Gabinete de Estratégia e Estudos
Ministério da Economia

Temas Económicos

Número 54

Agosto de 2018

A Economia da Cibersegurança

Gabriel Osório de Barros

Rua da Prata, nº 8 - 1149-057 Lisboa
Tel.: (351) 217921372
Fax: (351) 217921398
Web Site: www.gee.min-economia.pt

ISSN 1647-6204

Índice

1. Introdução....1
2. Enquadramento....1
2.1. Conceitos....2
2.2. Ameaças....3
3. O valor da informação....5
4. O valor da informação pessoal....7
5. A abordagem económica da Cibersegurança....10
6. O impacto da Cibersegurança....15
6.1. Custos de segurança....16
6.2. Nível de segurança....16
6.3. Benefícios de segurança....18
7. Gestão do Risco de Segurança da Informação....19
8. Estratégias de Segurança e Gestão do Risco....21
9. As falhas de mercado....22
9.1. Bens Públicos....23
9.2. Assimetria de Informação....23
9.3. Externalidades....25
9.4. Outras falhas de mercado....25
10. Notas finais....26
Referências....27

A Economia da Cibersegurança

Gabriel Osório de Barros

1. Introdução

A propagação de Ciberataques à escala global (por exemplo o *Wannacry* em Maio de 2017 e o *Petya* em Junho de 2017) provoca cada vez mais receios nos cidadãos e nas empresas que temem ser vítimas. Os riscos tecnológicos na era digital exigem que cada vez mais os utilizadores estejam protegidos e essa protecção passa também por garantir políticas públicas que procurem salvaguardar os seus interesses.

O Fórum Económico Mundial anunciou, em Janeiro de 2017, a criação de um Centro Global para o Ciberespaço que pretende fomentar a colaboração público-privada no âmbito da Cibersegurança. Segundo referiu o Director-Geral do Fórum, Alois Zwinggi, em conferência de imprensa em Davos, "a Cibersegurança transformou-se num dos assuntos mais importantes em todo o mundo", considerando que os custos com crimes informáticos atingirão já cerca de 500 mil milhões de dólares por ano.

Com o intuito de dar resposta a diversas questões sobre o papel da Economia, este Tema Económico apresenta uma resenha da teoria económica associada ao Ciberespaço e, em particular, à Cibersegurança, seguindo alguns dos pontos abordados por EdX/Delft (2017).

2. Enquadramento

O que actualmente conhecemos como computador teve a sua origem no início do século XX, culminado com a invenção do ENIAC em 1935 por John Eckert e John Mauchly.

A preocupação com a segurança da informação foi uma preocupação, em particular, desde que se iniciou a utilização mais generalizada de computadores a partir das décadas de 1960 e 1970.

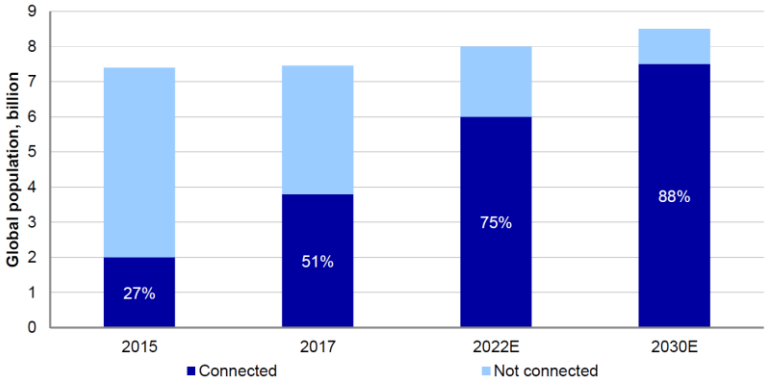
Inicialmente, com o advento dos primeiros sistemas informáticos, as empresas estavam isoladas entre si (em termos informáticos) pelo que os riscos eram mais limitados e a preocupação principal estava em restringir o acesso à informação dentro das próprias empresas (por exemplo, mantendo o controlo de informação sensível apenas acessível aos níveis hierárquicos superiores). No caso dos bancos, por exemplo, um erro informático ou um ataque aos sistemas de um banco não teria efeitos em cadeia.

O aparecimento da internet e a progressivamente maior ligação entre as empresas e entre estas e as pessoas veio alterar aquela realidade pois os impactos passaram a ter um potencial sistémico. A internet permitiu que os ataques informáticos ganhassem escala. Os primeiros softwares antivírus emergem a partir do momento em que surgem de forma expressiva *worms* (1989)[1] [2] e vírus informáticos [3] [4] (década de 1990), bem como ataques por hackers (década de 1990)[5].

[1] "Worm (general term): A worm is a self-replicating, self-contained software program that does not need to be part of another program to propagate. A virus, in contrast, attaches itself to and becomes part of another executable program. Worms as well as viruses typically contain some kind of malicious payload besides the propagation and infection mechanism." (Schell e Martin, 2006)

A este respeito, a Nordea estima que os potenciais alvos de Cibercrimes aumentem consideravelmente face à existência de um cada vez maior universo de pessoas conectadas (gráfico 1).

Gráfico 1 – Evolução dos potenciais alvos de Cibercrimes:
Utilizadores de Internet na população global



Fonte: Cybersecurity Ventures - Cybersecurity - Nordea On Your Mind (2018)

2.1. Conceitos

Para enquadramento dos principais conceitos associados à Cibernética que iremos tratar ao longo do documento, utilizaremos os conceitos de Kissel (2013):

- "Cyberspace – A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."
- "Cyber Infrastructure – Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure."

---

[2] "(…) on November 3, 1988, Robert Morris Jr. became known to the world when as a graduate student at Cornell University, he accidentally unleashed an Internet worm that he had developed. The worm, later known as "the Morris worm," infected and subsequently crashed thousands of computers." (Schell e Martin, 2006)

[3] Virus (general term): Can be a harmful, self-replicating program usually hidden in another piece of computer code, such as an email message. However, some virus infections are purely hostbased, so they do their "black magic" only locally. Because viruses replicate across a network in a variety of ways, they can cause Denial of Service (DoS) attacks in which the victim is not specifically targeted but is an unlucky host. Depending on the type of virus, the DoS can be hardly noticeable—or it can cause a major disaster. (Schell e Martin, 2006)

[4] O vírus Michelangelo vou um dos primeiros exemplos, embora o seu impacto tenha sido muito limitado. "Michelangelo virus (general term): In 1992, a virus scare centered on the Michaelangelo virus. Up to five million computers were estimated to be targets for infection by the virus, according to John McAfee, producer of McAfee's virus-scan software. Millions of dollars were spent by companies, institutions, and government agencies to prepare for this possible cyber Apocalypse— which turned out to be no more than a minor virus scare. The virus received its name from the day on which it was expected to strike—Michelangelo's birthday. Because of McAfee's obvious error in predicting a potential cyber Apocalypse, his IT career ended. However, McAfee left with a nice "golden parachute" from the anti-virus software company he founded." (Schell e Martin, 2006)

[5] "The years from 1990 through 2000 are known as the Great Hacker Wars and Hacker Activism Era because during this time, cyberwars became a media story spinner. For example, the early 1990s brought in the "Hacker War" between two hacker clubhouses in the United States—the Legion of Doom (LoD) and the Masters of Deception (MoD)." (Schell e Martin, 2006)

- "Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks."
- "Cyber incident – Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein."
- "Cyberattack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."

2.2. Ameaças

Malware, uma abreviação de "*malicious software*" (software malicioso), é qualquer software que tenha como objectivo criar um dano no sistema operativo que o utilizador tenha conhecimento. Existem diversos tipos de *malware* mas os mais comuns são os vírus[6] e os *worms*[7]. No caso dos vírus, entra nos programas através de uma "*host file*" fazendo com que o CPU execute as instruções maliciosas, podendo espalhar-se e replicar-se para outros ficheiros. Já os *worms*, permanecem em ficheiro autónomos, não precisando de uma "*host file*" e não precisam de intervenção humana na execução do ficheiro "hospedeiro", podendo espalhar-se na rede aproveitando falhas em protocolos e configurações.

Um outro conhecido *malware* é o chamado *Trojan horse*[8] (cavalo de Tróia), cujo nome lhe é atribuído por alusão à história do cavalo de madeira deixado pelos gregos que os troianos levaram para dentro das muralhas como um troféu mas que carregava gregos no seu interior o que permitiu conquistar Tróia. Segundo o relatório da Microsoft (2017) relativo às ameaças verificadas no primeiro trimestre de 2017, os *trojans* constituem a categoria mais frequentemente identificada de *malware* por uma grande margem.

Outro *malware* é a chamada *logic bomb*[9] (bomba lógica)), a qual se trata de um código escondido que dá instruções a um vírus para desenvolver acções sempre que se verificam determinados critérios. Este tipo de *malware* mantém-se latente até que chegue um determinado momento ou que ocorra determinado evento e será tanto mais destrutivo quanto mais tempo estiver latente pois permite que se espalhe sem que as empresas de antivírus se apercebam da sua existência. O funcionamento em termos informáticos é semelhante: o utilizador instala programas que escondem outros programas maliciosos que desenvolver diversas acções como espiar o utilizador, espalhar *malware*, danificar o computador, entre outras.

O *phishing*[10], por seu lado, constitui uma forma de roubo de identidade uma vez que os "golpistas" utilizam endereços de email reais para enviar emails levando os receptores desses emails a fornecer informação pessoal como o cartão de crédito, os códigos de acesso à conta bancária, o número de cartão de cidadão, entre outras.

---

[6] "Virus, code that not only replicates itself but also infects another program, a boot sector, a partition sector, or a document with executable instructions (such as macros) by attaching itself or inserting itself into that medium. Although most viruses just replicate and do little more, others can cause a significant amount of damage." (Schell e Martin, 2006)

[7] "Worms, programs that make copies of themselves and infect other computer systems, typically without a user's action, exploiting vulnerabilities in operating system or application software. Worms can compromise the security of the computer and cause considerable damage." (Schell e Martin, 2006)

[8] "Trojan horses, software programs (often arriving in a joke program) that do not replicate or copy themselves but can and often do cause considerable system damage or compromise the system's security." (Schell e Martin, 2006)

[9] "Logic Bomb (general term): Hidden code instructing a computer virus to perform some potentially destructive action when specific criteria are met." (Schell e Martin, 2006)

[10] "Phishing (general term): A form of identity theft whereby a scammer uses an authentic looking email from a large corporation to trick email receivers into disclosing online sensitive personal information, such as credit card numbers or bank account codes." (Schell e Martin, 2006)

Outros exemplos de *malware* são o *spyware*[11], que faculta informação do utilizador a terceiros, ou o *adware*[12], que apresenta automaticamente publicidade ao utilizador e recolhe informação sobre os seus hábitos.

Existem muitos outros tipos de *malware*, como as *back orifice*[13] ou os *rootkit*[14] mas que não iremos tratar neste documento.

Finalmente, referimos duas ameaças recentes: o *Ransomware* e a *Cloud threat intelligence*.

O *Ransomware* é um tipo de *malware* que bloqueia o computador até que uma quantia em dinheiro seja paga aos hackers. Segundo a Microsoft (2017), os ataques do *Ransomware* têm vindo a aumentar. Ataques como o *WannaCry* ou o *Petya* [15] (ver figuras 1 e 2)bloquearam milhares de computadores em todo o mundo no primeiro semestre de 2017, com especial impacto na Europa sendo os países com maiores incidências a República Checa, Itália, Hungria, Espanha, Roménia e Croácia.

