Eurostat).

Intuitivamente, espera-se que haja uma relação negativa entre segurança da informação e problemas de segurança. Contudo, os resultados apontam para uma relação positiva entre as duas variáveis, o que sugere a interpretação de que medidas de segurança aumentam a probabilidade de identificação dos problemas.

O artigo está estruturado da seguinte forma: além desta introdução, na seção 2 apresenta-se uma revisão de literatura de estudos teóricos e empíricos relacionando economia e segurança da informação; na seção 3 apresenta-se a fundamentação teórica dos modelos; na seção 4 mostram-se estatísticas descritivas da Pesquisa TIC Empresas 2009, inclusive com uma descrição do plano amostral; na seção 5 abordam-se os modelos empíricos e os resultados; e na seção 6 são apresentadas as conclusões e considerações para trabalhos futuros.

2. LITERATURA

2.1. Teoria econômica e segurança da informação

Anderson (2001) foi autor de um dos primeiros trabalhos a mostrar como a teoria econômica interage com o tema da segurança da informação. No trabalho, o autor defende que as externalidades de rede, as barreiras à entrada, o fato de as grandes empresas adotarem suas estratégias baseadas no valor, em vez de no custo, e as enormes vantagens de primeiro movimento em sistemas econômicos com fortes *feedbacks* são algumas das razões pelas quais os *software* de mercado, como o *Windows*, possuem tantas falhas.

De acordo com Varian (2004), muitos dos problemas de segurança da informação são por causa de falhas de incentivos econômicos. O autor argumenta que a responsabilidade é difusa. Um exemplo são os ataques *Distributed Denial of Service* (DDOS), em que *hackers* invadiram algumas redes desprotegidas de universidades norte-americanas e utilizaram as estruturas para distribuir um ataque contra alguns sítios eletrônicos, como o Yahoo, em 2000. Nesse exemplo, as universidades que foram invadidas não sofreram sanção alguma com relação aos prejuízos econômicos causados ao Yahoo e a outros *sites*. Varian (2004) argumenta que se houvesse uma responsabilização (*liability*), talvez as universidades tivessem incentivos mais fortes para proteger a sua rede. A proposta do autor é que os custos de ataques DDOS devem cair sobre os operadores de rede, os quais podem fazer uma melhor avaliação sobre que parte está mais bem posicionada para gerir os riscos.

Em um trabalho anterior, que também trata da questão das responsabilidades, Anderson (1994) mostra como os padrões de fraude em contas bancárias são associados a esse fenômeno. Nesse estudo, o autor compara os eventos de fraude ocorridos nos Estados Unidos da América (EUA), na Grã-Bretanha, na Noruega e na Holanda, e chega à conclusão de que nos países europeus o ônus da prova estava sobre os clientes e nos EUA, sobre os bancos. Como nos países europeus os bancos não têm muitos incentivos para melhorar seus sistemas de segurança, observou-se uma epidemia de fraudes. Nos EUA, os incentivos estavam no lado oposto e os bancos sofreram número substancialmente menor de fraudes. O autor argumenta que, embora nos EUA houvesse um gasto menor em segurança da informação, os investimentos eram realizados de forma eficiente.

Adotando uma abordagem diferente, de teoria dos jogos, Garcia e Horowitz (2006) analisam as motivações econômicas para o investimento em segurança e levantam a possibilidade de uma falha de mercado, possível sob a forma de subinvestimento em segurança. Os resultados dependem do fato de o valor social derivado do uso da internet exceder os rendimentos em jogo associados aos investimentos dos Provedores de Serviço de Internet (PSI). Segundo os autores, se a relação entre o valor social e as receitas em jogo para os provedores de internet continua a crescer, a probabilidade de subinvestimento em

segurança torna-se maior e alguma forma de regulamentação pode ser necessária.

Cremonini e Nizovtsev (2006), por sua vez, analisam o comportamento de atacantes sob diferentes cenários de informação. Num primeiro cenário, os atacantes obtêm informações completas sobre as características de segurança de alvos. Num segundo cenário, a análise é feita sob a hipótese de informação assimétrica. Os resultados do modelo mostram que quando os atacantes são capazes de identificar o nível de segurança de seus alvos e alternar entre múltiplos alvos diferentes, o efeito de uma medida de segurança determinada é mais forte. Qualquer aumento no nível de segurança tem dois efeitos sobre a frequência de incidentes. O efeito direto é atribuído às características técnicas de um sistema e diminui a probabilidade de sucesso de um determinado ataque devido ao esforço. Já o efeito indireto, ou de comportamento, diminui a quantidade de esforço que um atacante coloca em tentativas de intrusão, assim diminuindo ainda mais a frequência dos ataques e a perda esperada. Isso sugere que se esse efeito fosse ignorado, o resultado seria a má alocação de recursos de segurança. Os autores mostram, também, que sistemas com melhores níveis de segurança têm incentivos mais fortes para revelar suas características de segurança para os atacantes do que sistemas com baixa proteção.

2.2. Evidência empírica

A literatura acadêmica sobre segurança da informação já evoluiu ao ponto de haver quantidade razoável de modelos analíticos. Recentemente, pesquisadores vêm direcionando esforços para confirmar as premissas e as intuições dos modelos de forma empírica. Contudo, devido à dificuldade de coletarem-se dados relevantes para o tema de pesquisa, essa literatura ainda se encontra em um estágio primário de amadurecimento.

Entre as dificuldades de coletarem-se dados, destaca-se a veracidade de informações fornecidas por instituições e firmas acerca de ataques e intrusões no sistema. Uma evidência empírica a respeito desse fato é fornecida pelo trabalho de Cavusoglu, Mishra, e Raghunathan (2004). Os autores identificaram que dentre 66 tipos de ataques cibernéticos, durante o período de 1996 a 2001, 31 deles afetaram firmas que conduzem seus negócios pela internet. O resultado do estudo aponta que o valor na Bolsa de Valores das firmas afetadas sofre desvalorização média de 2% relativamente às firmas não afetadas por ataques cibernéticos. O estudo mostra que os tipos de ataques não são estatisticamente significantes para diferenciar o montante das perdas. Campbell, Gordon, Loeb, e Zhout (2003) também haviam chegado a resultados semelhantes, mas apontam que o tipo de ataque pode ser relevante no montante da desvalorização sofrida pela firma. Ataques que envolvem a perda de informação confidencial têm um impacto mais acentuado do que os demais tipos de ataques. Nesse sentido, a revelação de informações acerca de ataques cibernéticos pode ser custosa para as firmas e, portanto, informações a respeito desses eventos nem sempre estão disponíveis.

