Chapter 4. Cybersecurity and Economic Incentives

The past five years have witnessed the emergence of comprehensive efforts to improve the security of information systems and networks. A recent survey by the OECD (2005a) demonstrates that governments have developed national policy frameworks, as well as partnerships with the private sector and civil society, to combat cybercrime. Measures include Computer Security Incident Response Teams (CSIRTs), raising awareness, information sharing and education.

But improving cybersecurity is not a straightforward problem. Notwithstanding rapidly growing investments in security measures, it has become clear that cybersecurity is a technological arms race that, for the immediate future, no one can win. Take spam, for instance. Several years ago, so-called open e-mail relays were a major source of spam. ISPs and other actors developed measures, such as blacklisting, to collectively combat open relays. By the time adoption of these measures reached a critical mass, spammers had already shifted their tactics. As a result, the significant reduction in the number of open relays had hardly any impact on the amount of spam. The list of such examples goes on and on.

While many would agree that cybersecurity needs to be strengthened, the effectiveness of many security measures is uncertain and contested. Furthermore, security measures may also impede innovation and productivity. Those involved in improving cybersecurity sometimes tend to overlook that the reason why the Internet is so susceptible to security threats – namely its openness – is also the reason why it has enabled an extraordinary wave of innovation and productivity growth.

In the Internet world, the benefits of productivity growth often outweigh the costs of innovation – as in the case of online credit card transactions. From the start of moving their business online, credit card companies have struggled with rising fraud. However, this has not stopped them from expanding their online activities. The benefits of that growth have been consistently higher than the associated costs of the increase in fraud. While growing in absolute terms, the level of online fraud in the United States has been dropping relative to the overall dollar amount of online transactions

(Berner and Carter, 2005). Rather than implementing far-reaching security measures that would restrict the ease of use of their systems, credit card companies have adopted strategies to fight instances of fraud, up to the point where the costs of further reductions in fraud start to exceed the benefits: damages avoided.

All this means that total security is neither achievable nor desirable. In principle, actors need to make their own tradeoffs regarding what kind of security measures they deem appropriate and rational, given their business model. Clearly, business models vary widely for actors in the different niches of the complex ecosystem surrounding information systems and networks – from ISPs at different tiers to software providers of varying applications, to online merchants to public service organisations and to end users. All of these actors experience malware differently, as well as the costs and benefits associated with alternative courses of action. In other words, many instances of what could be conceived as security failures are in fact the outcome of rational economic decisions, reflecting the costs and benefits perceived by the actors during their decision-making timeframe.

What is needed, then, is a better understanding of these costs and benefits from the perspective of individual actors and of society at large. Part II of this report sets out to identify the incentives under which a variety of Internet market participants operate, and to determine whether these incentives adequately reflect the costs and benefits of security for society – *i.e.* whether these incentives generate externalities. To address these issues, the findings are presented of a recent research project on incentives that should help lay the groundwork for future policymaking.

Increased focus on incentive structures

Research in the field of cybersecurity is undergoing a major paradigm shift. More and more researchers are adopting economic approaches to study cybersecurity, shifting emphasis away from technological causes and solutions. Most of this innovative research has yet to find its way into the realm of policy makers, let alone into the policies themselves. While reports like the OECD survey on the culture of security (OECD, 2005a) generally recognise that cybersecurity is more than a technological issue, the proposed measures are still mostly oriented in that direction: developing technological responses and efforts to stimulate their adoption. The technological responses are typically accompanied by legal efforts and intensified law enforcement.

Box 4.1 OECD Guidelines and the Economics of Cybersecurity

In 2002, the OECD released the *Guidelines for the Security of Information Systems and Networks* (OECD, 2002a). A set of nine non-binding guidelines aim to promote "a culture of security" – that is, "a focus on security in the development of information systems and networks, and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks" – among "all participants in the new information society" (see below). The guidelines reflect the shared understanding of OECD member countries as well as a variety of business and consumer organisations.

OECD Guidelines for the Security of Information Systems and Networks

1. Awareness
   Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2. Responsibility
   All participants are responsible for the security of information systems and networks.
3. Response
   Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.
4. Ethics
   Participants should respect the legitimate interests of others.
5. Democracy
   The security of information systems and networks should be compatible with essential values of a democratic society.
6. Risk assessment
   Participants should conduct risk assessments.
7. Security design and implementation
   Participants should incorporate security as an essential element of information systems and networks.
8. Security management
   Participants should adopt a comprehensive approach to security management.
9. Reassessment
   Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

The "culture of security" that the guidelines aim to promote will be influenced by the incentive structures surrounding security tradeoffs. The focus on security may certainly be strengthened, but that in itself does not mean that actors will behave in ways that are beneficial to society. In other words, more attention to security does not equal better security decisions as long as economic incentives are ignored.