Figura 1 – *Screenshot* de computador infectado pelo WannaCry

Fonte: Cybersecurity – Nordea On Your Mind (2018)

[11] "Spyware, a stand-alone program that monitors a system's activities, detecting passwords and other confidential information without being detected, and sends this information to another computer." (Schell e Martin, 2006)

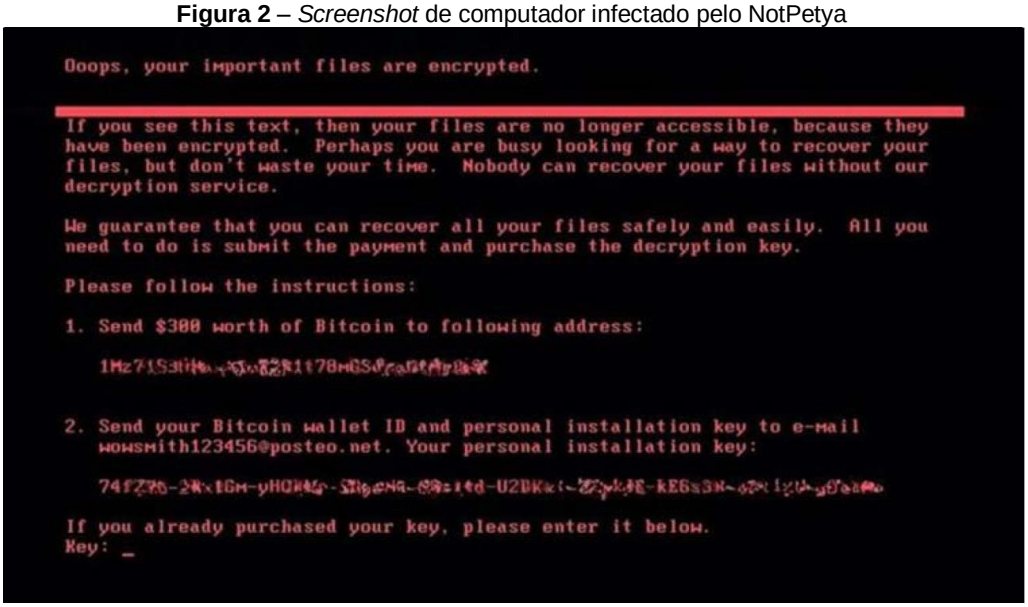
[12] "Adware programs that covertly gather personal information of online users and relay it to another computer, often for advertising objectives. This kind of information gathering is often done by tracking information related to Internet browser habits." (Schell e Martin, 2006)

[13] "Back Orifice (general term):Applies to a remote administration tool permitting system administrators to control a computer from a remote location, typically across the Internet." (Schell e Martin, 2006)

[14] "Rootkit (general term): A backdoor Trojan horse hiding behind or within processes and files that can provide crackers remote access to a compromised system. Besides being the name of a specific software tool, the term rootkit is often used in a more general sense to describe a tool providing system administrators access privileges to snoop while avoiding detection." (Schell e Martin, 2006)

[15] "Two new ransomware families, Win32/WannaCrypt (also known as WannaCry) and Win32/Petya, emerged in early 2017 to target out-of-date Windows operating systems." Microsoft (2017)

Figura 2 – *Screenshot* de computador infectado pelo NotPetya



Fonte: Cybersecurity – Nordea On Your Mind (2018)

3. O valor da informação

Segundo a teoria económica, o preço de equilíbrio num mercado em que existe concorrência de preços é o custo marginal de produção. Esta informação é importante quando analisamos o mercado de informação. A informação é tendencialmente gratuita e essa conclusão é fácil de retirar quando comparamos as antigas enciclopédias em papel (e.g., Enciclopédia Britânica) que tinham um custo elevado e as atuais enciclopédias *online* (e.g., Wikipédia) que são tendencialmente gratuitas pois o preço de "produzir" uma cópia adicional de uma enciclopédia online é zero, o que nos dá uma visão de uma característica realmente importante sobre os mercados de informação. Desta forma, este é o preço natural da informação. Esta conclusão é retirada por Varian (1998): "*Competitive markets tend to push price to marginal cost, which, in the case of information goods, is close to zero*".

A questão que se levanta quando analisamos a indústria da informação é como se faz dinheiro neste sector, quer estejamos a falar de *software*, filmes ou livros.

Por um lado, verifica-se que muitas vezes existem produtos associados ao produto que realmente queremos adquirir e que funcionam como um atractivo para consumir mais do mesmo fornecedor.

Por outro lado, a partir do momento em que o consumidor se adapta a um determinado produto tem alguma dificuldade em mudar (e.g., Windows vs. Macintosh).

Outra questão prende-se com os serviços que os consumidores adquirem que lhes permitem, por exemplo, ter tarifários ou consumos mais vantajosos mas que os deixa bloqueados a um determinado fornecedor [16].

[16] A respeito deste último ponto, convém notar as alterações introduzidas em 2016 ao período de fidelização (Lei n.º 15/2016, de 17 de junho [DRE]) que, embora se tenha mantido em 24 meses, passaram a obrigar as empresas operadoras de telecomunicações a apresentar ofertas com durações mais curtas e a reduzir o custo de rescindir dentro do período de fidelização.

Convém salientar, também, a questão do chamado *lock-in*. Os produtos associados à informação operam muitas vezes em sistemas diferentes, impedindo que o consumidor possa facilmente mudar de fornecedor. Este *lock-in* confere às empresas uma vantagem competitiva. Shapira e Varian (1998) dão um exemplo interessante, o do CD, que tinha elevados custos de transferência (switching costs). No entanto, neste caso o consumidor viu nesses custos uma vantagem pois o novo produto era superior aos anteriores LP [17].

Os *switching costs* a considerar são tanto do lado do consumidor (que poderá, por exemplo, perder uma oferta do operador para o fidelizar, como a atribuição de um maior pacote de dados móveis que não custam nada para a empresa) como do novo fornecedor (que para conseguir o novo cliente poderá ter que oferecer algo que este valorize, como um novo equipamento).

Outra questão relevante prende-se com a dimensão do mercado. Um sistema ou um *software* aumentam substancialmente o número de adesões à medida que aumentam a sua massa crítica. Tendencialmente, a evolução começa por ser pequena até que os clientes se comecem a aperceber de que há adesão pelo que se torna mais interessante aderir porque esse aumento torna esse sistema ou *software* mais propenso a estar associado a outros produtos desenvolvidos em complemento. Essa massificação também se torna propícia a que surjam vírus e *malwares*[18] direccionados para sistemas que têm mais utilizadores pois o seu impacto é maior.

O sector das Tecnologias da Informação e Comunicação (TIC) presta-se à criação de monopólios pois os produtos têm geralmente elevados custos fixos, reduzidos custos marginais, têm um efeito de *lock-in* que resulta das especificidades técnicas face a outros produtos e externalidades que favorecem produtos com maior adesão[19] (por exemplo, uma *app* de troca de mensagens só se torna relevante para aderir quando atinge uma determinada massa crítica).

Finalmente, os ganhos que são obtidos pelos fornecedores de serviços de informação estão intimamente ligados ao conhecimento que têm sobre os utilizadores, permitindo-lhes cobrar o valor correspondente à sua propensão marginal a pagar, ou seja, aplicando preços diferenciados conforme a propensão do cliente a adquirir.

Naturalmente, este funcionamento não é exclusivo da venda de *software* mas aplica-se também a outras indústrias como a venda de bilhetes de avião, o aluguer de viaturas ou o arrendamento de quartos de hotel.

[17] "Remember long-playing phonograph records (LPs)? In our lexicon, these were "durable complementary assets" specific to a turntable but incompatible with the alternative technology of CDs. In plain English: they were durable and valuable, they worked with a turntable to play music, but they would not work in a CD player. As a result, Sony and Philips had to deal with considerable consumer switching costs when introducing their CD technology. Fortunately for Sony and Philips, CDs offered significant improvement in convenience, durability, and sound quality over LPs, so consumers were willing to replace their music libraries." (Shapiro e Varian, 1998)

[18] "A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim." (Kissel, 2013)

[19] "Network externality has been defined as a change in the benefit, or surplus, that an agent derives from a good when the number of other agents consuming the same kind of good changes." (Liebowitz e Margolis, 1998)

4. O valor da informação pessoal

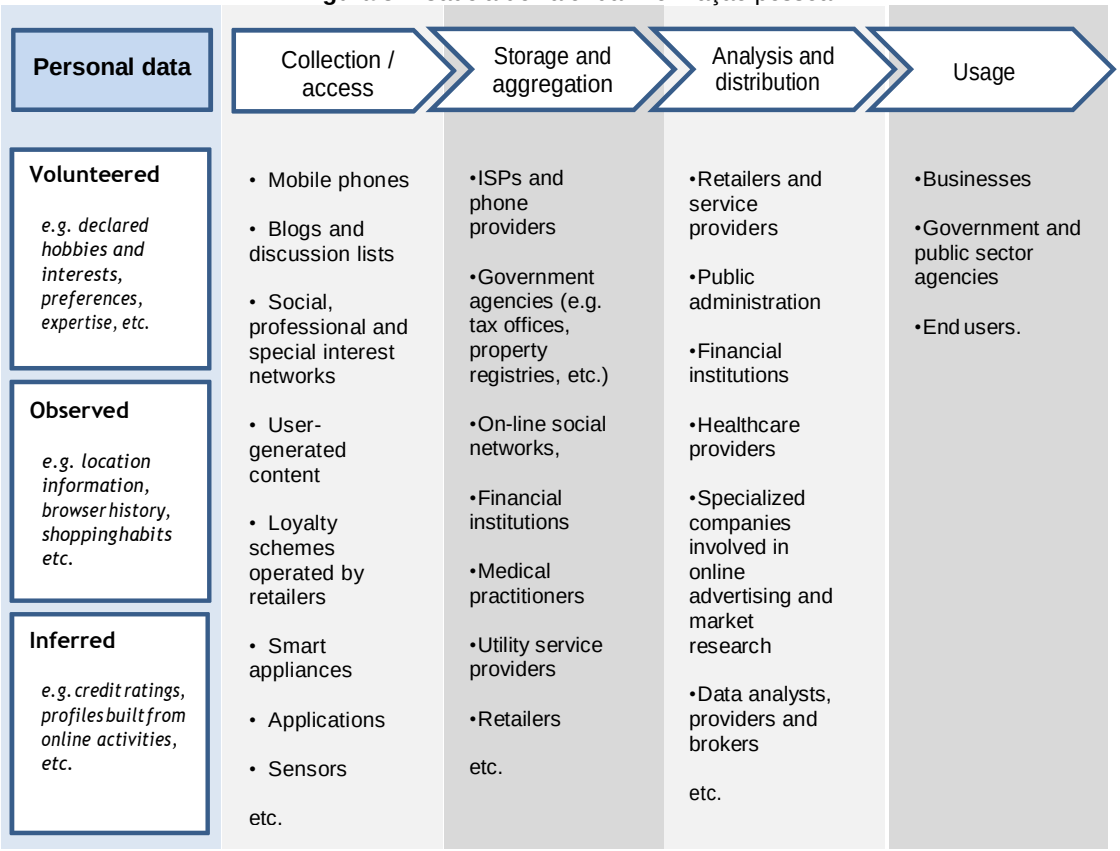
A informação pessoal é uma das áreas mais críticas da Cibersegurança pelo que abordaremos, de forma breve, as formas como essa utilização pode ocorrer e de que forma podemos valorizar essa informação.