Contudo, ainda há alguns trabalhos elaborados nesse âmbito. Moore e Clayton (2007) coletaram dados a respeito de remoção de *sites* de instituições financeiras clonados com o objetivo de obter as credenciais dos usuários. Uma medida comum é a remoção do *site* falso a tempo. Os autores monitoraram milhares de *sites* de bancos e observaram heterogeneidades em vários níveis. Dentre elas, a de que algumas instituições são mais visadas do que outras. Outro ponto é que o tempo médio de remoção dos *sites* clonados é de cerca de 20 horas e que a velocidade de remoção é altamente variável. O tempo de remoção segue uma distribuição lognormal em que a maioria dos *sites* é removida em poucas horas, ao passo que uma minoria substancial sobrevive por várias semanas. As variações observadas não aparentam ser aleatórias e sugerem que os criminosos identificam sistematicamente as vulnerabilidades mais rápido do que os gestores dos sistemas.

Alguns estudos empíricos examinam como os *hackers* selecionam seus alvos. Moore e Clayton (2011) mostram que ferramentas de busca são utilizadas para identificar potenciais vulnerabilidades. Geralmente são buscados termos específicos de programas ou versões de programas que um *hacker* consegue subverter. Um exemplo mostrado pelos autores é o termo **phpizabi v0.848b c1 hfp1**, que retorna de *sites* que utilizam *software* sofrendo de uma vulnerabilidade de carregamento irrestrito (*unrestricted file upload vulnerability*). Por meio dos *logs* de *sites* comprometidos por *phishing*, eles chegaram ao resultado de que cerca de 18% dos *sites* comprometidos são cuidadosamente selecionados pelo uso de termos específicos que remetem a vulnerabilidades do sistema.

Moore e Clayton (2011) também revelam que 19% dos *sites* já comprometidos são selecionados novamente após um intervalo de seis meses, e essa taxa praticamente dobra se o *site* já tiver sido identificado por meio de termos específicos.

No que concerne às evidências de estudos elaborados por meio de *survey*, Liu, Tanaka, e Kanta (2008), utilizando dados de uma pesquisa governamental de 2002 e 2003 sobre firmas japonesas, mostram que o investimento em segurança da informação tem efeitos estatisticamente significantes na redução da probabilidade de ocorrência de problemas de segurança relacionados a vírus de computador.

Por meio de uma regressão logística que leva em conta características como tipo do mercado de atuação da firma, número de funcionários com *e-mail* corporativo como *proxy* de vulnerabilidade e variáveis que captam medidas de investimento em segurança da informação, Liu *et al.* (2008) mostram que existe uma relação inversa entre investimento em segurança e a probabilidade de sinistros causados por vírus de computador. As medidas de investimento consideradas são se a firma possui algum tipo de política de segurança da informação, se há treinamento ou palestras informativas aos funcionários e se a firma adota mecanismos de defesa como antivírus, *firewall* e outros sistemas tecnológicos. Os primeiros resultados mos-

tram que as variáveis relacionadas a investimento em segurança não são significativas. Entretanto, quando os autores utilizam uma interação entre as três medidas de investimento os resultados mostram um impacto negativo e significante sobre a probabilidade de a firma ter problemas de vírus. Os autores também verificam que esse resultado é prevalente para firmas que adotaram as três medidas de investimento nos dois anos analisados. As firmas que adotaram as três medidas conjuntamente apenas no último ano ou somente no primeiro ano apresentaram maior propensão a ter problemas de segurança.

Tanaka, Kmatsuura e Sudoh (2005) analisaram a relação entre investimentos de segurança da informação e vulnerabilidades cibernéticas por meio de dados a respeito dos governos eletrônicos de municípios japoneses. Os autores partem dos resultados do modelo de Gordon e Loeb (2002), os quais mostraram que apenas firmas com vulnerabilidade média estariam dispostas a investir um montante substancial para deter problemas de segurança da informação. Para classificar as vulnerabilidades dos municípios, Tanaka *et al.* (2005) partem do pressuposto de que quanto mais compartilhada uma rede, mais vulnerável essa rede é a ataques e problemas de segurança de informação. Tanaka *et al.* (2005) dividem os municípios com base em três tipos de compartilhamento de redes: municípios com redes simples ou sem conexão com outros municípios ou governo federal, municípios com redes regionais ou que apresentam conexões com outros municípios dentro de uma mesma região e, por fim, municípios com conexões com o governo federal e outras regiões. Por meio de uma regressão simples, Tanaka *et al.* (2005) apresentam resultados que vão ao encontro dos pressupostos teóricos do modelo de Gordon e Loeb (2002). Os autores verificam que apenas os coeficientes ligados a *dummies* de municípios com vulnerabilidade média apresentam sinal positivo e significante numa regressão que tenta explicar o montante investido em tecnologias de segurança da informação.

Takemura, Osajima, e Kawano (2008) analisaram o efeito de medidas de segurança em informação e educação adotadas por firmas provedoras de internet no Japão. Eles utilizam dados de uma pesquisa realizada em 2007 e que inclui respostas de 63 empresas PSI. Os resultados da regressão logística estimada pelos autores mostram que há uma relação positiva entre o risco de sofrer um problema de segurança e o número de contramedidas adotadas com relação à segurança da informação. No entanto, os autores evidenciam que medidas de educação sobre segurança da informação possuem um sinal negativo e estatisticamente significante, o que, segundo eles, mostra que o investimento em educação apresentaria uma relação custo benefício maior do que o investimento em tecnologias de defesa e que, portanto, deveriam ser incentivadas para reduzir o risco de problemas de segurança da informação.

A análise que se propõe neste artigo é semelhante à análise elaborada por Takemura *et al.* (2008), mas o foco de observações é mais amplo e, no que se refere às interpretações, será mostrado adiante que a relação positiva entre as contramedidas de segurança de informação e a ocorrência de problemas de segurança da informação não deve ser interpretada como um risco.

Como forma de motivar a estratégia empírica utilizada neste trabalho, na próxima seção introduz-se um modelo simples sobre a relação do investimento em segurança, da vulnerabilidade cibernética e dos riscos de sinistros ligados à tecnologia da informação e comunicação.