Box 4.1 OECD Guidelines and the Economics of Cybersecurity (continued)

Chapter 5 provides a more detailed discussion of why this is the case. For now, it suffices to mention a few examples. Take firms' investment in security measures.. Research has demonstrated that a focus on security may mean actively participating in information sharing with other firms. Under certain conditions, this actually leads to decreased investment levels. Also, a firm taking protective measures may create positive externalities for others – that is, benefits for others that are not reflected in the decision by that firm – which may reduce their investments to a level that is below the social optimum.

Another example is the manufacturing of software. According to the *OECD Guidelines* (OECD, 2002b), "Suppliers of services and products should bring to market secure services and products." Even if it was clear what the term "secure software" means, many software markets do not reward such behaviour. Rather, they reward first movers – that is, those companies that are first in bringing a new product to market. This means it is more important to get to the market early, rather than first investing in better security. A final example relates to end-users. The *Guidelines* argue that end users are responsible for their own system. In the case of malware, however, this responsibility may lead to security tradeoffs that are rational for the end users, but have negative effects on others. More and more malware actively seeks to reduce its impact on the infected host, so as not to be detected or removed, using the infected host to attack other systems instead of the host itself.

In short: the development of a "culture of security" is very sensitive to economic incentive structures. Whether such a culture will actually improve overall security performance requires a better understanding of the incentives under which actors operate as well as policies that address those situations in which incentives produce outcomes that are not socially optimal. The research project presented in this Part II of the malware report aims to contribute to this undertaking.

Notwithstanding the necessity of these initiatives, they typically overlook the economic factors affecting cybersecurity – *i.e.* the underlying economic incentive structure. As Anderson and Moore (2006, p. 610) have argued, "over the past 6 years, people have realised that security failure is caused at least as often by bad incentives as by bad design." Many of the problems of information security can be explained more clearly and convincingly using the language of microeconomics: network effects, externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons. Within this literature, designing incentives that stimulate efficient behaviour is critical.

The power that incentive structures can exert on security threats is visible everywhere. Take the distribution of viruses and other malware.

During the second part of the 1990s, when the scale of virus distribution was rapidly increasing and countless end users (home, corporate, governmental) were affected, many ISPs argued that virus protection was the responsibility of the end users themselves. The computer was their property, after all. ISPs further argued that they could not scan the traffic coming through their e-mail servers, because that would invade the privacy of the end user. Mail messages were considered the property of the end users.

About five years ago, this started to change, partly due to the growth of broadband and always-on connections. The distribution of viruses and worms had increased exponentially and now the infrastructure of the ISPs themselves was succumbing to the load, requiring potentially significant investment in network expansion. Facing these potential costs, ISPs radically shifted their position. Within a few years, the majority of them started to scan incoming e-mail traffic, deleting traffic identified as malignant, since this had become a lower-cost solution than infrastructure expansion. *De facto*, ISPs re-interpreted the various property rights associated with e-mail – *e.g.* regarding ownership of the message. Their changed policies have made e-mail based viruses dramatically less effective as an attack strategy.

The economic perspective

An economic perspective on cybersecurity – and malware in particular – presents a potentially fruitful starting point for future policymaking. That's because it leads to a focus on market partcipants' (1) incentive structures and (2) market externalities, or the consequences of inadequate security measures that are borne by other market participants or society in general.

In this chapter and those following, the economic perspective on malware and cybersecurity are examined, building on the innovative research efforts of the past six years (for a brief overview of the existing literature, see Anderson and Moore, 2007; Anderson *et al.,* 2008). It is a first step in this direction, and given the complexity of the problem, more work will undoubtedly be needed.

One promising approach is to complement the existing research with new, qualitative field work. Field research is important because there is limited information in the public domain on how Internet market participants actually make their information-security decisions. And this makes it difficult to calibrate any form of public policy.

Box 4.2 The problem with prevailing research methods

So far, most of the Internet-related economics research has been based on the methods of neo-classical and new-institutional economics. While powerful, these methods are based on rather stringent assumptions about how actors behave – such as their rationality, their security tradeoffs and the kind of information they have – and how they interact with their institutional environment.

Three key limitations of studies founded on these methodological assumptions are:

1. they provide limited insight into how actors actually perceive the cost, benefits and incentives they face;
2. they have difficulty taking into account dynamic and learning effects, such as how a loss of reputation changes the incentives an actor experiences; and
3. they often treat issues of institutional design as rather trivial. That is to say, the literature assumes that its models indicate what market design is optimal, that this design can be brought into existence at will, and that actors will behave according to the model's assumptions.

If the past decade of economic reforms – including privatisation, liberalisation and deregulation – have taught us anything, it is that designing markets is highly complicated and sensitive to the specific context in which the market is to function. It cannot be based on formal theoretical models alone. Institutional design requires an in-depth empirical understanding of current institutional structures and their effects on outcomes. Even with such an understanding, it may not be possible to fully control the setup and working of a market as they are in part emerging from the interaction of multiple actors. However, it should be possible to nudge the system in the desired direction.