Os dados pessoas podem ser disponibilizados voluntariamente (e.g., informação sobre hobbies partilhados através das redes sociais), observados através de comportamentos (e.g., informação sobre consultas online realizadas) ou inferidos (e.g., perfil de consumo realizado através das atividades online).

O Regulamento Geral de Proteção de Dados que entrou em vigor no dia 25 de maio de 2018 introduziu um novo regime em matéria de proteção de dados pessoais e constitui um passo também ao nível das questões de Cibersegurança, ao criar regras para o tratamento dos dados pessoais, definindo ainda novas regras e procedimentos do ponto de vista tecnológico. A forma como os dados pessoais podem ser tratados e arquivados passou a depender de autorização expressa das pessoas e o incumprimento pode ser sujeito a coimas elevadas, atribuindo uma maior segurança à informação.

Na cadeia de valor dos dados pessoais podem ser envolvidas diversas entidades em 4 fases: (i) a informação é recolhida com recursos a diversos dispositivos (e.g., telefones móveis), (ii) é armazenada e agregada (e.g., nas redes sociais), (iii) é analisada e distribuída (e.g., por empresas de estudos de mercado) e (iv) é utilizada (e.g., por empresas no seu marketing).

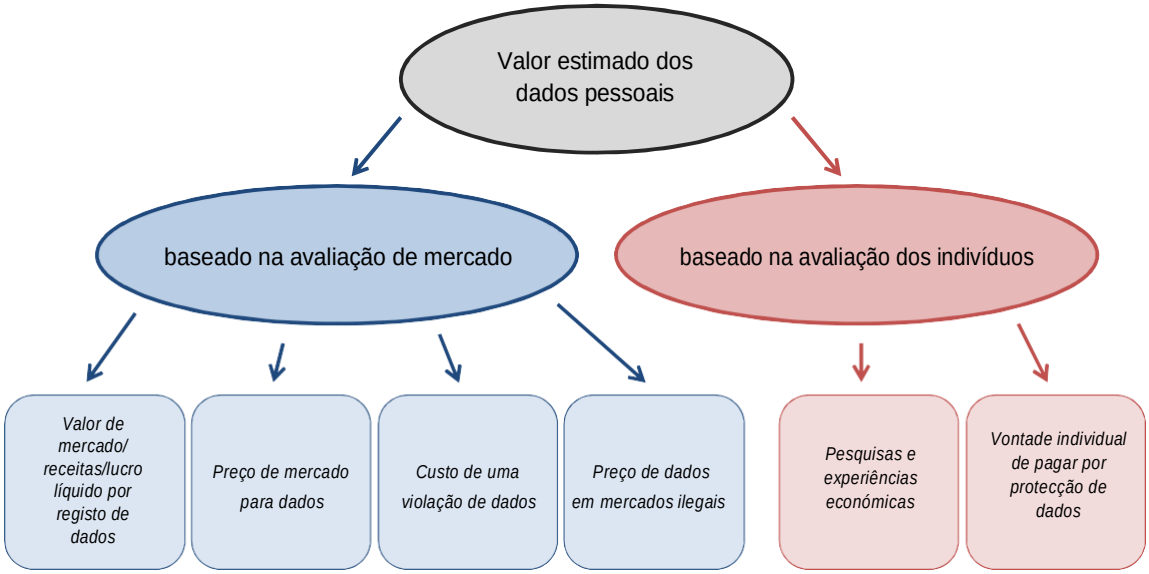
Figura 3 – Cadeia de valor da informação pessoal



Fonte: Exploring the Economics of Personal Data:
A Survey of Methodologies for Measuring Monetary Value (OCDE, 2013)

A avaliação do valor estimado dos dados pessoais é uma outra questão relevante quando procuramos analisar os impactos das quebras de segurança. Esta avaliação pode ter como base a avaliação do mercado (o valor de mercado d os dados pessoais) ou a avaliação que os próprios indivíduos fazem (verificada através de pesquisas ou estimadas a partir da necessidade de nível de protecção de dados que os indivíduos sentem necessidade).

Figura 4 - Estimativa do valor dos dados pessoais



Fonte: Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value (OCDE, 2013)

Segundo a OCDE (2013),

Não é, no entanto fácil medir o valor dos dados pessoais e existem várias abordagens metodológicas para o fazer. A tabela 1 resume uma série de medidas que podem ser utilizadas para a avaliação dos dados pessoais considerando as duas perspectivas referidas.

Tabela 1 - Summary of measures of value of personal data

Indicator	Description	Benefits	Potential Drawbacks
Indicators based on market valuation			
Financial results per data record	Aggregated market cap (revenues, or net income) of a company divided by the total number of personal data records used by this company.	- Relatively easy to identify. - Reflects actual economic value added generated through personal data.	- Likely to be inaccurate, as numerous other components impact market cap / revenues / income of a company. - Possible synergy effects could lead to overestimates for firms with larger datasets. Appropriateness of this approach depends on what portion of turnover is directly tied to personal data.
Market prices for data	Price per personal data entry offered on the market by data brokers.	- Relatively easy to identify; - Reflects market value of a given, specific data entry.	- Apart from the data value, it includes the cost of data search and processing. It also neglects the context in which the data is sold, which has a large influence on the demand (and price) for data.
Cost of a data breach	Economic cost of a data breach (for firms and individuals) per data entry.	- Reflects a real market value and a portion of the risk that companies must protect against.	- Captures market costs of damage caused by data breach rather than value of data themselves. Does not include the costs of damage to a firm's reputation.
Data prices in illegal markets	Estimation of prices of personal data (per data entry) in illegal markets.	- Reflects market value of a given, specific data entry.	- Difficult to measure and only applies to the context where the data is used again to obtain other benefits illegally. Because criminals must balance the risk of detection and punishment, the value of the personal data is likely undervalued by such an approach.
Indicators based on individual (data subjects') valuation			
Surveys and economic experiments	Valuation of personal data in monetary terms are reported / revealed by individuals in surveys / economic experiments.	- No ambiguity in data identification. - Captures the pure economic value of personal data from an individual perspective. - Results usually can be used for comparative studies (across economies and across various types of data).	- Hypothetical value not verified by the market. Previous research shows that a person's valuation of their own personal data is highly sensitive to context, meaning that the way questions are phrased could significantly alter the responses.
Individual willingness to pay to protect data.	Amounts that individuals are ready to spend to protect their personal data.	- Captures the pure economic value of privacy from an individual perspective.	- Captures individually perceived aggregate costs of damage caused by data breach, rather than value of data themselves.

Fonte: Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value (OCDE, 2013)

5. A abordagem económica da Cibersegurança

Como já foi referido, com o advento da internet, a questão da Cibersegurança e dos Cibercrimes emergiu como um problema, abrangendo áreas tão distintas como a fraude com cartões de crédito, o roubo de comércio eletrónico, a violação dos direitos de autor, o roubo de identidade, a pornografia infantil ou o *stalking (Schell e Martin, 2006)*.

Focar-nos-emos, agora, na importância da Segurança Informática na Economia, a qual começa a ter expressão no início da década de 1990.

No relatório do *System Security Study Committee* (1991), sobre "*Why the Security Market has not worked well*", Carl Landweh alertava para o facto de haver o risco de as principais empresas se dedicarem a mercados de massas sem a necessária preocupação com as questões de segurança.[20]

Dois anos mais tarde, Anderson (1993) verificou que existia uma melhor proteção dos consumidores nos bancos dos Estados Unidos da América em comparação com os do Reino Unido, não obstante estes últimos apresentarem um gasto superior com segurança, sendo de salientar que neste último os bancos conseguiam repercutir os custos das fraudes nos clientes.

A questão da Cibersegurança passa por perceber se as vulnerabilidades são externalidades e se podem ser resolvidas pelo mercado tal como no caso da poluição ambiental (mercado de CO2).

Varian (1996) verificou que o mercado não conseguia resolver os problemas de privacidade pessoal. Num momento em que ocorriam as primeiras tentativas de desenvolver sistemas de pagamento *online* sem grande sucesso, Varian (2000)[21] volta a recuperar o paradoxo entre uma maior despesa com segurança e, ainda assim, uma menor proteção do consumidor, considerando que tal se devia ao facto de o ónus da prova em situações de fraude ser do consumidor pelo que os bancos tratavam a questão com algum desleixo. O autor considerava que a realização de pagamentos *online* seria mais segura se houvesse uma melhor distribuição das responsabilidades de forma a incentivar todos os intervenientes a ter uma maior preocupação com a fraude.

A principal conclusão que se pode daqui retirar é que, num mundo em que cada vez mais as vulnerabilidades de uma empresa podem acarretar riscos para outras empresas, ter uma entidade a garantir a segurança do sistema e outra a suportar os custos associados às fraudes pode ser problemático.

[20] "The possible adverse consequences of holding software and system vendors to a higher standard of care must be carefully weighed against the potential benefits. As more powerful and more highly interconnected systems become more widespread, there will be increasing concern that the current allocation of the risk of software failure is too one-sided for an information society, at least for off-the-shelf software." System Security Study Committee (1991)

[21] "Why were the local banks so sloppy? The answer lies in the way liability is assigned in Britain. In the United States, if there is a dispute between a customer and a bank, the customer is right unless the bank can show that he is wrong. In Britain, the burden of proof is reversed; the bank is right unless the customer can show it is wrong. Since it is almost impossible for a customer to prove the bank made a mistake, British banks had little incentive to take care. The resulting sloppiness led to a rash of A.T.M. fraud. In the United States, banks have an incentive to invest in risk management techniques. Banks in areas prone to A.T.M. fraud, for example, have installed cameras and trained their staff in security practices. So, even though American banks spend less on security than do British banks, Mr. Anderson concluded, they deal with it more effectively." (Varian, 2000)

Adicionalmente, ao longo dos anos houve um aumento da preocupação por parte das empresas de contratar seguros que permitissem fazer face a situações de fraude. Nestes casos, tornou-se claro que as entidades que garantem em caso de fraude apenas aceitam segurar quando da parte das empresas existe uma segurança informática forte - caso contrário, o risco seria demasiado grande. Mais uma vez, verifica-se que a forma como o custo associado às fraudes é distribuído pode funcionar como um incentivo à implementação de sistemas de segurança.

Os estudos iniciais sobre o tema da Economia da Cibersegurança referem-se a uma época em que o comércio eletrónico era ainda irrelevante e em que o risco ainda era reduzido. O *boom* ocorreu no início do século XXI com estudos como os de Gordon e Loeb (2002), Böhme (2005) ou Anderson e Moore (2006).

Nos últimos anos, os estudos da European Union Agency for Network and Information Security sobre Threat Landscape (ENISA, 2014, 2015, 2016 e 2017) têm vindo a assinalar como principais ameaças à Cibersegurança o "*malware*", os "*web based attacks*" e os "*web application attacks*". Entre as principais ameaças, destacam-se, também, o "*phishing*", "*spam*", "*denial of service*", "*ransomware*" e "*botnets*".