3. FUNDAMENTAÇÃO TEÓRICA

No presente trabalho, utiliza-se um modelo simples de otimização do lucro esperado como forma de entender as decisões sobre investimento em segurança da informação. Dar-se-á enfoque a duas possíveis interpretações para o problema de otimização da firma. Basicamente, na primeira abordagem o problema é visto como a maximização de lucro esperado, e a ocorrência de problemas de segurança é associada a possíveis perdas de ativos informacionais.

Entretanto, o evento aleatório considerado pode ser interpretado também como a probabilidade da firma identificar o problema de segurança e com isso minimizar possíveis perdas de ativos, o que representa a segunda interpretação possível.

Adiante, ver-se-á que o modo como esse problema é interpretado tem fundamental importância na interpretação dos resultados obtidos na seção de análise empírica.

Assume-se que γ_i denota o número de problemas de informação que ocorrem na firma *i*. Como só é observado se a firma sofreu ou não algum tipo de problema, γ_i é representado por uma variável latente que depende do grau de vulnerabilidade da firma, v_i, e do quanto a firma investe em segurança da informação, z_i, de tal forma que:

$$\gamma_i^* = \propto v_i + \beta z_i + \varepsilon_i \qquad [1]$$

Em que ε_i representa um termo idiossincrático de perturbação estocástica com função de distribuição de probabilidade simétrica tal que $0<F(.)<1$. Mais precisamente, ε_i representa as características não observáveis da firma e que são independentes do seu grau de vulnerabilidade e investimento. Portanto, a probabilidade de ocorrer um problema de segurança é denotada por:

$$Pr(\gamma_i^*>0) = Pr(\propto v_i + \beta z_i + \varepsilon_i > 0) \qquad [2]$$

$$Pr(\gamma_i^*>0) = Pr(-\varepsilon_i < \propto v_i + \beta z_i) \qquad [3]$$

$$Pr(\gamma_i^*>0) = F(\propto v_i + \beta z_i) \qquad [4]$$

3.1. Enfoque I – Maximização do lucro esperado

Tomando ρ_i como o valor das informações da iésima firma que seriam perdidas caso houvesse um problema de segurança

da informação, as firmas tomam decisões de investimento em segurança da informação de forma a maximizar o lucro esperado E(π). Seguindo essa representação, o problema de maximização de lucro da firma pode ser representado da seguinte forma:

$$Max_{zi}\ F(\propto v_i+\beta z_i)(\pi_i-z_i-\rho_i)+(1-F(\propto v_i+\beta z_i))(\pi_i-z_i) \quad [5]$$

Rearranjando os termos, tem-se o seguinte problema:

$$Max_{zi}\ -F(\propto v_i+\beta z_i)\ \rho_i+\pi_i-z_i \quad [6]$$

cujas condições de primeira e segunda ordens são, respectivamente:

$$z_i:\ -\frac{\partial F}{\partial z}\beta\rho_i-1:-\frac{\partial^2 F}{\partial z^2}\beta^2\rho_i \quad [7]$$

Essas condições mostram que, basicamente, a decisão de investir em mecanismos de segurança da informação dependerá do sinal do coeficiente β. Se o coeficiente é positivo, então o efeito marginal do investimento sobre o lucro esperado será negativo e, logo, haveria uma solução de canto para o problema. Caso o coeficiente seja negativo, a condição de primeira ordem satisfaz os requisitos para que haja incentivos para adotar níveis positivos de investimento em segurança da informação. Um ponto relevante a ser ressaltado é que a primeira derivada da função densidade é a própria função distribuição de probabilidade que assume valores positivos. Para que haja uma solução interior é necessário que a segunda derivada da função densidade seja positiva. Em outras palavras, como se assume que a distribuição de probabilidade seja simétrica:

$$E(\varepsilon_i)>\propto v_i+\beta z_i^* \quad [8]$$

$$\propto v_i-E(\varepsilon_i)<-\beta z_i^* \quad [9]$$

Essa condição mostra que haverá uma solução interior quando o efeito total do investimento em segurança da informação sobre a probabilidade de perda for maior do que o efeito total da vulnerabilidade sobre a probabilidade de perda corrigida pelo erro médio[2].

3.2. Enfoque II – Minimização / Identificação do problema de segurança

Caso γ_i denote o evento em que a firma identifica um problema de segurança da informação, tem-se um problema análogo ao anterior, entretanto, as interpretações obtidas anteriormente são revertidas. Basicamente, o fato de uma firma identificar esse problema associa-se de forma negativa com a ocorrência de uma perda por parte da firma. O argumento é que as firmas que conseguem identificar o problema podem adotar medidas de forma a minimizar as possíveis perdas. Como a formulação do problema agora é vista como uma minimização da perda esperada, obtêm-se condições de primeira ordem análogas[3] ao do enfoque I. Entretanto, a interpretação do coeficiente β é revertida no sentido de que, se for positivo, indica que a firma terá incentivos para investir em segurança da informação.

No que concerne ao grau de vulnerabilidade da firma, assume-se que é uma variável exógena e, portanto, por meio do teorema do envelope ter-se-ia que a relação entre o grau de vulnerabilidade da firma e seu lucro esperado pode ser representada por:

$$:\ -\frac{\partial F}{\partial z}\beta\rho_i-1:-\frac{\partial^2 F}{\partial z^2}\beta \quad [10]$$

Pelas condições acima, nota-se que a relação do grau de vulnerabilidade com o lucro esperado dependerá do efeito marginal da vulnerabilidade sobre a probabilidade de ocorrência de perda. É razoável que essa última relação seja crescente. Quanto mais vulnerável é uma firma, maior se torna a probabilidade de ocorrência da perda. O modelo desenvolvido por Gordon e Loeb (2002) relaciona o grau de vulnerabilidade com o nível de investimento e mostra que apenas firmas com grau médio de vulnerabilidade investirão em segurança da informação. Em outras palavras, firmas com pequeno grau de vulnerabilidade não investirão, pois o custo do investimento é maior do que a perda esperada, e também as firmas com alto grau de vulnerabilidade não investirão, pois o custo do investimento é inviável, ou seja, é estabelecida uma relação de custo efetividade. De certa maneira, os resultados obtidos refletem esse fato, dado que o investimento só será ótimo caso o efeito total do investimento sobre a probabilidade da perda ou identificação seja superior ao efeito total da vulnerabilidade.