Part II presents efforts to: (1) collect evidence on the security tradeoffs faced by Internet market participants; (2) how those participants perceive the incentives under which they operate; (3) which economic decisions these incentives support, and (4) the externalities that arise from these incentive structures. The objective of Part II is to contribute to the debate on the economics of malware from an empirical and analytical perspective. It is not designed to explore and develop detailed policy recommendations.

Chapter 5 reports the findings of the field work. Based on 41 interviews with 57 representatives of Internet market participants, as well as governmental agencies and security experts, we present a variety of incentives faced by Internet Service Providers, e-commerce companies (with a focus on financial service providers), software vendors, domain registrars and end users.

Chapter 6 aggregates the research findings and discusses the externalities that emerge as market participants make incentive-driven security decisions. In some cases, externalities are borne by market participants able to influence the security tradeoffs of those generating the externalities bringing the net market impact closer to the optimum. In other cases, the externalities are simply borne by market participants or by society at large. Part II concludes with a summary of the efficiency and distributional effects of externalities and an overall assessment of the costs of malware.

The annex at the end of Chapter 5 contains a list of the survey participants. Annex B at the end of this report describes the survey in detail.

Glossary of Malware Terms

Authentication factors: Used to obtain access; something the user knows (such as a password); something the user has (such as a credit card or token); or something the user is (a photograph or thumbprint).

Authentication/Authenticity: Being able to prove or verify a person's or entity's identity with a certain level of assurance. Authentication mechanisms are used to provide access control to information systems.

Availability: Ensuring that digital data within an information system and the system itself are available to authorised users.

Backdoors[1]: A backdoor is malicious code that allows unauthorised access to a computer system or network by accepting remote commands from an attacker elsewhere on the Internet.

Bluejacking: Sending unsolicited messages to Bluetooth connected devices.

Bluesnarfing enables unauthorised access to information from a wireless device through a Bluetooth connection.

Bot programme: A type of 'backdoor' programme that allows attackers to remotely control many compromised information systems (often thousands) simultaneously (or individually).

Botnet(s): Group of malware infected computers that can be used to remotely carry out attacks against other computer systems.

Confidentiality: Being able to protect information and data from unauthorised access.

CERTs: Computer emergency response teams.

CSIRTs: Computer security incident response teams.

DDoS: Distributed denial of service attacks.

1. NIST (2005), pp. 2-12.

Digital certificate: A means of authenticating an identity for an entity when doing business or other transactions on the web or on line. Digital certificates exist as part of public key infrastructures (PKI).

Domain name: The identifier or address of any entity on the Internet. Domain Name System (DNS): The way Internet domain names are located and translated into an Internet Protocol, or IP, address. For example, the domain name www.oecd.org is a more user friendly and memorable alternative to the IP address 193.51.65.71.

Honeynet: Two or more honeypots on a network form a honeynet.

Honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorised use of information systems. Generally it consists of a computer, data or a network site that appears to be part of a network but which is actually isolated, (un)protected and monitored, and which seems to contain information or a resource that would be of value to attackers.

Integrity: A primary security goal of information systems which seeks to ensure that the system as a whole (people, data, software) have not been compromised and can continue to be trusted. Internet Protocol The native language of programmatic communication on the Internet.

Keystroke loggers[2] *:* A hidden programme that records and "logs" each key that's pressed on the compromised system's keyboard, as the legitimate user of the system is typing.

Malware payload: The primary function of a piece of malware.

Non-repudiation: A security goal which seeks to prevent a person from denying they undertook an electronic transaction when they did.

Operating system: A computer program that manages the hardware and software on a computer.

Packet: The minimum autonomously-routable quantum of data which can be transmitted across a modern digital "packet switched" network.

Patch/Workaround: A small piece of software code designed to correct or rectify an existing bug or flaw in an operating system or application programme. A work-around is a set of actions that network security managers can take to reduce their exposure to a known software vulnerability.

---

2. Ibid.

Payload: The essential data that is being carried within a packet or other transmission unit. The payload does not include the "overhead" data required to get the packet to its destination.

Rootkit: A set of programmes designed to conceal the compromise of a computer at the most privileged "root" level, by modifying operating system files or inserting code into the memory of running processes.

Social engineering: Techniques designed to fool human beings into providing information or taking an action that leads to a subsequent breach in information systems security.

Spam: Commonly understood to mean bulk, unsolicited, unwanted and potentially harmful electronic messages.[3]

Spoofing is a technique designed to deceive an uninformed person about the origin of, typically, an e-mail or a website.

Spyware: A form of malware that is capable of capturing a range of data from user input (keyboards, mice) and output (screens) and other storage (memory, hard drive etc.) and sending this information to the attacker without the user's permission or knowledge.

Transaction signing: The process of calculating a keyed hash function to generate a unique string that can be used to verify both the authenticity and integrity of an online transaction.

Trojan horses: A computer program that appears legitimate but actually has hidden functionality used to circumvent security measures and carry out attacks.