Tabela 2 - Principais ameaças à Cibersegurança

	2014	2015	2016	2017
1	Malicious code: Worms / Trojans	Malware	Malware	Malware
2	Web-based attacks	Web based attacks	Web based attacks	Web based attacks
3	Web application / Injection attacks	Web application attacks	Web application attacks	Web application attacks
4	Botnets	Botnets	Denial of service	Phishing
5	Denial of service	Denial of service	Botnets	Spam
6	Spam	Physical damage / theft / loss	Phishing	Denial of servisse
7	Phishing	Insider threat accidental)	Spam	Ransomware
8	Exploit kits	Phishing	Ransomware	Botnets
9	Data breaches	Spam	Insider threat	Insider threat
10	Physical damage / theft / loss	Exploit kits	Physical manipulation / damage / theft / loss	Physical manipulation / damage / theft / loss
11	Insider threat	Data breaches	Exploit kits	Data breaches
12	Information leakage	Identity theft	Data breaches	Identity theft
13	Identity theft / fraud	Information leakage	Identity theft	Information leakage
14	Cyber espionage	Ransomware	Information leakage	Exploit kits
15	Ransomware / Rogueware / Scareware	Cyber espionage	Cyber espionage	Cyber espionage

Fonte: Threat Landscape, ENISA (2014, 2015, 2016 e 2017)

Embora sejam de difícil mensuração, tem-se verificado um aumento dos incidentes de segurança em termos de sofisticação, frequências e magnitude, com elevados custos para a economia[22]. A tabela 2 resume as principais quebras de segurança por sensibilidade da informação.

[22] "Although difficult to measure quantitatively, security incidents appear to be increasing in terms of sophistication, frequency and magnitude of impact. Security incidents can affect organisations' reputation, finances, and even their physical assets, undermining their competitiveness, ability to innovate and position in the marketplace. Individuals can suffer tangible physical or economic harms and intangible harms such as damage to reputation, or intrusion into private life. In addition, security incidents can impose significant costs on the economy as a whole, including by eroding trust, not just in the affected organisations, but also across sectors." (OCDE, 2016a)

Conforme podemos verificar, os principais ataques ocorreram entre 2014 e 2017 (17 dos 26 maiores).

Tabela 3 - Data Breaches by Data Sensivity

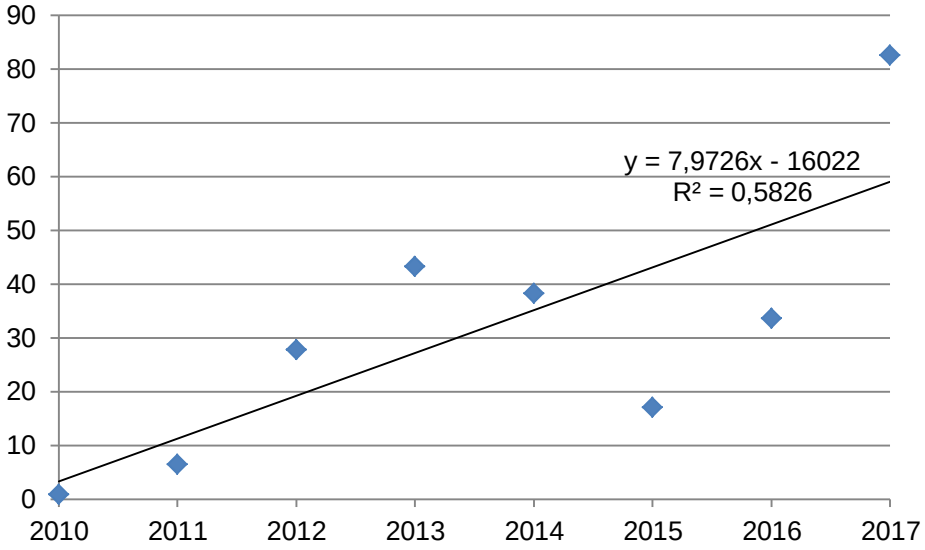
Entity	Alternative name	Year	Organisation	No of Records Stolen
Massive American business hack	7-Eleven, JC Penney, Hannaford, Heartland, JetBlue, Dow Jones, Euronet, Visa Jordan, Global Payment, Diners Singapore and Ingenicard	2012	financial	160000000
Equifax		2017	financial	143000000
Securus Technologies	Prison phone service provider	2015	web	70000000
Philippines' Commission on Elections	COMELEC	2016	government	55000000
Adobe		2013	tech	36000000
US Office of Personnel Management (2nd Breach)		2015	government	21500000
Korea Credit Bureau		2014	financial	20000000
Mossack Fonseca	Panamanian law firm	2016	legal	11500000
Premera	US healthcare provider	2015	healthcare	11000000
ClixSense		2017	web	6600000
VTech	Toymaker company	2015	web	6400000
Swedish Transport Agency		2017	government	3000000
Three Iranian banks	Saderat, Eghtesad Novin, & Saman	2012	financial	3000000
CarPhone Warehouse	UK mobile phone supplier	2015	web	2700000
HSBC Turkey		2014	financial	2700000
UK Ministry of Defence		2008	government	1700000
National Security Agency		2013	government	1500000
South Shore Hospital, Massachusetts		2010	healthcare	800000
Australian Immigration Department		2015	government	500000
Hacking Team		2015	web	500000
Embassy Cables	Confidential communications between 274 embassies in countries throughout the world and the State Department in Washington DC, between 1966-2010.	2010	government	300000
US Military	Wikileaks / Bradley Manning/Cablegate.	2010	military	300000
Wonga		2017	financial	270000
Massachusetts Government	Massachusetts Executive Office of Labor and Workforce	2011	government	200000
Mutuelle Generale de la Police	French police health insurance	2016	healthcare	112000
Invest Bank	United Arab Emirates bank	2015	financial	40000

Fonte: World's Biggest Data Breaches - DataBreaches.net, IdTheftCentre, press reports
(http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/)

Como é possível observar nos dados constantes da tabela 3, uma parte significativa das quebras de segurança registaram-se em entidades financeiras ou governamentais

A evolução da violação de dados registada entre 2010 e 2017 permite identificar uma tendência crescente deste fenómeno, não obstante o valor mais reduzido registado em 2015.

Gráfico 2 – Evolução da violação de dados
(valor médio anual de registos roubados, em milhões)



Fonte: World's Biggest Data Breaches - DataBreaches.net, IdTheftCentre, press reports
(http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/)

Considerando a Cibersegurança de uma perspetiva económica, verificamos que os problemas relacionados com a segurança da informação estão sempre associados, de alguma maneira, a incentivos.

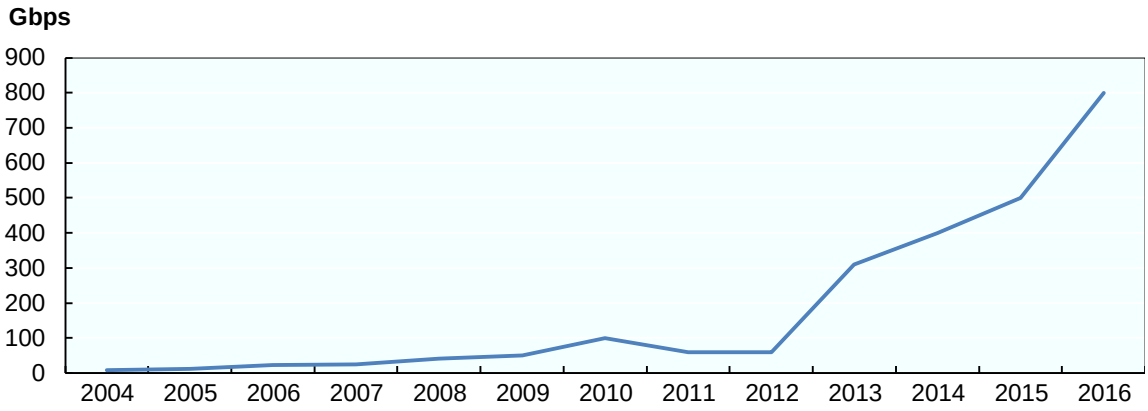
Quando surgiram os primeiros vírus, os utilizadores podiam ter os computadores infectados com riscos para a informação como a eliminação de conteúdo no disco rígido. Com o surgimento dos primeiros antivírus, esta situação passou a ter como consequência uma despesa com este software para proteger os computadores.[23] Mais recentemente, com o surgimento de *malware*, os computadores passaram a ser infectados por estes programas para o envio de spam ou para ataques de DDoS (*distributed denial of service* – negação de serviço [24]).

Segundo a OCDE (2016), "although small businesses are often victims of these so-called denial-of-service attacks, large companies and core digital infrastructure components can also be targeted, as demonstrated by the 2013 massive attack carried out against anti-spam organization Spamhaus. The strength of such attacks has increased over time, using an ever increasing amount of bandwidth. In 2015, several attacks used over 300 Gigabits per second (Gbps) and one peaked at 500 Gbps, which represents a tenfold increase compared to 2009".

[23] "In short, anti-virus software is not foolproof. On February 25, 2005, for example, a critical vulnerability was reported in the anti-virus engine used by Trend Micro's complete product line of client, server, and gateway security products. For that month alone, it was, in fact, the third report of flaws found in recognized security firms' anti-virus software." Schell e Martins (2006)

[24] "A cyber attack in which a cracker bombards a targeted computer with thousands (or more) of fake requests for information, causing the computer to run out of memory and other resources and to either slow down dramatically or to stop. The cracker uses more than one (typically hundreds or thousands) of previously cracked computers connected to the Internet to start the attack. These computers are called "zombies," indicating that they operate under somebody else's control who has evil intentions. The multiple origins of the attack make it difficult to defend against." (Schell e Martin, 2006)
"Denial of service attacks render corporate Websites inaccessible, causing a loss of revenues." (Schell e Martin, 2006)

Gráfico 3 - Evolução da largura de banda usada para os maiores *denial of service attacks*



Gbps = Gigabits per second

Fonte: OECD Digital Economy Outlook 2017 (OCDE, 2017) - http://dx.doi.org/10.1787/888933586464

Esta forma de ataque fez com que o prejuízo deixasse de ser suportado por quem tem o computador, desincentivando a que estes tomem medidas de segurança.

Relativamente aos terminais ATM (*Automated Teller Machines*), novamente se coloca a questão dos incentivos pois a entidade que paga pelos terminais não é a mesma que suporta os custos da fraude – ainda que dentro de uma mesma instituição bancária. Este tipo de fraude tem tido um impacto significativo: segundo a European ATM Security Team, a fraude física nos ATM teve um impacto média de aproximadamente 33 milhões de euros por ano entre 2010 e 2016. Não obstante, também ao nível da fraude informática a ATM, em termos de *Malware*, tem vindo a aumentar o impacto.