4. DADOS E ESTATÍSTICAS DESCRITIVAS

Os dados utilizados na análise empírica provêm da Pesquisa Sobre Uso das Tecnologias da Informação e Comunicação – TIC Empresas 2009 – CETIC. O desenho da amostra foi feito pelo Instituto Brasileiro de Opinião Pública e Estatística IBOPE Inteligência, que foi responsável pela coleta de dados e tratamento estatístico, de forma que o erro amostral fosse de 2% em um intervalo de confiança de 95% (CGI, 2010).

O plano amostral das Tecnologias da Informação e Comunicação (TIC) Empresas foi elaborado com o objetivo de medir o acesso e o uso das TIC em empresas com dez ou mais funcionários, pertencentes ao setor organizado da economia no Brasil, listadas na Relação Anual de Informações Sociais (RAIS) e integrantes de determinados segmentos da Classificação Nacional de Atividades Econômicas (CNAE)[4]. Para a edição de 2009, foram selecionadas 3.737 empresas, sendo 47,9% pertencentes à região Sudeste, 16,8% à Sul, 9,6% à Centro-Oeste, 8,5% à Norte e 17,2% à Nordeste. Essa amostra é representativa de 340.000 empresas e representa cerca de 12% de todas as firmas listadas no cadastro da RAIS.

No que concerne à composição do porte das empresas, 35% apresentam de 10 a 19 empregados, 19% de 20 a 49, 16% de 50 a 99, 8% de 100 a 249 e 22% mais de 250 empregados.

Na Tabela 1 são fornecidas algumas estatísticas sumárias a respeito da incidência de problemas de segurança da informação, da composição de funcionários que acessam a internet na empresa e das medidas de segurança da informação adotadas.

Conforme é mostrado na Tabela 1, 71,6% das firmas reportaram ter encontrado algum tipo de problema de segurança da informação. Quando se analisa esse evento em relação ao número de funcionários com acesso à internet, percebe-se uma relação positiva. Assumindo que o grau de vulnerabilidade cibernética de uma firma está diretamente associado ao número de funcionários com acesso à internet, pelos dados a

Tabela 1

Estatísticas Sumárias – Porcentagem sobre o Total de Firmas com Acesso à Internet em 2009

Variáveis	Total	Proporção de Funcionários com Acesso à Internet			
		Até 20%	De 21% a 50%	De 51% a 70%	Acima de 70%
Problema de Segurança	71,6	65,1	75,7	81,6	81,0
Vírus	63,0	53,6	65,7	75,9	71,0
Cavalos de Tróia	53,0	44,3	56,3	58,2	60,8
Worms ou *Bots*	21,0	14,9	19,7	29,7	29,4
Acesso Interno Não Autorizado	9,0	7,4	7,9	11,9	11,0
Acesso Externo Não Autorizado	9,0	5,8	9,7	14,8	13,2
Fraude Facilitada por TIC	6,0	5,7	4,4	7,4	9,1
Ataque de Negação de Serviço (DOS)	5,0	3,6	4,9	7,9	8,5
Ataque ao Servidor	5,0	3,0	5,6	5,8	7,6
Departamento de TI (DP.TI)	25,0	16,2	25,1	38,4	49,7
Treinamento em TIC[1]	31,0	22,5	32,3	49,4	43,0
Política de Segurança	38,0	27,1	35,3	54,2	59,7
Mecanismos de Defesa	98,0	93,6	98,6	99,2	99,8
Antivírus	98,0	92,3	98,2	99,0	99,4
Antispam	73,0	62,1	71,9	74,5	86,7
Antispyware	66,0	53,9	64,2	74,2	83,4
Firewall	61,0	45,6	60,7	71,8	80,5
Sistema IDS[2]	34,0	26,2	29,1	45,2	53,6
Nenhum	2,0	–	–	–	–

Variáveis	Contramedidas em Segurança da Informação			
	Departamento TI	Sem Departamento TI	Política Segurança	Sem Política Segurança
Problema de Segurança	78,1	69,3	77,8	66,4
Vírus	69,9	58,1	68,5	57,0
Cavalos de Tróia	58,1	48,9	57,0	48,0
Worms ou *Bots*	32,3	15,1	29,9	13,7
Acesso Interno Não Autorizado	11,2	7,4	11,1	6,9
Acesso Externo Não Autorizado	14,5	6,5	12,8	6,2
Fraude Facilitada por TIC	7,5	5,6	8,0	5,0
Ataque de Negação de Serviço (DOS)	8,6	3,8	7,3	3,8
Ataque ao Servidor	6,6	4,0	6,5	3,7
Departamento de TI (DP.TI)	–	–	46,9	14,5
Treinamento em TIC[1]	50,4	23,1	49,0	19,4
Política de Segurança	65,2	26,5	–	–
Mecanismos de Defesa	98,5	95,7	99,4	94,3
Antivírus	98,1	94,6	98,9	93,6
Antispam	84,2	64,8	84,8	61,3
Antispyware	80,8	56,8	79,4	53,7
Firewall	78,4	49,9	77,2	46,0
Sistema IDS[2]	55,0	25,2	53,2	21,3
Nenhum	1,5	4,5	0,5	5,7

Notas: [1]Percentual sobre o número de firmas que utilizam computador. [2]IDS = Sistema de Detecção de Intrusão.

Fonte: Elaborada com base na Pesquisa Sobre o Uso das Tecnologias da Informação e Comunicação – CETIC 2009 – Comitê Gestor de Informática – CGI (2010).

seguir aponta-se uma relação crescente entre o grau de vulnerabilidade e a proporção de firmas que identificaram problemas de segurança da informação, até a faixa de 51 a 70% de funcionários com acesso à internet. A partir desse patamar, a incidência de problemas de segurança continua a crescer em alguns casos (*trojans*, fraudes, DOS e ataques a servidor) e a decrescer em outros (vírus, *worms*, acessos internos e externos não autorizados).

Dentre os problemas de segurança, vírus é o tipo mais comum seguido dos "cavalos de tróia", *worms*, acessos não autorizados e fraudes. Nota-se que, dentre as firmas que possuem um departamento de Tecnologia da Informação (TI) e/ou adotam uma política de segurança da informação, as frequências dos problemas reportados são maiores do que para o extrato de firmas que não possuem política ou departamento de TI.

De certa forma, isso revela um dado preocupante, pois, em uma primeira análise, sugere que o investimento em segurança da informação aumenta a propensão da firma a ter algum tipo de problema de segurança da informação. Contudo, uma análise cautelosa deve ser feita, uma vez que o fato de a firma reportar um problema de segurança está diretamente atrelado ao fato de que ela identificou esse problema de segurança.