Virus: Directly analogous to its biological namesake, a virus is hidden code that spreads by infecting another program and inserting a copy of itself into that program.

Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management of software that could be exploited.

Worm: A type of malware that self replicates without the need for a host programme or human interaction.

3. OECD (2006).

Bibliography

A-i3 (2006), Zur Haftung von Phishing-Opfern. *Arbeitsgruppe Identitätsschutz im Internet e.V, www.a-i3.org/content/view/975/230/.*

Anderson, R. (2001), "Why Information Security is Hard: An Economic Perspective", Proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, IEEE Computer Society, *www.acsac.org/2001/papers/110.pdf.*

Anderson, R. (2002), "Unsettling Parallels between Security and the Environment", First Annual Workshop on Economics and Information Security, *www.cl.cam.ac.uk/~rja14/econws/37.txt*.

Anderson, R. (2007), "Closing the Phishing Hole – Fraud, Risk and Nonbanks", *www.cl.cam.ac.uk/~rja14/Papers/nonbanks.pdf*.

Anderson, R. and T. Moore (2006), "The Economics of Information Security", *Science*, 314: 610-613.

Anderson, R. and T. Moore (2007), "Information Security Economics – and Beyond", Computer Laboratory, University of Cambridge, *www.cl.cam.ac.uk/~rja14/Papers/econ_crypto.pdf.*

Anderson, R., *et al.* (2008), "Security Economics and the Internal Market", European Network and Information Security Agency, *www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf.*

APACS (2008), "Fraud abroad pushes up losses on UK cards following two-year fall", press release, *www.apacs.org.uk/2007Fraudfiguresrelease.html*.

APWG (Anti-Phishing Working Group) (2006a), *Phishing Activity Trends Report*, *www.antiphishing.org/reports/apwg_report_april_2007.pdf*, last accessed 14 December 2007.

APWG (2006b), *Phishing Activity Trends Report, www.websense.com/securitylabs/resource/PDF/apwg_report_december_2006.pdf*, last accessed 14 December 2007.

Arbor Networks (2007), *Worldwide Infrastructure Security Report, Volume III*, *www.arbornetworks.com/report*.

August, T. and T. I. Tunca (2006), "Network Software Security and User Incentives, *Management Science*, 52(11): 1703–1720.

AusCERT (2005), "Windows Rootkit, Prevention, Detection and Response", *www.auscert.org.au/*, last accessed 11 December 2007.

AusCERT (2006), "Haxdoor – An anatomy of an online ID theft Trojan", *www.auscert.org.au/render.html?cid=1920*, last accessed 10 December, 2007.

Australian Government, Office of the Privacy Commissioner (2004), *Community Attitudes towards Privacy 2004, www.privacy.gov.au/publications/rcommunity/chap10.html*, last accessed 11 December 2007.

Bangeman, E. (2006), "Court likely to order ICANN to suspend Spamhaus' domain", *Ars Technica*, *http://arstechnica.com/news.ars/post/20061009-7938.html*.

Banktip (2006). "Phishing: Kunden haften für Trojaner", Banktip.de, *www.banktip.de/News/20648/Phishing-Kunden-haften-fuer-Trojaner.html*.

Barnum, S. and M. Gegick (2005), *Economy of Mechanism*, Build Security In, *https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/348.html?branch=1&language=1*.

Bauer, J. M., *et al.* (2008), "Financial Aspects of Network Security: Malware and Spam", International Telecommunication Union, July, *www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf*.

BBC News (2004), "MyDoom virus biggest in months", BBC News website, *http://news.bbc.co.uk/1/hi/technology/3432639.stm*, last accessed 14 December 2007.

BBC News (2007a), "Google searches web's dark side", BBC News website, *http://news.bbc.co.uk/2/hi/technology/6645895.stm*.

BBC News (2007b), "Burgers paid for by mobile phone", BBC News website, *http://news.bbc.co.uk/2/hi/technology/6400217.stm*, last accessed 7 December, 2007.

Becker, G. S. (1968), "Crime and Punishment: An Economic Approach", *The Journal of Political Economy*, 76(2): 169-217.

Becsi, Z. (1999), "Economics and Crime in the States," *Economic Review - Federal Reserve Bank of Atlanta*, 84(1): 38-56, *http://ezproxy.msu.edu:2047/login?url=http://proquest.umi.com/pqdweb?did=40779835&Fmt=7&clientId=3552&RQT=309&VName=PQD*.

Berner, R. and A. Carter (2005), "The truth about credit-card fraud", *Business Week Online*, *www.businessweek.com/technology/content/jun2005/tc20050621_3238_tc024.htm*.

Bernstein, D. J. (2007), "Some thoughts on security after ten years of qmail 1.0", 1st Computer Security Architecture Workshop in conjunction with 14th ACM Conference on Computers and Communication Security, Fairfax, Virginia, *http://cr.yp.to/qmail/qmailsec-20071101.pdf*.