Tabela 4 – European Payment Terminal Crime Report Statistics - Summary

Terminal Related Fraud Attacks	H1 2013	H1 2014	H1 2015	H1 2016	H1 2017	% +/- 16/17
Total reported Incidents	12,676	7,345	8,421	10,820	11,934	+10%
Total reported losses	€124m	€132m	€156m	€174m	€124m	-29%%
ATM Related Physical Attacks	H1 2013	H1 2014	H1 2015	H1 2016	H1 2017	% +/- 16/17
Total reported Incidents	1,007	1,032	1,232	1,604	1,696	+6%
Total reported losses	€10m	€13m	€26m	€27m	€12.2m	-55%
ATM Malware & Logical Attacks	H1 2013	H1 2014	H1 2015	H1 2016	H1 2017	% +/- 16/17
Total reported Incidents		20	5	28	114	+307%
Total reported losses			€0.14m	€0.41m	€1.51m	+268%

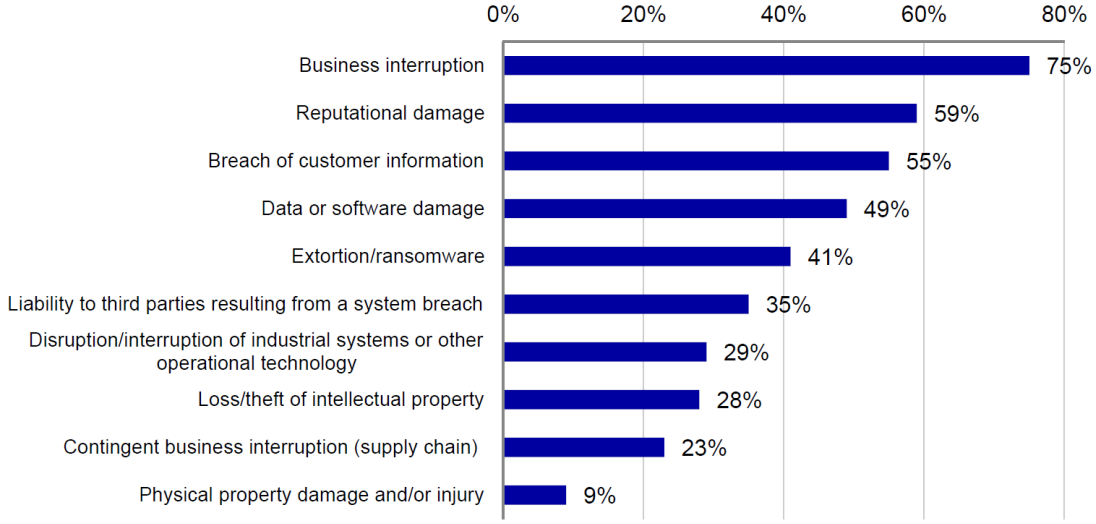
Fonte: European Association for Secure Transactions (EAST)

Outra questão que afecta o combate ao Cibercrime é a sua dimensão. Se não houver a devida articulação entre autoridades, as fraudes na internet podem ter valores relativamente baixos e não serem alvo do devido acompanhamento pelas autoridades policiais. Este é, exactamente, a forma mais eficaz de actuar de quem pratica este tipo de crimes: subtrair pequenas quantias a muita gente. Neste sentido, é perfeitamente justificada a aposta da Comissão Europeia num maior combate ao Cibercrime, nomeadamente através de uma melhor coordenação entre autoridades.

O inquérito sobre a percepção de Ciber-risco realizada a 1.300 executivos pela Marsh e pela Microsoft (Fevereiro de 2018) verificou que o cenário com maior potencial de impacto em termos de perdas está associado à "interrupção do negócio" (75%), seguido do risco de "danos reputacionais" (59%) e da "violação da informação dos clientes" (55%).

Em último lugar, representando uma menos preocupação dos gestores, encontra-se a "danificação e dano de bens físicos" (9%).

Gráfico 4 – Cenários com maior impacto de perda



Fonte: Marsh and Microsoft Cyber perception survey – Cybersecurity - Nordea (2018)

6. O impacto da Cibersegurança

Um incidente de Cibersegurança é qualquer ação não autorizada ou ilegal que envolva computadores (sistemas ou aplicações) ou redes, representando quebras nas medidas de Cibersegurança. As medidas de resposta envolvem o bloqueio do ataque e a reposição do normal funcionamento, bem como a identificação das causas do incidente de forma a prevenir futuros ataques, fraudes e extorsões. Sem uma protecção adequada, poderá ficar em causa a reputação das empresas, o dispêndio de recursos financeiros e o registo de perdas financeiras.

Ao nível dos Cibercrimes, poderão estar em causa crimes como fraude através da manipulação de registros, quebra de controlos de segurança, acesso não autorizado ou modificação do sistema, roubo de propriedade intelectual, pirataria informática, manipulação de mercados (e.g. acções), roubo de identidade, propagação de spam e de *malware*, negação de serviço ou criação e distribuição de pornografia infantil.

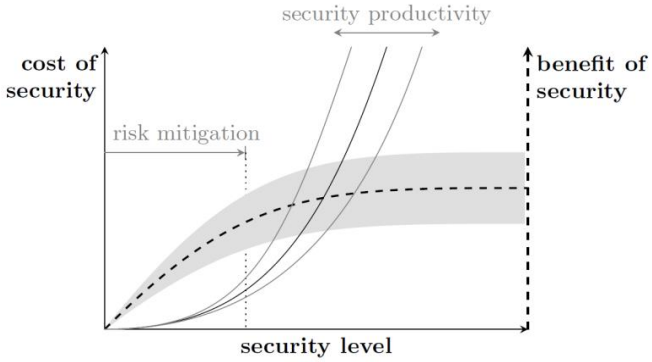
Em termos de impacto da Cibersegurança, importa, antes de mais, conhecer as métricas que devemos ter em conta. Tal como em todas as matérias económicas, os recursos disponíveis para aplicar em Cibersegurança são escassos, em particular em períodos de depressão económica. É essencial para a organizações disporem de métricas que lhes permitam definir estratégias de Cibersegurança.

Para tal, é necessário quantificar os custos e os benefícios dos softwares de segurança, associando sempre que possível os custos aos respectivos benefícios, procurando definir o nível de segurança.

A função de produtividade da segurança indica que para um determinado investimento em segurança obtermos um certo nível de segurança, representada pela linha contínua no gráfico 5 (Böhme, 2010), e indica que à medida que se aumenta o investimento em segurança começa a obter-se cada vez menos aumento no nível de segurança.

Por outro lado, a linha tracejada indica a evolução no benefício de segurança à medida que se aumenta o nível de segurança. O resultado é uma redução cada vez menos no benefício à medida que aumentamos o nível de segurança.

Gráfico 5 - Decomposição da função de produção de segurança em duas etapas



Fonte: Security Metrics and Security Investment Models (Böhme, 2010)

Veremos, de seguida, as 3 variáveis essenciais - custo de segurança, nível de segurança e benefício de segurança – tal como definidas por Böhme (2010).

6.1. Custos de segurança

Os custos de segurança variam conforme o tipo de entidade (e.g. particular, empresa de retalho, instituição financeira ou administração pública) e as necessidades inerentes.

Os custos directos incluem, em geral, a compra e instalação de software antivírus, a formação de funcionários ou a preparação de uma estratégia para resposta a potenciais incidentes. Por outro lado, poderão resultar custos indirectos como por exemplo os custos administrativos decorrentes da necessidade de adicionar complexidade às tarefas para garantir maior segurança do sistema.

Em termos de periodicidade, os custos poderão ser num único momento, como a definição da estratégia de segurança, ou podem ser periódicos, como é o caso da actualização do software antivírus.

Numa outra perspectiva, poderemos considerar custos fixos que são independentes da actividade da instituição (por exemplo a compra de um antivírus) e custos variáveis que em geral terão alguma ligação com a evolução da actividade da mesma (tal como o custo de armazenamento de informação).

Os custos poderão, ainda, ser reversíveis (por exemplo, um equipamento de segurança que pode voltar a ser vendido) ou irreversíveis (como é o caso da despesas com formação na área da segurança).

Naturalmente, os requisitos de segurança e os respectivos custos são proporcionais à sensibilidade da informação.

6.2. Nível de segurança

É importante medir também o nível de segurança, ou seja, de que forma os custos suportados permitem reduzir os riscos que as instituições enfrentam. Este nível de segurança poderá ser medido considerando indicadores determinísticos (os quais consideram, por exemplo, se existem antivírus instalados) ou estocásticos (os quais reflectem o comportamento dos atacantes, por exemplo o número de situações de bloqueio de intrusões).

A complexidade de medir o nível de segurança de uma instituição varia consoante o tipo de organização. Em todo o caso, a análise deverá ter em conta os mesmos factores em qualquer dos casos. Para tal, é necessário definir indicadores que possam ajudar a definir esse nível. O mesmo se passa com a Economia – tentamos criar indicadores que consideramos que podem reflectir diversos aspectos da economia para tentar descrever a realidade. No caso da segurança, interessa encontrar métricas que permitam avaliar as medidas vulnerabilidades.

Podemos identificar 4 tipos de métricas baseadas em:

- Controlos – medem a existência de medidas de segurança,
- Vulnerabilidades – medem como os controlos se comportariam perante uma ameaça hipotética e as suas eventuais vulnerabilidades,
- Incidentes – medem ataques reais,
- Perdas (ocorridas e evitadas) – medem as perdas económicas que os incidentes provocaram e as que foram evitadas[25] pela existência de medidas se Cibersegurança, incluindo custos tangíveis e intangíveis.

A maioria das métricas habitualmente disponíveis são ao nível dos controlos e das vulnerabilidades, por serem mais fáceis de medir) mas raramente ao nível dos incidentes e das perdas. Em todo o caso, estas métricas deverão ser desejavelmente consideradas em conjunto pois nos incidentes as perdas são métricas que resultam de dados históricos, não permitindo conhecer exactamente a evolução no futuro, pelo que é essencial que o foco esteja também nos controlos e nas vulnerabilidades.

Nelson (2015) resume da seguinte forma a situação actual das métricas de Cibersegurança:

- As métricas de Cibersegurança e os processos de reporte ainda se encontram numa fase muito inicial,
- Existem uma tendência para centrar o foco nos controlos (e.g., quantidade de informação que se impediu de ser indevidamente acedida) e não nos riscos,
- A existência de um elevado volume de produtos para segurança tonar a utilização de métricas mais difícil,
- A Cibersegurança passou a ser uma questão central em termos de funções de negócio e não apenas uma questão da área das TICs.

Quando analisamos as questões da Cibersegurança, consideramos o facto de haver ameaças que não se concretizam e seria difícil que uma entidade se dedicasse a combater todas as ameaças previsíveis ao mesmo tempo. Por outro lado, existem ameaças que surgem e que não eram anteriormente conhecidas. Daí a importância das métricas de incidentes, uma vez que permitem direccionar os recursos.

E de que forma esta informação poderá ser utilizada? Conhecendo o número de ataques poderemos calcular uma taxa de incidência, quer ao nível de uma instituição, de um país ou global, e acompanhar essa taxa ao longo do tempo para verificar a evolução do nível de segurança, procurando identificar o comportamento dos atacantes. Naturalmente, esta informação deverá sempre considerar o número de utilizadores em cada rede pois uma rede com mais ataques não significará obrigatoriamente uma rede menos segura pois poderemos estar a considerar uma rede de maior dimensão.

[25] Medir incidentes que não ocorreram é particularmente exigente pois é muito difícil de verificar se ocorrer uma redução dos incidentes devido às medidas de Cibersegurança ou apenas porque houve uma redução nos ataques.

A este respeito, é relevante referir que os sistemas Android e iOS já representam 94% dos sistemas operativos móveis no mercado mundial (Mearian, 2017). O potencial de risco associado a estes sistemas será, como vimos, muito elevado.

Outra questão interessante quando falamos de potencial de risco é o tipo de entidade que garante mais segurança. Conforme refere Greenberg (2012), "users have learned over the last few years that Apple's "walled garden" approach to third party apps isn't quite as protective of their sensitive data as it might sound". Segundo o mesmo autor, é surpreendente que "the popular unauthorized apps outside those walls tend to respect privacy better than the approved ones inside".

6.3. Benefícios de segurança

Interessa, finalmente, medir os benefícios de segurança. De uma forma simples, o nível de segurança permite prevenir incidentes, podendo traduzir-se num benefício de segurança. Podemos estimar os benefícios de segurança considerando perdas que teria ocorrido caso não houvesse medidas de segurança. Não obstante, é difícil identificar estes potenciais incidentes pois a redução nas perdas poderá resultar do comportamento dos "atacantes" e não das medidas de segurança implementadas. A dificuldade em medir as perdas levanta questões quanto às medidas correctas a implementar.

É essencial comparar o custo de um investimento em Cibersegurança com os seus benefícios. De facto, não sendo possível garantir uma segurança total, o importante é definir qual o montante ideal a gastar em segurança.