Um aspecto revelado pela tabela, que dá suporte a essa ideia, é que as firmas com maior vulnerabilidade são também as que apresentam uma estrutura de TI e defesa cibernética mais sofisticada. Nota-se, por exemplo, que à medida que aumenta o extrato de funcionários com acesso à internet, expande-se também a proporção de firmas que possuem um Sistema de Identificação de Intrusão (IDS) que dentre as ferramentas de defesa é a menos comum. Portanto, essa relação positiva pode indicar maior probabilidade de identificação do problema.

Contudo, os fatos expostos na Tabela 1 não levam em conta a influência de efeitos cruzados de algumas características das firmas. Na próxima seção, são estimados modelos *logit* e *probit* ordenado como forma de avaliar os efeitos sobre a probabilidade de problemas de segurança da informação, levando-se em conta efeitos covariados como região, tipo de mercado, estrutura de rede da firma, quantidade de funcionários com acesso à internet e variáveis ligadas à segurança da informação como forma de avaliar o efeito de investimentos sobre o risco ou a probabilidade de identificação.

5. MODELOS EMPÍRICOS E RESULTADOS

Conforme apresentado anteriormente, neste trabalho buscou-se analisar como medidas associadas a investimentos em segurança da informação influenciam a probabilidade de identificar a ocorrência de problemas associados à segurança da informação para uma amostra representativa de firmas com mais de dez funcionários no Brasil, a partir de dados do CGI. Para atingir o objetivo, modelos *logit* e *probit* ordenado foram desenvolvidos e serão detalhados a seguir.

5.1. Modelos *logit*

A primeira pergunta que se procura responder no estudo é:

- Quais os determinantes da probabilidade das firmas identificarem ou não problemas de segurança da informação?

De maneira a responder a essa pergunta e compreender como as medidas de segurança da informação e o grau de vulnerabilidade cibernética das firmas influenciam a probabilidade da identificação de problemas de segurança da informação (SI), propõe-se o seguinte modelo *Logit*:

$$Pr(\gamma=1 \mid X)=\Lambda(X'\beta)=\frac{1}{1+e^{-(X'\beta)}} \quad \textbf{[11]}$$

em que:

$$\gamma=\begin{cases} 1 \text{ se identificou-se problema de SI} & |\text{-}\varepsilon_i < X'\beta \\ 0 \text{ se não se identificou problema de SI} & |\text{-}\varepsilon_i \geq X'\beta \end{cases}$$

e

$$X'\beta=\beta_0+\beta_1 ÁREA_i+\beta_2 MERCADO_i+\beta_3 \ln(LInternet_i)+\beta_4 Política_i+\beta_5 Treinamento_i+\beta_6 Defesa_i$$

tal que:

$ÁREA_i$ = Região geográfica da firma (Sudeste, como referência).

$MERCADO_i$ = Setor de atuação da firma, tais como Indústria da Transformação, Comércio etc. (Outros, como referência).

$LInternet_i$ = Número de funcionários da firma que possuem acesso à internet. Essa variável representa uma *proxy* da medida de vulnerabilidade cibernética.

$Política_i$ = Variável *dummy* que indica se a firma possui algum tipo de política de segurança da informação (firmas que não possuem política, como referência).

$Treinamento_i$ = Variável *dummy* que indica se a firma aplica algum tipo de treinamento para o uso de Tecnologias da Informação e Comunicação (firmas que não aplicam treinamento, como referência).

$Defesa_i$ = Conjunto de variáveis *dummy* que indicam o número de mecanismos de defesa cibernética que a firma adota, tais como: antivírus, *antispam*, *antispyware*, sistema de identificação de intrusão (IDS) e *firewall* (para cada *dummy* a referência são as firmas que não adotam o determinado mecanismo representado pela *dummy*).

Como tanto o investimento em segurança em informação quanto o grau exato de vulnerabilidade cibernética podem ser observados, utilizam-se medidas associadas a essas variáveis.

O investimento em segurança da informação é associado ao grau de sofisticação dos mecanismos de defesa e às medidas de conscientização de capital humano, tais como a presença de uma política de segurança da informação e treinamento aos funcionários para o uso de TICs.

O grau de vulnerabilidade cibernética é uma medida imensurável; entretanto, postula-se que quanto mais funcionários uma firma possui, maior será o grau de vulnerabilidade por causa da maior presença de canais de intrusão, como contas de *e-mail* e número de acessos a *sites* indevidos na internet.

Na Tabela 2, são expostos os resultados da regressão do modelo logístico.

Os coeficientes estimados pelo modelo logístico (Tabela 2) apontam que há uma relação positiva entre o número de funcionários com acesso à internet e a ocorrência de problemas de segurança. Os resultados das colunas (1), (2) e (3) apresentam coe-

Tabela 2

Modelos Logísticos para Identificação de Problemas de Segurança da Informação pelas Firmas

Variáveis	(1)	(2)	(3)	(4)	(5)
LnLInternet[1]	0,267***	0,292***	0,292***		
	(0,0525)	(0,0487)	(0,0487)		
Política	0,0201			0,207*	
	(0,127)			(0,120)	
Treinamento em TIC	0,356***			0,460***	
	(0,120)			(0,116)	
Firewall	0,184			0,314***	
	(0,128)			(0,122)	
IDS	-0,226*			-0,174	
	(0,132)			(0,128)	
Antispyware	0,126			0,215	
	(0,148)			(0,140)	
Antispam	0,253*			0,420***	
	(0,152)			(0,142)	
Defesa1			-1,386***		-2,506***
			(0,369)		(0,292)
Defesa2		1,018***	-0,368**		-0,786***
		(0,371)	(0,172)		(0,153)
Defesa3		1,326***	-0,0598		-0,396**
		(0,381)	(0,185)		(0,172)
Defesa4		1,650***	0,264		0,0463
		(0,373)	(0,167)		(0,159)
Defesa5		1,500***	0,114		-0,00305
		(0,368)	(0,150)		(0,147)
Defesa6		1,386***			
		(0,369)			
Vulnerabilidade Média				0,414***	0,377***
				(0,121)	(0,121)
Vulnerabilidade Alta				0,166	0,208
				(0,263)	(0,254)
Constante	-0,112	-1,085**	0,302	-0,336	0,729***
	(0,305)	(0,444)	(0,318)	(0,268)	(0,281)
Teste F – Valor *p*[2]	0,000	0,000	0,000	0,000	0,000
Observações	3.437	3.437	3.437	3.557	3.557