Böhme, R. (2005), "Cyber-Insurance Revisited", Fourth Workshop on the Economics of Information Security, Harvard University, *http://infosecon.net/workshop/pdf/15.pdf*.

Brendler, B. (2007), "Spyware/Malware Impact on Consumers"; APEC-OECD Malware Workshop, StopBadware Project, April, *www.oecd.org/dataoecd/33/55/38652920.pdf*, last accessed 13 December 2007.

Camp, L. J. (2006), *Mental Models of Privacy and Security*, *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=922735*.

Camp, L. J. and C. Wolfram (2004), *Pricing Security: Vulnerability as Externalities*, *http://ssrn.com/abstract=894966*.

Campbell, K., *et al*. (2003), "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", *Journal of Computer Security* 11(3): 431-448, *http://brief.weburb.dk/archive/00000130/01/2003-costs-security-on-stockvalue-9972866.pdf*.

Cavusoglu, H., B. Mishra and S. Raghunathan (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, *www.gvsu.edu/business/ijec/v9n1/p069.html*.

Cavusoglu, H., H. Cavusoglu and S. Raghunathan (2005), *Emerging issues in responsible vulnerability disclosure*, Fourth Workshop on the Economics of Information Security, Harvard University, *http://infosecon.net/workshop/pdf/cavusoglu.pdf*.

CERT (United States Computer Emergency Response Team), Federal Incident Reporting Guidelines, *www.us-cert.gov/federal/reportingRequirements.html*.

CERT Coordination Center (2006), List of CSIRTs with national responsibility, www.cert.org/csirts/national/contact.html, last accessed 10 December 2007.

CERT Coordination Center (2007), The Use of Malware Analysis in Support of Law Enforcement, *www.securitynewsportal.com/securitynews/article.php?title=The_Use_of_Malware_Analysis_in_Support_of_Law_Enforcement*, last accessed 11 December 2007.

Charney, S. (2005), "Combating Cybercrime: A Public-Private Strategy in the Digital Environment", Microsoft Corporation, www.nwacc.org/programs/conf05/UNCrimeCongressPaper.doc, last accessed 11 December 2007.

Chen, P.-Y., G. Kataria and R. Krishnan (2005) "Software Diversity for Information Security", Fourth Workshop on the Economics of Information Security, Harvard University, http://infosecon.net/workshop/pdf/47.pdf.

Choi, J. P., C. Fershtman and N. Gandal (2005), "Internet Security, Vulnerability Disclosure, and Software Provision", Fourth Workshop on the Economics of Information Security, Harvard University, http://infosecon.net/workshop/pdf/9.pdf.

Clayton, R. (2007), "Phishing and the gaining of 'clue'", Light Blue Touchpaper, www.lightbluetouchpaper.org/2007/08/16/phishing-and-the-gaining-of-clue/.

Computer Economics (2007), 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets and other malicious code, *www.computereconomics.com/page.cfm?name=Malware%20Report*.

Congressional Budget Office Cost Estimate (2007), "H.R. 1525 Internet Spyware (I-SPY) Prevention Act of 2007", as ordered reported by the House Committee on the Judiciary, 7 May, *www.cbo.gov/ftpdocs/80xx/doc8076/hr1525.pdf*.

Consumer Reports WebWatch (2005), "Leap of Faith: Using the Internet Despite the Dangers", results of a National Survey of Internet Users for Consumer Reports WebWatch, www.consumerwebwatch.org/dynamic/web-credibility-reports-princeton.cfm ;

Consumers Union (2007), "State of the 'Net' Survey '07", *Consumer Reports*, 2007(9): 28-34.

Consumentenbond (2006), "PC beveiliging & veilig Internet: Een enquête onder computergebruikers", *Consumentengids*, 2006(11).

Council of Europe (2001), *Convention on Cybercrime*, Budapest, 23 November, *http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm*.

Council of Europe (2007), "Status of Signatories and Parties to the Convention on Cybercrime", CETS No. 185, *http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=16/04/04&CL=ENG*, last accessed 11 December 2007.

Counterpane & MessageLabs (2006), *2005 Attack Trends & Analysis*, *www.counterpane.com/dl/attack-trends-2005-messagelabs.pdf*.

CSI (Computer Security Institute) (2007), *CSI Survey 2007: The 12th Annual Computer Crime and Security Survey*, *www.gocsi.com/forms/csi_survey.jhtml*.

CSI/FBI Computer Crime and Security Survey (2006), *www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml;jsessionid=4SCJQ3Y0PCPTOQSNDLPCKHSCJUNN2JVN*.

Dancho D. (2006), "Malware – future trends", *www.linuxsecurity.com/docs/malware-trends.pdf*, last accessed 7 December 2007.

Dearne, K. (2007), "Online security begins at home", *Australian IT News*, *http://australianit.news.com.au/articles/0,7204,21675098%5E24169%5E%5Enbv%5E,00.html*, last accessed 11 December 2007.