Em geral, interessará uma estratégia em que os benefícios superem os custos. Uma das métricas habitualmente utilizadas é a rentabilidade do investimento em segurança (ROSI – *Return on Security Investment*):

$$ROSI = \frac{benefit\ of\ security - cost\ of\ security}{cost\ of\ security}$$

Um valor superior indicará um investimento em segurança mais eficiente.

Gordon e Loeb (2002) apresentam um modelo económico para determinar o investimento ideal para proteger um determinado conjunto de informação considerando a vulnerabilidade da informação a uma quebra de segurança e o custo potencial dessa perda [26]. Segundo os autores, o investimento não se deve concentrar nos conjuntos de informação com maior vulnerabilidade pois podem ser excessivamente caros de proteger. Os autores defendem ainda que as empresas devem gastar apenas uma pequena fracção da perda esperada no caso de uma violação para maximizar o benefício esperado do investimento [27].

Novamente considerando o artigo de Böhme (2010), é interessante notar que os investimentos em Cibersegurança apresenta benefícios marginais decrescentes, isto é, cada euro adicional gasto resulta num benefício proporcionalmente inferior.

[26] "We demonstrate that under certain sets of assumptions concerning the relationship between vulnerability and the marginal productivity of the security investment, the optimal investment in information security may either be strictly increasing or first increase and then decrease as vulnerability increases. Thus, under plausible assumptions, investment in information security may well be justified only for a midrange of information vulnerabilities. That is, little or no information security is economically justified for extremely high, as well as extremely low, levels of vulnerability." (Gordon e Loeb, 2002)

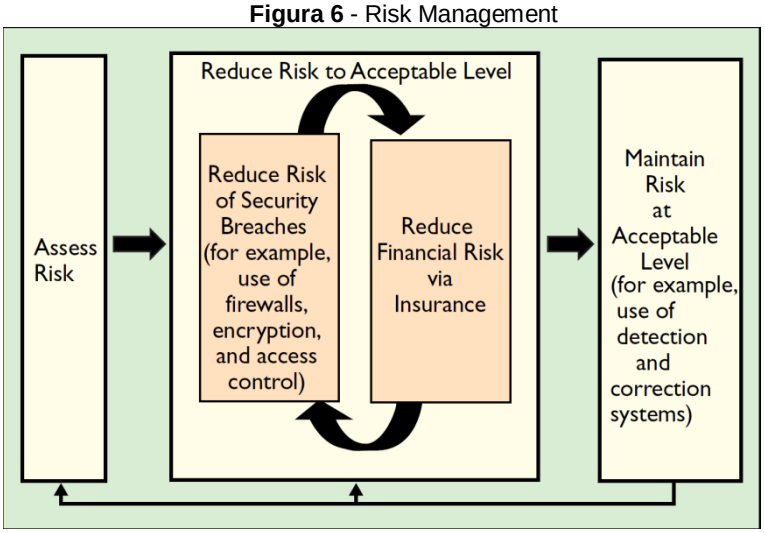
[27] "Furthermore, for two broad classes of security breach probability functions, the optimal amount to invest in information security should not exceed 37% (≈1/e) of the expected loss due to a security breach." (Gordon e Loeb, 2002)

7. Gestão do Risco de Segurança da Informação

A gestão do risco associado à segurança da informação é, segundo Gordon, Loeb e Sohail (2013a), o processo de avaliar os riscos, tomar medidas para reduzir o risco a um nível aceitável e manter esse nível de risco. Segundo os referidos autores, a gestão do risco desenvolve-se em 3 fases (figura 6):

- Numa primeira fase, as organizações deverão identificar as ameaças e vulnerabilidades dos seus sistemas de informação;
- Numa segunda fase, as organizações deverão identificar a informação vulnerável que deverá ser alvo de medidas de segurança, procurando reduzir o risco para níveis que sejam considerados aceitáveis:
    - Investindo em proteção contra o risco de ataque (por exemplo através da instalação de *firewalls*, criptografia e técnicas de controlo do acesso.
    - Adquirindo seguros contra Ciberataques, apesar de ainda haver um longo caminho a percorrer na implementação deste tipo de instrumentos [28], enquanto forma de reduzir o risco de perdas financeiras em caso de ataque [29],
    - O risco que mesmo assim permaneça, não obstante o investimento em protecção e em seguros, deverá ser o já referido "nível de risco aceitável", isto é, um valor de risco residual;
- Atingido o nível de risco aceitável é necessário manter esse nível, pelo que as organizações deverão proceder à monitorização contínua do estado dos seus sistemas de informação, bem como investir em sistemas de detecção de ataques e criar planos de contingência para fazer face a ataques. Naturalmente, o nível de risco aceitável poderá variar consoante o sector de actividade, a idade ou a dimensão da empresa.

Figura 6 - Risk Management



Fonte: Gordon, Loeb e Sohail (2013a)

[28] O mercado de Ciber-seguros ainda se encontra numa fase muito incipiente, em grande parte porque as empresas de seguros têm dificuldade em identificar o nível de segurança dos seus clientes, ficando assim impedidas de calcular o grau de risco. Adicionalmente, o Ciber-risco apresenta um risco acrescido, o do efeito sistémico, uma vez que os incidentes num *software* têm rapidamente um impacto generalizado em todos os utilizadores desse software, torando o risco dos Ciber-seguros muito elevados para as empresas seguradoras. Por estes factos, os prémios deste tipo de seguros são ainda muito elevados.

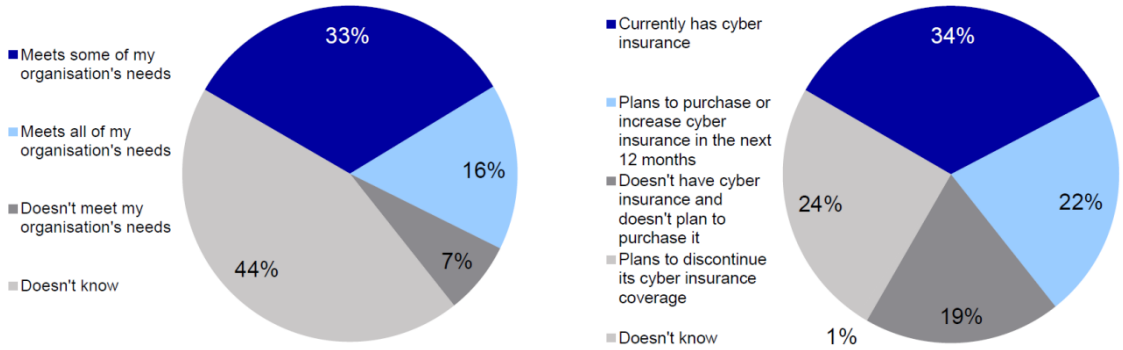
[29] Quanto maior for o nível de segurança, menor deverá ser o valor investido em seguros – e vice-versa.

Segundo a World Economic Forum e o The Boston Consulting Group (2018), ainda que as seguradoras incentivem uma mitigação adequada do risco de Cibersegurança, a sua actividade deve ser cuidadosamente monitorizada relativamente ao aumento do risco financeiro associado à cobertura de custos com Ciberataques, tendo em conta o aumento da dimensão do passivo assumido pelas seguradoras que garantem riscos de Cibersegurança.

Adicionalmente, a juntar ao estado ainda incipiente do sector segurador tradicional ao nível de produtor dirigidos à economia digital, há que considerar também a entrada das gigantes tecnológicas no sector segurador. Segundo o World Insurance Report 2018 (Capgemini e Efma, 2018), cerca de 30% dos clientes estão dispostos a comprar seguros a gigantes tecnológicas como a Amazon ou a Google. Sendo uma ameaça para as empresas tradicionais de seguros, o relatório sugere que estas se deverão adaptar às novas tecnologias para que possam competir com as "*BigTechs*", sem descurar, como é óbvio, a necessária avaliação de risco.

O inquérito ao Ciber-risco realizado pela Marsh e pela Microsoft (Fevereiro de 2018) a 1.300 executivos verificou que o sector de seguros está a começar a responder à crescente necessidade de protecção contra riscos financeiros por incidentes cibernéticos, com quase 50% dos entrevistados a considerar que dão resposta à totalidade ou a parte das suas necessidades. Relativamente à situação real das empresas em termos de utilização de Ciber-seguros, apenas 34% dos entrevistados afirmam ter este tipo de seguros (gráfico 6).

Gráfico 6 – Ciber-seguros – Seguros disponíveis e Seguros contratados



Fonte: Marsh and Microsoft Cyber perception survey – Cybersecurity - Nordea (2018)

Relativamente ao nível de risco aceitável, convém referir que não deverá ser aceite qualquer nível de risco que ponha em causa a protecção de dados em instituições que lidem com informação pessoal, enquadrável nos termos do Regulamento Geral de Protecção de Dados (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016).

Finalmente, uma instituição poderá sempre tentar evitar o risco adaptando a sua estratégia, por exemplo limitando a sua actividade acima de determinados montantes ou em países com maior risco.

8. Estratégias de Segurança e Gestão do Risco

Tal como referem Moore e Anderson (2011), os sistemas de informação tendem a falhar quando a pessoa que é responsável pela sua segurança não é a mesma que sofre quando a protecção falha[30]. De facto, os fornecedores de *software* e de venda de produtos e serviços online têm pouco incentivo a investir em Cibersegurança uma fez que as consequências de um ataque por *hackers* são reduzidas. Da parte do consumidor, também há pouco estímulo para apostar em segurança porque muitas vezes desconhecem o alcance dos problemas de segurança. Esse facto também leva a que não exijam maior segurança aos fornecedores. Acresce o facto de ser difícil distinguir o que é seguro e o que não é [31].

Por outro lado, esta situação é semelhante ao "mercado de limões" descrito por Akerlof (1970): os utilizadores menos informados não são capazes de distinguir quais são os dispositivos/sistemas que são seguros ou não. De facto, a maioria dos utilizadores não está preocupada porque não compreende exactamente o porquê de dever ser uma preocupação. Ao não haver essa percepção por parte dos utilizadores também não há estímulo para que os fornecedores invistam em segurança. É, por isso, essencial garantir a exigência de standards de segurança.

No que respeita às estratégias de segurança e gestão do risco, convém antes de mais recordar que Portugal assinou em junho de 2016 a declaração de Cancún sobre "*Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity*" (OCDE, 2017).

A declaração reflete um empenho dos vários países subscritores em promover o investimento nas tecnologias digitais e no capital baseado no conhecimento, a inovação digital, a livre circulação de informação enquanto catalisador da inovação, a banda larga, o comércio eletrónico e a IoT (*Internet of Things*).

No que respeita à economia digital, a declaração foca-se na importância de promover a criação de emprego no âmbito das novas plataformas online e a formação dos cidadãos com competências que permitam a integração nas novas tecnologias.

Estas apostas vêm, no entanto, acompanhadas por preocupações ao nível da confiança dos consumidores, pelo que se identifica como área fundamental a promoção da segurança digital e a proteção da privacidade, através da implementação de práticas de segurança digital da gestão do risco de privacidade.

A este respeito, Friedman e Resnick (1998) referem que "in systems where identities are easy to create, new identities are not trusted". Esta afirmação é reflexo da importância das boas práticas de segurança digital como forma de assegurar os dados pessoais.

Ao nível das 50 maiores empresas de Cibersegurança, é interessante observar que a grande maioria tem sede nos Estados Unidos da América e muito poucas na área da União Europeia.