Notas: [1]Número de funcionários com acesso à internet na firma. [2]Teste de significância global. Desvio padrão entre parênteses (). ***p<0,01, **p<0,05, *p<0,1.
Variáveis controle: região e mercado de atuação da firma.

ficientes positivos e significantes a um nível de significância de 1%, suportando em parte os resultados obtidos pelo modelo teórico. Contudo, na coluna (1) nota-se também que algumas variáveis ligadas a contramedidas em segurança da informação apresentam um efeito positivo sobre a probabilidade de identificação de problemas ligados à segurança da informação. Na coluna (1) a variável treinamento TIC apresenta um coeficiente significante a um nível de 1% e a variável *antispam,* a 10%. A única das variáveis ligadas à segurança da informação que apresentou efeito negativo e significante é a variável IDS, que denota se a firma possui um sistema de detecção de intrusão. Nesse sentido, esse resultado, perante a primeira abordagem do modelo teórico apresentado, sugere que o investimento em segurança da informação tem efeitos negativos sobre o lucro esperado.

De forma a confrontar os resultados obtidos na coluna (1), são elaboradas formas alternativas de mensurar as contramedidas em segurança da informação. Nas colunas (2), (3) e (5), em vez de especificar *dummies* relativas às medidas de segurança, são agregados os mecanismos de defesa de forma a ordenar as firmas com respeito ao número de mecanismos de defesa.

Os resultados das colunas (2) e (3) são distintos apenas devido às referências utilizadas. No caso da coluna (2), a referência é o grupo de firmas que não possui nenhum dos mecanismos de defesa, ao passo que na coluna (3) a referência é o grupo de firmas que possui todos os mecanismos de defesa cibernética.

Os resultados das colunas (2) e (3) continuam a sustentar os resultados obtidos na coluna (1). Observa-se que há uma relação crescente entre o número de mecanismos de defesa cibernética e a probabilidade de ocorrência de problemas de segurança.

Nas colunas (4) e (5) são utilizadas *dummies* que denotam o grau de vulnerabilidade. Basicamente, o que se observa nessas duas especificações é que o efeito positivo da vulnerabilidade cibernética é em grande parte atribuído às firmas com vulnerabilidade média, ou seja, firmas que possuem de 21 a 70% dos funcionários com acesso à internet. Nota-se que as firmas que possuem mais do que 70% dos funcionários com acesso à internet não têm uma probabilidade diferente das firmas com até 20%.

É válido ressaltar que na coluna (4) são utilizadas variáveis *dummies* específicas de cada mecanismo de defesa cibernética e elas se mostram positivas e algumas significantes.

Os resultados positivos relativos às medidas de defesa cibernética obtidos nessa primeira análise sugeririam, *a priori*, que os investimentos em segurança da informação aumentam as chances de identificação de problemas correlacionados.

Do ponto de vista econométrico, esse resultado pode ser uma consequência da dinâmica dos fatos no sentido de que uma firma adota mecanismos de defesa porque sofreu algum problema de segurança da informação anteriormente.

Contudo, há evidências que também suportam outra razão. Na Tabela 3, são apresentados os coeficientes de correlação entre o número de mecanismos de defesa e a proporção de funcionários com acesso à internet. Observa-se que há uma relação crescente entre o número de funcionários com acesso à internet e o número de mecanismos de defesa adotados.

Esse fato dá suporte à hipótese de que as firmas que adotam mecanismos de defesa sejam mais propensas à identificação de problemas de segurança. Entretanto, isso ocorreria não porque os investimentos são ineficazes, mas sim pelo fato de que – ao possuírem um sistema mais sofisticado de defesa – essas firmas estariam mais aptas a identificar os problemas de segurança.

5.2. Modelos *probit* ordenado

A segunda pergunta que se procura responder no estudo é:

- Quais os determinantes da probabilidade das firmas identificarem um ou mais problemas de segurança da informação?

De forma a responder a essa pergunta e verificar a hipótese citada no fim da seção 5.1, agregam-se também os tipos de problemas de segurança para testar se as firmas com sistemas de defesa mais sofisticados estão mais propensas a identificar mais tipos de problemas de segurança da informação. Basicamente, na pesquisa elaborada pela CGI é perguntado se as firmas identificaram vírus, *worms*, fraudes, negação de serviços (DOS) e invasão de sistema (*cyber attack*). As informações relativas a esses ataques são utilizadas para construir uma variável dependente que mensura

Tabela 3

Correlações entre Medidas de Segurança e Número de Funcionários com Acesso à Internet

Porcentagem de Funcionários com Acesso à Internet	Número de Mecanismos de Defesa Cibernética					
	0	1	2	3	4	5
Até 20%	0,1199***	0,1314***	0,0516***	0,0324**	-0,0488***	-0,1399***
De 21% a 50%	-0,0572***	-0,0189	0,0318*	-0,0026	0,0283*	-0,0104
De 51% a 70%	-0,0285*	-0,0529***	-0,0492***	0,0172	0,0011	0,0612***
Acima de 70%	-0,0729***	-0,1158***	-0,0721***	-0,0491***	0,0304**	0,1544

Notas: ***p<0,01, **p<0,05, *p<0,1.

Fonte: Elaborada a partir de dados da Pesquisa Sobre Uso das Tecnologias da Informação e Comunicação – CETIC 2009 – Comitê Gestor de Informática – CGI (2010).

o número de tipos de ataques que a firma identificou[5]. Com base nessa variável, são estimados modelos de *probit* ordenado. As variáveis independentes são as mesmas dos modelos *logit*.

Na Tabela 4 são apresentados os resultados do modelo *probit* ordenado para quatro especificações. Os resultados obtidos continuam a mostrar sinais positivos para as medidas de segurança da informação, indicando que quanto mais sofisticado o sistema de defesa cibernética da firma maior será a probabilidade de identificar um maior número de tipos de problemas de segurança da informação.

Observa-se nas colunas de (1) a (4) que o sinal positivo ligado às medidas de vulnerabilidade cibernética continua a persistir. No que se refere às medidas de defesa cibernética, observa-se nas colunas de (2) a (4) que, relativamente às firmas que não adotam medida alguma, as firmas que possuem maior número de mecanismo de defesa têm maior probabilidade de identificação de um maior número de problemas cibernéticos. Na coluna (1) observa-se que o Treinamento em TIC possui efeito positivo e mecanismos como *firewall* e *antispam* também apresentam um sinal positivo estatisticamente significante.