Denning, D. (2000), "Statement by Dorothy E. Denning", Georgetown University, *http://ftp.fas.org/irp/congress/2000_hr/00-05-23denning.htm*.

Devillard, A. (2006), *Le « phishing » en France, peu de victimes mais une menace grandissante*, 01net, *www.01net.com/editorial/311785/cybercriminalite/le-phishing-en-france-peu-de-victimes-mais-une-menace-grandissante/*, last accessed 11 December 2007.

Dhamija, Rachna, *et al.* (2007), "The Emperor's New Security Indicators, An evaluation of website authentication and the effect of role playing on usability", *http://usablesecurity.org/emperor*.

Dot-TK (2007), "Dot Tk Free Domain Names – A New Approach To Make A Whole Top Level Country Domain Free Of Illicit Content", *www.dot.tk/en/press_jul16-07.pdf*.

Du, Y. (2007), "Introduction of malware Issues", presentation by CNCERT/CC at the APEC-OECD Malware Workshop, *www.oecd.org/dataoecd/33/59/38653107.pdf*, last accessed 10 December, 2007.

Dynes, S., E. Andrijicic and M. E. Johnson (2006), "Costs to the U.E. Economy of Information Infrastructure Failure from Field Studies and Economic Data", Fifth Workshop on the Economics of Information Security 2006, *http://weis2006.econinfosec.org/docs/4.pdf*.

Dynes, S., H. Brechbühl and M. E. Johnson (2005), *Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm*, Fourth Workshop on the Economics of Information Security, Harvard University, *http://infosecon.net/workshop/pdf/51.pdf*.

The Economist (2007), "A cyber riot", 10 May, *www.economist.com/world/europe/displaystory.cfm?story_id=9163598*, accessed 4 December, 2007.

Edwards, L., (2004), "Reconstruction Consumer Privacy Protection Online", *International Review of Law – Computers & Technology*, Vol. 18, No. 3, p. 315.

Eeten, M. J. van and J. M. Bauer (2008), "Economics of Malware: Security Decisions, Incentives and Externalities", *OECD Science, Technology and Industry Working Papers*, 2008/1, OECD Publishing, doi:10.1787/241440230621.

Ehrlich, I. (1996), "Crime, Punishment, and the Market for Offenses", *The Journal of Economic Perspectives*, 10(1): 43-67, *http://links.jstor.org/sici?sici=0895-3309%28199624%2910%3A1%3C43%3ACPATMF%3E2.0.CO%3B2-U*.

ENISA (European Network and Information Security Agency) (2006), *Provider Security Measures Part 1: Security and Anti-Spam Measures of Electronic Communication Service Providers - Survey*, *www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf*.

Ernst & Young (2007), *Global Information Security Survey 2006*, *www.ey.nl/download/publicatie/2006_GISS_EYG_AU0022.pdf*.

European Union (1995), "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal of the European Communities*, L 281/31, *http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf*, accessed 11 December 2007.

European Union (2002), "Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector", *Official Journal of the European Communities*, L 201/37, *http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_201/l_20120020731en00370047.pdf*, accessed 11 December 2007.

European Union (2005), "Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems", *Official Journal of the European Communities,* L 69/67 *http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf*.

European Commission (2007), "E-Communication Household Survey", Special Eurobarometer 274, Wave 66.3, *http://ec.europa.eu/public_opinion/archives/ebs/ebs_274_en.pdf*, last accessed 10 December 2007.

Fox, J. (2007), *Consumer Reports: Putting Consumers Back in Control*, Federal Trade Commission, *www.ftc.gov/bcp/workshops/spamsummit/presentations/Consumers.pdf*.

Franklin, J., *et al*. (2007), "An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants", CCS'07, *www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf*.

Friedman, L. S. (2002), *The Microeconomics of Public Policy Analysis*, Princeton University Press, Princeton.

F-Secure (2007), "IT Security Threat Summary for H1 2007", F-Security Data Security Wrapup 1/2007, *www.f-secure.com/2007/1/*.

Gal-Or, E. and A. Ghose (2003), "The Economic Consequences of Sharing Security Information", 2nd Annual Workshop on Economics and Information Security, *www.cpppe.umd.edu/rhsmith3/papers/Final_session7_galor.ghose.pdf*.

Gal-Or, E. and A. Ghose (2005), "The Economic Incentives for Sharing Security Information", *Information Systems Research*, 16(2): 186-208, *www.andrew.cmu.edu/user/aghose/Infosec.pdf*.

Gartner (2005), "Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce", press release, *www.gartner.com/press_releases/asset_129754_11.html*.

Gaudin, S. (2007), "T.J. Maxx Security Breach Costs Soar To 10 Times Earlier Estimate", *Information Week*, *http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201800259*.

GetSafeOnline (2006), *The Get Safe Online Report*, October, *www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf*.