[30] "Information systems are prone to fail when the person responsible for protecting a system is not the one who suffers when it fails" (Moore e Anderson, 2011)

[31] "But the difficulty of distinguishing good quality from bad is inherent in the business world; this may indeed explain many economic institutions and may in fact be one of the more important aspects of uncertainty." (Akerlof, 1970)

Tabela 5 - 50 maiores empresas de Cibersegurança em todo o mundo

Company name	Market cap, USDm	Revenue, USDm	Headquarters	Description
Level 3	19451	8172	Broomfield, USA	Network & Managed Security Services
Check Point Software	17592	1730	Tel Aviv, Israel	Unified Threat Management
Palo Alto Networks	17314	1762	Santa Clara, USA	Threat Detection & Prevention
Symantec	17310	4019	Mountain View, USA	Endpoint, Cloud & Mobile Security
Splunk	15166	950	San Francisco, USA	Big Data Security
ZixCorp	11699	1165	Dallas, USA	Email Encryption & Data Protection
Fortinet	9147	1495	Sunnyvale, USA	Enterprise Security Solutions
F5	9121	2090	Seattle, USA	Cloud & Data Center Security
Juniper Networks	9085	5027	Sunnyvale, USA	Threat Intelligence & Network Security
Varonis	7818	1131	New York City, USA	Data Security & Analytics
Qihoo 360	7812	1805	Beijing, China	Internet & Mobile Security
BlackBerry	6908	1297	Waterloo, Canada	Mobile & Data Security
Proofpoint	6007	515	Sunnyvale, USA	Security-as-a-Service
Gemalto	5519	3350	Meudon Cedex, France	Digital Identity Management
FireEye	3445	751	Milpitas, USA	Advanced Threat Protection
Sophos	3440	508	Abingdon, UK	Anti-Virus & Malware Protection
Qualys	3030	231	Redwood City, USA	Cloud Security & Compliance
VeriSign	2628	1062	Reston, USA	Internet Security Solutions
LifeLock	2259	587	Tempe, USA	Identity Theft Detection
Mimecast	2236	187	Watertown, USA	Email Security
CyberArk	1771	217	Petach-Tikva, Israel	Cyber Threat Protection
VASCO Data Security	1639	217	Marlborough, USA	Authentication & e-Signature Solutions
Ixia	1635	485	Calabasas, USA	Network Visibility, Security & Testing
Imperva	1619	322	Redwood Shores, USA	Data & Applications Security
Barracuda Networks	1478	353	Campbell, USA	Email & Web Security Appliances
Infoblox	1471	358	Santa Clara, USA	Automated Network Control & Security
Gigamon	1437	311	Milpitas, USA	Data Center & Cloud Security
Rapid7	1256	157	Boston, USA	Security Data & Analytics Solution
Radware	932	195	Tel Aviv Israel	Application Security & Delivery
NCC Group	807	316	Manchester, UK	Information Assurance Services
AhnLab	755	118	Gyeonggi-do, South Korea	Internet Security Solutions
F-Secure	717	167	Helsinki, Finland	Internet Security for All Devices
Verint	528	192	Melville, USA	Security Intelligence & Compliance
Digital Arts	521	45	Tokyo, Japan	Web & Email Filtering Software
Imprivata	493	119	Lexington, USA	Security for Healthcare Providers
A10 Networks	467	230	San Jose, USA	DDoS Cyber Attack Protection
MobileIron	466	164	Mountain View, USA	Mobile Device & App Security
KEYW	386	288	Hanover, USA	Cyber Defense & Digital Forensics
Fingerprint Cards AB	376	731	Gothenburg, Sweden	Fingerprint Biometrics
Mitek	295	45	San Diego, USA	Mobile Identity Verification
FFRI, Inc.	274	13	Tokyo, Japan	Cybersecurity R&D
Guidance Software	236	111	Pasadena, USA	Endpoint Data Security
Absolute	209	93	Austin, USA	Endpoint Visibility & Control
INSIDE Secure	146	48	Aix-en-Provence, France	Smartphone & Mobile Device Security
SecureWorks	109	430	Atlanta, USA	Managed Security Services
CYREN	107	31	McLean, USA	Web, Email & Mobile Security
SSH Communications	103	19	Helsinki, Finland	Privileged Access Control
Finjan Holdings	86	18	East Palo Alto, USA	Cybersecurity IP Licensing
Globalscape	76	33	San Antonio, USA	Secure File Transfer
Precise Biometrics AB	61	11	Lund, Sweden	Mobile Identity Authentication

Fonte: Cybersecurity Ventures and Thomson Reuters - Cybersecurity - Nordea On Your Mind (2018)

9. As falhas de mercado

As falhas de mercado ocorrem quando os recursos não são alocados de forma eficiente. Neste estudo, abordaremos exemplos destas falhas de mercado e a sua aplicação às questões da Economia Digital e da Cibersegurança.

Segundo Anderson (2006), "many perverse aspects of information security that had long been known to practitioners but were dismissed as "bad weather" have turned out to be quite explicable in terms of the incentives facing individuals and organizations, and in terms of different kinds of market failure". Anderson et al. (2008) referem que "market failures are involved in every step of the cyber crime process, and many of them have implications for the Single Market".

As falhas de mercado justificam, por isso, intervenções ao nível da regulação e são importantes para o desenho das políticas públicas. Após analisarmos as falhas de mercado veremos de que forma as políticas públicas estão a dar resposta.

9.1. Bens Públicos

Os bens públicos (não confundir com bens do Estado) distinguem-se pelas seguintes características:

- São não-rivais, ou seja, o consumo de um bem por uma pessoa não reduz a quantidade disponível desse bem disponível para outras pessoas;
- São não-exclusivos, isto é, não é possível impedir alguém os consumir.

Kopp et al. (2017) consideram que "access to and the use of the internet is largely non-rival and non-excludable, which are key properties of public goods".

Segundo Böhme (2005), "network security appears to have properties of a public good: Insecure nodes not only risk the sanity of their own systems, but also compromise the security of all users, for instance by spreading worms unintentionally and by irresponsibly tolerating distributed attacks from their computers. Since these public costs are not attributed to the responsible parties, individuals have no incentive to upgrade the security of their systems".

No caso de bens de informação como o software, verifica-se que são não rivais (o facto de alguém utilizar o Microsoft Office não impede que outras pessoas o utilizem também) mas a utilização de mecanismos de segurança pode torna-los exclusivos e, dessa forma, evitar que se comportem como bens públicos.

9.2. Assimetria de Informação

A assimetria de informação ocorrer quando um agente económico detém mais informação do que a contraparte na transacção, podendo resultar em risco moral e em selecção adversa. Um exemplo do risco moral é o caso do utilizador que contrata um seguro e que se passa a agir de forma menos cuidadosa porque sabe que está seguro. Quanto à selecção adversa, pode considerar-se, por exemplo, a maior probabilidade de um tomador de um seguro ser o utilizador tem menos investimento em segurança e que por isso subscreve o seguro para precaver.

Akerlof (1970), no *paper* "*The Market for "Lemons*"[32]", analisa a relação entre qualidade e informação e as implicações que têm no funcionamento dos mercados. Quando alguém compra um carro novo, dificilmente sabe se será um carro bom ou um "*lemon*", apenas que existe uma determinada probabilidade de o carro ser um "*lemon*". Ao fim de algum tempo, o comprador formará uma ideia da qualidade do carro e atribui uma nova probabilidade de ser um "*lemon*" que será mais exacta que a inicial. Neste caso, surge uma assimetria na informação: o vendedor tem uma maior noção da qualidade do carro que o comprador. Ainda assim, os carros bons e os "*lemons*" continuarão a ser vendidos ao mesmo preço pois o comprador não conseguirá distinguir um do outro. Por exemplo, se existirem no mercado o mesmo número de carros bons e "*lemons*" e se os carros bons valerem 4.000€ e os "*lemons*" valerem 2.000€, então o preço dos carros deverá ser 3.000€. No entanto, por este preço os vendedores de carros bons não estarão disponíveis para vender por esse preço e os vendedores de má mercadoria serão atraídos para o mercado levando o preço para os 2.000€. O facto de haver um período de garantia permite mitigar o problema pois os vendedores dos "lemons" terão que suportar custos superiores.

O problema da assimetria da informação também afecta o mercado de antivírus. Uma empresa que produza um antivírus tem duas opções: desenvolver um software dispendioso ou gastar o dinheiro no marketing. Naturalmente que devido à assimetria de informação esta segunda opção é mais apetecível, até porque, mais uma vez, apenas o vendedor sabe a real qualidade do produto que vende. Adicionalmente, como o comprador não tem como saber se o antivírus é eficaz não aceita pagar um preço elevado por um produto sobre o qual não consegue aferir a qualidade. Existe o risco de o vendedor se focar mais em características que possam ser observadas tais como a rapidez, a clareza do funcionamento ou o design, em prejuízo da segurança.

Também no caso da segurança dos dados pessoais, dificilmente a segurança é demonstrável – mais facilmente se identificam as quebras de segurança.

Em qualquer dos casos, as falhas na garantia de segurança serão sempre o melhor incentivo para que as empresas invistam na segurança pois as perdas reputacionais podem ser consideráveis. Aliás, esta é a principal razão pela qual as empresas evitam comunicar incidentes. E se as empresas não comunicam as perdas que têm, dificilmente outras empresas terão a noção das potenciais perdas em caso de sofrerem um incidente, o que constitui uma assimetria de informação entre as empresas.

A falta de informação sobre incidentes anteriores impede não só que se analisem possíveis medidas para futuro mas também que se estime qual foi a eficácia do investimento em medidas de segurança. Neste sentido, se essa comunicação for uma obrigação maiores garantias haverá de que as empresas procedem em conformidade.

Os antivírus também têm vindo a desactualizar muito rapidamente pois existe uma grande indústria associada ao desenvolvimento de *malware* que está constantemente a desenvolver novas ameaças – os antivírus vão actualizando mas imediatamente as ameaças vão mudando, desenvolvendo vírus que não são detectados pelos antivírus existentes. A vulnerabilidade surge exactamente quando o utilizador ainda não tem a defesa necessária para fazer face a um ataque novo, pelo que neste caso se destaca a importância de o cliente sinalizar a nova ameaça.

A forma como o mercado muitas vezes enfrenta o problema da assimetria de informação é através de sinais que possam indiciar um determinado tipo de comerciante.

[32] "There are good cars and bad cars (which in America are known as "lemons")" (Akerlof, 1970)

A certificação do comerciante também é uma possibilidade. Mas vejamos, por exemplo, o caso dos cartões de multibanco duplicados. Na verdade, o esquema é possível ainda que os operadores tivessem certificado os equipamentos – na verdade, os meliantes utilizavam um equipamento sobre o equipamento verdadeiro sem que a pessoa que estava a realizar se apercebesse.

Finalmente, Kopp et al. (2017) consideram que "cyber insurance can help arrive at a more efficient allocation of risks as it is a potential solution to the problem of information asymmetries".

9.3. Externalidades

Em Economia, consideram-se externalidades os efeitos colaterais (positivos ou negativos) sofridos por pessoas que não participaram da decisão que os originou.

No caso de uma externalidade positiva, é considerada uma falha de mercado porque o vendedor não tem a percepção de todo o benefício gerado pelo produto e subvaloriza o produto. No caso da Cibersegurança, a aquisição de software de segurança gera externalidades positivas ao reduzir o risco de terceiros.

Quanto a uma externalidade negativa ao nível da segurança da informação, vejamos o exemplo *botnets* que descrevemos anteriormente. Os computadores infectado não têm incentivo a investir em segurança pois são computadores terceiros que irão sofrer as consequências negativas. De facto, os *botnets* são utilizados para infectar outros computadores ou enviar spam, entre outros. Desta forma, a acção de utilizador num computador tem efeitos negativos noutros computadores.