Portanto, o fato de os últimos resultados apontarem para a persistência da relação positiva entre as contramedidas de segurança da informação e a identificação de problemas de segurança da informação não quer dizer que os investimentos em defesa cibernética não devam ser realizados. Ao contrário, reforça a premissa de que investimentos em defesa cibernética aumentam as chances de identificação do problema e, com isso, permitem maiores chances de reação por parte das firmas de forma a evitar maiores prejuízos.

Tabela 4

Probits Ordenados para Números de Tipos de Ataques que as Firmas Identificaram

Variáveis	(1)	(2)	(3)	(4)
LnLInternet[1]	0,135*** (0,0210)	0,160*** (0,0196)	0,160*** (0,0196)	
Política	0,0852 (0,0558)			
Treinamento em TIC	0,193*** (0,0551)			
Firewall	0,154*** (0,0572)			
IDS	-0,00338 (0,0569)			
Antispyware	0,0973 (0,0713)			
Antispam	0,145** (0,0721)			
Defesa1		-0,997*** (0,198)		
Defesa2		-0,481*** (0,0819)	0,516*** (0,199)	0,926*** (0,158)
Defesa3		-0,241*** (0,0831)	0,756*** (0,202)	1,216*** (0,162)
Defesa4		-0,115 (0,0733)	0,882*** (0,199)	1,382*** (0,157)
Defesa5		-0,103 (0,0653)	0,894*** (0,197)	1,430*** (0,156)
Defesa6			0,997*** (0,198)	1,571*** (0,156)
Vulnerabilidade Média				0,253*** (0,0511)
Vulnerabilidade Alta				0,319*** (0,0700)
Teste F – Valor *p*[2]	0,000	0,010	0,020	0,030
Observações	3.437	3.437	3.437	3.557

Notas: [1]Número de funcionários com acesso à internet na firma. [2]Teste de significância global. Desvio padrão entre parênteses (). ***p<0,01, **p<0,05, *p<0,1.
Variáveis controle: região e mercado de atuação da firma.

6. CONCLUSÃO E TRABALHOS FUTUROS

Neste trabalho, teve-se como objetivo analisar como medidas associadas a investimentos em segurança da informação influenciam a probabilidade de identificar a ocorrência de problemas associados à segurança da informação, para uma amostra representativa de firmas com mais de dez funcionários no Brasil.

Os resultados obtidos pela análise empírica apontam para uma relação positiva entre as medidas de segurança da informação e a probabilidade de ocorrência de problemas de segurança. Contudo, uma análise mais cautelosa levanta a hipótese de que a relação positiva entre medidas associadas à proteção tecnológica e a ocorrência de problemas de segurança da informação seja atribuída ao fato de que uma sofisticação das medidas de proteção aumente a probabilidade de identificação dos problemas e não uma maior incidência deles.

Esse resultado é evidenciado por meio de uma análise do modelo *probit* ordenado, que leva em conta o número de tipos de problemas identificados pelas firmas e sustenta o resultado positivo entre as medidas de investimento e o número de problemas de segurança. Em outras palavras, firmas com maior grau de proteção identificam um maior número de tipos de problemas. Ademais, por meio de uma simples análise de correlação revela-se que as firmas de menor proporção de funcionários com acesso à internet são

também firmas com menor sofisticação em seus mecanismos de proteção cibernética e reforça a hipótese de identificação dos problemas.

A relevância desse resultado é evidenciar que investimentos em segurança da informação não têm o papel de inibir os problemas, mas sim de identificá-los e com isso diminuir as chances de prejuízos relacionados a ativos ligados à informação. Conforme defendem os especialistas do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT), "os riscos sempre vão existir, em qualquer meio" (Hoepers, 2011, p. 16).

Os especialistas do CERT também defendem que "educação é a chave" (Hoepers, 2011, p. 16). Takemura *et al.* (2008) identificaram que investimentos em educação sobre segurança são mais efetivos que investimentos em proteção tecnológica. Os resultados obtidos no presente artigo — tanto nos modelos de regressão logística quanto nos modelos de *probit* ordenado — mostram que as firmas que investem em treinamento em TIC também são mais propensas à identificação de problemas, o que se contrapõe aos resultados obtidos por Takemura *et al.* (2008).

É importante ressaltar que neste trabalho não foram levados em conta problemas de endogeneidade ligados à dinâmica dos eventos. Uma firma pode ter adotado medidas de segurança por ter sofrido algum problema anteriormente. Entretanto, a correlação entre o tamanho das firmas e a presença de mecanismos de proteção tecnológica coloca essa última hipótese em dúvida. Firmas de grande porte geralmente têm uma história de existência maior do que firmas pequenas e, portanto, a adoção de tais mecanismos de defesa muito provavelmente deve ter sido anterior à ocorrência de problemas no ano de 2009.

No entanto, essa é uma hipótese que deve ser testada para confirmação dos resultados obtidos. No caso, seria necessário olhar para dados relativos aos anos anteriores como forma de controlar a dinâmica dos investimentos. A pesquisa elaborada pelo CGI é realizada anualmente, mas as firmas sorteadas não são mantidas e o número de interseções entre os anos das pesquisas não é suficiente para que uma análise rigorosa possa ser feita. ◆

NOTAS

(1) Os dados das pesquisas do Comitê Gestor de Informática (CGI) mostram claramente que as firmas de maior porte são aquelas mais propensas a adotar mecanismos de segurança de informação e, igualmente, a identificar problemas de segurança. Uma análise simplista poderia inferir que quanto mais se investe em segurança, mais problemas ocorrem. A interpretação dos autores, discutida com os especialistas do CGI, é de que quanto maior a sofisticação tecnológica e o investimento em ferramentas de segurança, maior a probabilidade de identificar e informar os problemas. Por isso, adota-se ao longo do texto a nomenclatura de **identificação de problemas de segurança**. As ameaças e intrusões cibernéticas são uma realidade da internet. Se, por exemplo, um computador sofre ameaça de infecção por vírus, o usuário terá chance de detectar e resolver o problema caso tenha uma ferramenta de antivírus instalada. Caso contrário, o computador será contaminado, independente do conhecimento ou não do usuário.

(2) Se a distribuição considerada for uma normal padronizada, então a condição é simplificada e haverá solução interior quando o efeito total do investimento for superior ao efeito total da vulnerabilidade.