Google, Inc. (2007), "The Ghost In The Browser Analysis of Web-based Malware", *www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf*, accessed 12 December 2007.

Gordon, L. A. and M. P. Loeb (2002), "The Economics of Information Security Investment", *ACM Transactions on Information and System Security*, Vol. 5, Issue 4, pp. 438-457, *http://portal.acm.org/citation.cfm?id=581274*.

Govcert.nl (2006), *Annual Review, www.govcert.nl/render.html?it=147*, last accessed 13 December 2007.

Govcert.nl (2007), "Botnets", presentation given by Douwe Leguit at the APEC-OECD Malware Workshop, *www.oecd.org/dataoecd/34/36/38653287.pdf*, accessed 10 December 2007.

Greene, T. (2007), "Kapersky seeks help from international police to fight cybercrime", *Network World*, *www.networkworld.com/news/2007/013107-kaspersky-cybercrime.html*, accessed 14 December 2007.

Heidrich, J. (2007), "IP-Blacklisting zur Spam-Abwehr kann rechtswidrig sein", *Heise Online, www.heise.de/newsticker/meldung/97568*.

Higgins, K. J. (2007a), "Battling Bots, Doing No Harm", *Dark Reading*, *www.darkreading.com/document.asp?doc_id=118739*.

Higgins, K. J. (2007b), "Untying the Bot Knot", *Dark Reading*, *www.darkreading.com/document.asp?doc_id=114081&WT.svl=news1_6*

Honeynet Project and Research Alliance (2007), *Know your enemy: Fast-Flux Service Networks*, *www.honeynet.org/papers/ff/*, accessed 13 December, 2007.

House of Lords (2007a), *Science and Technology Committee, 5th Report of Session 2006–07, Personal Internet Security, Volume I: Report*, Authority of the House of Lords, *www.publications.parliament.uk/pa/ld/ldsctech.htm*.

House of Lords (2007b), *Science and Technology Committee, 5th Report of Session 2006–07, Personal Internet Security, Volume II: Evidence*, Authority of the House of Lords, *www.publications.parliament.uk/pa/ld/ldsctech.htm*.

Hypponen, M. (2006); "Malware goes mobile"; *Scientific American,* pp.70-77, *www.cs.virginia.edu/~robins/Malware_Goes_Mobile.pdf*, accessed 13 December 2007.

iGillottResearch, Inc. (2006), "The Trusted Computing Group Mobile Specification: Securing Mobile Devices on Converged Networks", White Paper, September, *www.trustedcomputinggroup.org/groups/mobile/Final_iGR_mobile_security_white_paper_sept_2006.pdf*, accessed 7 December 2007.

ITU (International Telecommunications Union) (2007), "Executive Summary", *World Information Society Report 2007: Beyond WSIS*, *www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07-summary.pdf*.

Javelin Strategy & Research (2007), *2007 Identity Fraud Survey Report – Consumer Version How Consumers Can Protect Themselves, www.acxiom.com/AppFiles/Download18/Javelin_ID_Theft_Consumer_Report-627200734724.pdf*, accessed 14 December 2007.

Just, R. E., D. L. Hueth and A. Schmitz (2004), *The Welfare Economics of Public Policy: A Practical Approach to Project and Policy Evaluation*, Edward Elgar, Cheltenham, UK and Northampton, MA.

Kaspersky Labs (2006), *Malware Evolution 2006: Executive Summary*, *www.kaspersky.com/malware_evolution_2006_summary*.

Krebs, B. (2006), "The New Face of Phishing", Washington Post Security Fix weblog, *http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html.*

Krebs, B. (2007), "Study: $3.2 Billion Lost to Phishing in 2007", Washington Post Security Fix weblog, *http://blog.washingtonpost.com/securityfix/2007/12/study_32_billion_lost_to_phish_1.html*.

Krebs, B. (2008), "Banks: Losses from Computer Intrusions Up in 2007", Washington Post Security Fix weblog, *http://blog.washingtonpost.com/securityfix/2008/02/banks_losses_from_computer_int.html*.

Kunreuther, H. and G. Heal (2003), "Interdependent security", *Journal of Risk and Uncertainty*, 26(2): 231.

Lacohée, H., S. Crane and A. Phippen (2006), "Trustguide: Final Report", BT Group Chief Technology Office, Research & Venturing / HP Labs / University of Plymouth, Network Research Group, *www.trustguide.org.uk/Trustguide%20-%20Final%20Report.pdf*.

LaRose, R., N. Rifon, S. Liu and D. Lee (2005), "Understanding Online Safety Behavior: A Multivariate Model", International Communication Association, New York, *www.msu.edu/~isafety/papers/ICApanelmult21.htm*.

Lemos, R. (2006), "Attackers pass on OS, aim for drivers and apps", Security Focus website, *www.securityfocus.com/news/11404*.

Lemos, R. (2007), "Estonia gets respite from web attacks", Security Focus website, *www.securityfocus.com/brief/504*.