Conforme questiona Varian (2000), "if a particular user's computer is taken over, should he have liability for the cost of the attack on someone else?". A preocupação dos utilizadores individuais tende a ser com a sua própria segurança e não com a segurança de terceiro. Ainda assim, este comportamento também acaba por ter reflexos na segurança informática de terceiros.

Como consequências destas externalidades podemos enfrentar um menor investimento em Cibersegurança (no primeiro caso) e uma maior disseminação de *malware* (no segundo caso).

9.4. Outras falhas de mercado

A falta de diversidade em termos de plataformas e de redes aumenta o impacto dos Ciberataques que são bem-sucedidos pois as falhas de segurança são comuns. Esta questão levanta grandes dificuldades aos Ciberseguros pois, apesar de serem a forma mais adequada para partilhar os riscos, neste cenário verifica-se uma grande probabilidade de efeitos sistémicos em larga escala.

Finalmente, a fragmentação das legislações nacionais dos países a nível mundial dificultam a rapidez na acção em caso de Ciberataques, a prevenção de Ciberataques. Para fazer face a este constrangimento, é essencial que os países coordenem legislação ao nível da Cibersegurança e do Cibercrime e que apostem na cooperação entre si (tal como tem sido feito, por exemplo, ao nível da EU).

10. Notas finais

Segundo o World Economic Forum, estima-se que em 2017 tenham ocorrido perdas financeiras a pessoas e empresas de mais de 500 mil milhões de euros em todo o mundo em resultado de ataques informáticos. Este valor será superior pois muitas empresas não comunicam esta informação para evitar dar a conhecer a sua vulnerabilidade e para impedir que tenha um impacto negativo na sua credibilidade e confiabilidade.

Ataques informáticos como o *Wannacry* ou o *Petya* (ambos em 2017) trouxeram para a agenda mediática a questão da Cibersegurança. Embora não tenham sido os mais graves, foram os mais mediáticos e deixaram como certa a possibilidade de ocorrerem novos ataques no futuro.

No actual estado de evolução da Economia Digital, é totalmente relevante abordar a questão da Cibersegurança na perspetiva Económica e das Políticas Públicas. Na verdade, a existência de um mercado digital tem diversas semelhanças em termos de funcionamento face aos mercados tradicionais, embora com especificidades que por vezes colocam questões difíceis às Políticas Públicas [33].

Como pudemos ver, muitas questões que põem em causa a Cibersegurança resultam de falhas de mercado. Relativamente à assimetria, destaca-se a importância de os Governos publicarem ou obrigarem as instituições a publicar informação relativa a Ciberataques com base em critérios objectivos. Quanto às externalidades, salienta-se que a adopção de legislação pode ajudar a resolver algumas situações de externalidades embora, em geral, demorem a produzir efeitos - os processos legislativos tendem a ser mais lentos que a evolução tecnológica. Por outro lado, é importante a responsabilização efectiva dos cidadãos e das empresas pelas actividades *online*, ou seja, que quem é responsável por uma determinada acção sofra consequências e que não se torne apenas uma externalidade negativa sobre terceiros. A preocupação dos "*providers*" com a segurança será tanto maior quanto mais tiverem a perder com as falhas de segurança [34].

Relativamente ao Estado, salienta-se a necessidade de existir uma estratégia e um conjunto de políticas públicas que permitam garantir a Cibersegurança, tendo em conta, em particular, a necessidade de cooperação com outros países nesta matéria. Outra das áreas em que o Estado pode intervir, além da tentativa de identificar e impedir possíveis Ciberataques, é na sensibilização dos cidadãos para as questões da Cibersegurança e da Privacidade, dando-lhes informação sobre as consequências das suas actividades *online*, ajudando a reduzir vulnerabilidades a ataques

Quanto às empresas, a grande questão é saber se existe estímulo suficiente para que invistam em Cibersegurança, isto é, se têm percepção das potenciais perdas financeiras que poderão resultar de Ciberataques. Adicionalmente, na ausência de medidas de sensibilização por parte do Estado, o papel de defesa parece estar mais do lado das empresas (e dos cidadãos).

[33] "As Europe moves online, information security is becoming increasingly important: first, because the direct and indirect losses are now economically significant; and second, because growing public concerns about information security hinder the development of both markets and public services. While information security touches on many subjects from mathematics through law to psychology, some of the most useful tools for both the policy analyst and the systems engineer come from economics." Anderson et al. (2008a)

[34] "But security analysts should go one step further and examine the incentives of those responsible for the system. Such an analysis could be used to assign liability so that those who are best positioned to control the risks have appropriate incentives to do so." - New York Times; New York, N.Y.; Jun 1, 2000; Hal R. Varian

Ainda assim, da parte das empresas ainda parece não se verificar uma aposta forte na Cibersegurança. Muitas empresas ainda optam pela internalização desta função, por não considerarem uma área prioritária, o que poderá ser explicado pelo facto de o tecido empresarial ser constituído na sua grande maioria por PMEs, com menos capacidade financeira para fazer face às necessidades de uma política de Cibersegurança eficaz. Neste sentido, é importante que as políticas públicas possam dar os estímulos adequados para que as empresas invistam nesta área.

Tal como foi referido, é importante que as empresas estimem o valor da informação e da sua reputação para que possam decidir quanto deverão investir na Cibersegurança. O custo com a Cibersegurança deve ser considerado como um investimento da imagem da empresa, uma vez que uma empresa segura é mais atractiva não só aos olhos dos clientes mas também dos fornecedores

A capacitação dos trabalhadores das empresas nas questões digitais também poderá impedir que ocorram ataques informáticos pelo que é importante ter recursos humanos cada vez mais preparados.

A alternativa para as quebras de segurança passa também pelos seguros de risco [35]. No entanto, uma seguradora tenderá a assegurar clientes com um risco mais controlado, ou seja, que investiram em medidas de segurança informática. Por outro lado, a promoção de um mercado de Ciberseguros para gestão dos riscos de Cibersegurança, face à dimensão do Ciberespaço, apenas é possível através de uma estratégia concertada a nível global.

Finalmente, é muito difícil impedir que ocorram ataques informáticos, mas é possível que do estudo dos ataques ocorridos se retire aprendizagem que permita melhorar a Cibersegurança e a prevenção de novos Ciberataques.

Referências

Akerlof, George (1970). “The Market for "Lemons": Quality Uncertainty and the Market Mechanism”. The Quarterly Journal of Economics, Vol. 84, No. 3.

AMROP (2017). “Digitization on Boards Report | 2nd Edition - Are Boards Ready for Digital Disruption?”. Leadership Study.

Anderson, Ross (1993). “Why Cryptosystems Fail”. University of Cambridge.

Anderson, Ross; Moore, Tyler (2006). “The Economics of Information Security”. Science, Vol. 314, October 2006.

Anderson, Ross; Böhme, Rainer; Clayton, Richard; Moore, Tyler (2008a). “Security Economics and European Policy”.

Anderson, Ross; Böhme, Rainer; Clayton, Richard; Moore, Tyler (2008b). “Security Economics and The Internal Market”. Study commissioned by ENISA.

Böhme, Rainer (2005). “Cyber-Insurance Revisited”. Workshop on the Economics of Information Security (WEIS), Kennedy School of Government, Cambridge.

Capgemini e Efma (2018). “World Insurance Report 2018”.

[35] “an insurer against computer crime will give you a reduced rate if you install security patches within two weeks of their posting, provide continuing education for security staff and engage in other good risk management practices” - New York Times; New York, N.Y.; Jun 1, 2000; Hal R. Varian

Comissão Europeia (2015). "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security".

Cyberwiser (2017). "Wide-Impact Cyber Security Risk framework - Portugal". Consultado em 30 de junho de 2018 em https://cyberwiser.eu/portugal-pt.

EastWest Institute (2016). "Purchasing Secure ICT Products and Services: A Buyers Guide". Global Cooperation in Cyberspace Initiative.

EdX/Delft (2017). "Cyber Security Economics".

European Network and Information Security Agency (2014). "ENISA Threat Landscape 2014".

European Network and Information Security Agency (2016). "ENISA Threat Landscape 2015".

European Network and Information Security Agency (2017). "ENISA Threat Landscape 2016".

European Network and Information Security Agency (2018). "ENISA Threat Landscape 2017".

Friedman, R.; Resnick; M. (1998). "The Social Cost of Cheap Pseudonyms". Journal of Economics and Management Strategy, Vol. 10.

Gordon, Lawrence; Loeb, Martin (2002). "The Economics of Information Security Investment". ACM Transactions on Information and System Security, Vol. 5, No. 4, November 2002.

Gordon, Lawrence; Loeb, Martin; Sohail, Tashfeen (2003a). "A Framework for Using Insurance for Cyber-Risk Management". Communications of the ACM, March 2003, Vol. 46, No. 3.

Greenberg, Andy (2012). "Unauthorized iPhone And iPad Apps Leak Private Data Less Often Than Approved Ones". Forbes.

Horak, Ray (2008). "Webster's New World Telecom Dictionary". Wiley Publishing.

Kissel, Richard (Ed.) (2013). "Glossary of Key Information Security Terms". NISTIR - National Institute of Standards and Technology Interagency or Internal Report 7298R2.

Kopp, Emanuel; Kaffenberger, Lincoln; Christopher Wilson (2017). "Cyber Risk, Market Failures, and Financial Stability". International Monetary Fund, Working Paper WP/17/185.

Liebowitz, S.; Margolis, S. (1998). "*Network Externalities (Effects)*". The New Palgrave's Dictionary of Economics and the Law (http://www.utdallas.edu/~liebowit/palgrave/network.html).

Mearian, Lucas (2017). "Android vs iOS security: Which is better?". Computerworld.

Microsoft (2017). "Microsoft Security Intelligence Report – Portugal". Volume 22, January through March, 2017 (https://www.microsoft.com/en-us/security/intelligence-report).

Moore, Tyler, & Anderson, Ross (2011). "Economics and Internet Security: A Survey of Recent Analytical, Empirical, and Behavioral Research". Harvard Computer Science Technical Report TR-03-11.

Nelson, Elden (2015). "IT's security metrics and reporting problem: A communication failure". CSO Online.

Nordea (2018). "Cybersecurity - Nordea On Your Mind". Nordea Bank AB (publ).

OCDE (2013). "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value". OECD Digital Economy Papers No. 220, OECD Publishing, Paris.

OCDE (2016). "Managing Digital Security and Privacy Risk". 2016 Ministerial Meeting on the Digital Economy Background Report.

OCDE (2017). "OECD Digital Economy Outlook 2017". OECD Publishing, Paris.

Schell, Bernadette; Martin, Clemens (2006). "Webster's New World Hacker Dictionary". Wiley Publishing.

Shapiro, Carl; Varian, Hal (1998). "Information Rules - A Strategic Guide to the Network Economy". Harvard Business School Press Boston, Massachusetts.

System Security Study Committee (1991). "Why the Security Market has not worked well". "Computers at Risk", Chapter 6, National Research Council.

Varian, Hal (1996). "Economic Aspects of Personal Privacy". University of California - Berkeley School of Information.

Varian, Hal (1998). "Markets for Information Goods". University of California, Berkeley.

Varian, Hal (2000). "Managing Online Security Risks". New York Times, June.

Website Builder Expert (2017). "Which EU Country Is Most Vulnerable To Cybercrime?".

World Economic Forum e The Boston Consulting Group (2018). "Cyber Resilience Playbook for Public-Private Collaboration". Future of Digital Economy and Society System Initiative.