(3) Basicamente, a formulação do problema é da seguinte maneira: $Min_{zi}\ F(\propto v_i+\beta z_i)(z_i)+(1-F(\propto v_i+\beta z_i))(z_i+\rho_i)$ que gera as seguintes condições de primeira ordem: $-\partial F/\partial z\,\beta\rho_i+1$; $-(\partial^2 F)/(\partial z^2)\,\beta^2\rho_i$. É válido lembrar que agora $F(\propto v_i+\beta z_i)$ representa a probabilidade da firma identificar o problema de segurança. A análise das condições de primeira e segunda ordens mostra que a firma investirá em segurança da informação quando o coeficiente β for positivo e o efeito total do investimento em segurança sobre a probabilidade de identificação for superior ao efeito total da vulnerabilidade corrigido pela média do erro.

(4) Os setores selecionados incluem: Indústria da Transformação, Construção Civil, Comércio, Reparação de Veículos Automotores, Objetos Pessoais e Domésticos, Alojamento e Alimentação, Transporte, Armazenagem, Comunicações, Atividades Mobiliárias, Aluguéis e Serviços Prestados às Empresas, Outros Serviços Coletivos Sociais.

(5) Importante ressaltar que não é considerada a composição do número. Em outras palavras, duas firmas que identificaram dois tipos de ataques podem ter identificado conjuntos distintos de tipos de ataques. Essa decisão fundamenta-se basicamente na impossibilidade de atribuir um peso aos tipos de ataque.

REFERÊNCIAS

Anderson, R. (1994, November). Why cryptosystems fail. *Communications of the ACM*, *37*(11), 32-40.

Anderson, R. (2001). Why information security is hard: an economic perspective. *Proceedings of the Annual Computer Security Applications Conference,* Lousiana, ACSA, 17. Recuperado em 19 julho, 2011, de http://www.acsac.org/2001/papers/110.pdf.
doi: h10.1109/ACSAC.2001.991552

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhout, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 69-104.

Comitê Gestor de Informática (CGI) (2010). *Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil: TIC Domicílios e TIC Empresas 2009*. São Paulo: Comitê Gestor de Informática no Brasil.

Cremonini, M., & Nizovtsev, d. (2006). Understanding and influencing attackers' decisions: implications for security investment strategies. *Proceedings of the Workshop on The Economics of Information Security (WEIS),* Cambridge, I3P, 5. Recuperado em 19 julho, 2011, de http://weis2006.econinfosec.org/docs/3.pdf

Garcia, A., & Horowitz, B. (2006). The potential for underinvestment in internet security: implications for regulatory policy. *Proceedings of the Workshop on The Economics of Information Security (WEIS),* Cambridge, I3P, 5. Recuperado em 19 julho, 2011, de http://papers.ssrn.com/sol3/papers.cfm?abstract_id=889071.
doi:10.1007/s11149-006-9011-y

Gordon, L. A., & Loeb, m. p. (2002, November). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438-457.

Hoepers, C. (2011). *Princípios de segurança da informação*. I Ciberjur. São Paulo: OAB. Recuperado em 7 fevereiro, 2012, de http://www.cert.br/docs/palestras/certbr-ciberjur2011.pdf

Liu, W., Tanaka, H., & Kanta, M. (2008). Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms. *Information and Media Technologies*, *3*(2), 464-478.
doi: 10.2197/ipsjdc.3.585

Varian, H. (2004). System reliability and free-riding. In L. J. Camp, & S. Lewis (Eds.). Economics of Information Security. *Advances in Information Security*, *12*, pp. 1-15. New York: Springer.
doi: 10.1007/1-4020-8090-5_1

Moore, T., & Clayton, R. (2007). Examining the impact of website take-down on phishing. *Proceedings of the Anti-Phishing Working Group eCrime Researchers Summit*. New York: ACM. Recuperado em 19 julho, 2011, de http://www.ecrimeresearch.org/2007/proceedings/p1_moore.pdf.
doi: 10.1145/1299015.1299016

Moore, T., & Clayton, R. (2011). The impact of public information on phishing attack and defense. *Communications & Strategies*, *8*, pp. 45-68. Recuperado em 19 julho, 2011, de http://people.seas.harvard.edu/~tmoore/cs81.pdf

Takemura, T., Osajima, m., & Kawano, M. (2008, October). Economic analysis on information security incidents and the countermeasures: the case of Japanese internet service providers. *Advanced Technologies*.
doi: 10.5772/8203

Tanaka, H., Kmatsuura, k., & Sudoh, O. (2005, January/February). Vulnerability and information security investment: an empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, *24*(1), 37-59.
doi: 10.1016/j.jaccpubpol.2004.12.003

ABSTRACT

Countermeasures in information security and cybernetic vulnerability: empirical evidence of Brazilian companies

Recently, a series of cyber attacks to firms and governments, in Brazil and abroad highlighted the potential economic impact of this kind of activity, from private and public perspectives. There is a vast economic literature — theoretical and empirical — that evaluates the incentives for the adoption of measures of information security. The current study developed an empirical evaluation of this phenomenon in Brazil. Logit and ordered probit models were to evaluate the effects on the probability of occurrence of information security problems, considering firms' characteristics, including measures of information security. Results indicate that there is a positive correlation between measures of information security and the probability of identifying the occurrence of cyber attacks, what suggests that the sophistication of these measures of protection increase the probability of identification of the problems.

***Keywords*:** internet, information security, cyber attacks, econometrics.

RESUMEN

Las contramedidas en seguridad de la información y vulnerabilidad cibernética: evidencia empírica de las empresas brasileñas

Recientemente, una serie de ataques cibernéticos a firmas y gobiernos, en Brasil y en el exterior hizo público el potencial impacto económico de este tipo de actividad, tanto del punto de vista privado como público. Existe una extensa literatura económica — teórica y empírica — que analiza los incentivos para que las empresas adopten o no medidas de seguridad de la información. El presente estudio hizo una evaluación empírica de este fenómeno en Brasil. Modelos *logit* y *probit* ordenado fueron estimados para evaluar los efectos sobre la probabilidad de ocurrencia de problemas de seguridad de información, teniendo en cuenta características de las firmas, incluso las medidas de seguridad de información. Los resultados indican una relación positiva entre las medidas de seguridad de la información y la probabilidad de identificar la ocurrencia de problemas cibernéticos, lo que sugiere que la sofisticación de estas medidas de protección aumenta la probabilidad de identificación de los problemas.

Palabras clave: *internet*, seguridad de información, ataques cibernéticos, econometría.