Liu, P.-W. (2007), "Panel Discussion: Gaps and Challenges", presentation at the OECD-APEC Tel Malware Workshop by the Director of the Information and Communication Security Technology Center, Chinese Taipei, *www.oecd.org/dataoecd/34/19/38653499.pdf*, accessed 10 December 2007.

McAfee, Inc. (2006), "Virtual Criminology Report 2007 Organized Crime and the Internet", *McAfee Avert® Labs Technical White Papers,* December, *www.mcafee.com/us/threat_center/white_paper.html*.

McAfee Inc. (2007), "Identity Theft", *McAfee Avert® Labs Technical White Papers*, January, *www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf*.

McCarthy, C. (2007), "Study: Identity theft keeps climbing", *Cnet News*, *http://news.com.com/Study+Identity+theft+keeps+climbing/2100-1029_3-6164765.html*.

McNamara, P. (2007), "Survey: Identity theft on the decline", *Network World*, *www.networkworld.com/community/?q=node/11009*, accessed 11 December 2007.

Marshall, A. (1920), *Principles of Economics: An Introductory Volume*, Macmillan, London.

Mashevsky, Y. (2007), "The Virtual Conflict – Who Will Triumph?", *The Virtualist*, *www.viruslist.com/en/analysis?pubid=204791915*.

Mell, P., K. Kent and J. Nusbaum (2005), *Guide to Malware Incident Prevention and Handling*, National Institute of Standards and Technology, *http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf*.

Messaging Anti-Abuse Working Group (2007), "Email Metrics Program: The Network Operators' Perspective; Report #5 - First Quarter 2007, June 2007", *www.maawg.org/about/MAAWG20071Q_Metrics_Report.pdf*, accessed 10 December 2007.

NISCC (UK National Infrastructure Security Information Centre) (2005), "Targeted TrojanEmail Attacks", *NISCC Briefing*, 08/2005, *www.cpni.gov.uk/docs/ttea.pdf*, accessed 7 December 2007.

MessageLabs (2006), *MessageLabs Intelligence: 2006 Annual Security Report - A Year of Spamming Dangerously: The Personal Approach to Attacking, www.messagelabs.com/mlireport/2006_annual_security_report_5.pdf*, accessed 10 December 2007.

Messagelabs (2007), *MessageLabs Intelligence: 2007 Annual Security Report - A year of storms, spam and socializing, www.messagelabs.com/resources/mlireports*, accessed 10 December 2007.

Messmer, E. and D. Pappalardo (2005), "Extortion via DDoS on the rise: Criminals are using the attacks to extort money from victimized companies", *Computerworld*, *www.computerworld.com/networkingtopics/networking/story/0,10801,101761,00.html*, accessed 7 December 2007.

Microsoft (2005), *The Trustworthy Computing Security Development Lifecycle*, *http://msdn2.microsoft.com/en-us/library/ms995349.aspx*.

Microsoft (2006a), *Security Intelligence Report (January – June 2006)*, *www.microsoft.com/downloads/details.aspx?FamilyId=1C443104-5B3F-4C3A-868E-36A553FE2A02&displaylang=en*.

Microsoft (2006b), *Security Intelligence Report (July - December 2006), www.microsoft.com/downloads/details.aspx?familyid=af816e28-533f-4970-9a49-e35dc3f26cfe&displaylang=en*, accessed 3 December 2007.

Microsoft (2007), "Storm Drain", Anti-Malware Engineering Team Weblog, *http://blogs.technet.com/antimalware/archive/2007/09/20/storm-drain.aspx*.

Netcraft Toolbar Community (2007), "Phishing By The Numbers: 609,000 Blocked Sites in 2006", Netcraft website, *http://news.netcraft.com/archives/2007/01/15/phishing_by_the_numbers_609000_blocked_sites_in_2006.html*, accessed 11 December 2007.

NIST (National Institute of Standards and Technology) (2005), *Guide to Malware and Incident Handling: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-83, November, *http://csrc.nist.gov/publications/nistpubs/800-83/SP800 83.pdf*.

NIST (2008), *Computer Security Handling Guide: Recommendations of the National Institute of Standards and Technology*, Special Publication 800-61 Revision 1, March, *http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf*.

Nowotny, E. (1987), *Der öffentliche Sektor: Einführung in die Finanzwissenschaft*, Springer, Berlin.

Oberoi, S. (2007), "Addressing the Malware Problem", presentation given at the APEC-OECD Malware Workshop, *http://www.oecd.org/dataoecd/33/57/38653049.pdf*.

OECD (2002a), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, *www.oecd.org/dataoecd/16/22/15582260.pdf*.

OECD (2002b). "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security – Questions and Answers", *www.oecd.org/dataoecd/27/6/2494779.pdf*.

OECD (2005a), "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2005)1/FINAL, 16 December, *www.oecd.org/dataoecd/16/27/35884541.pdf*.

OECD (2005b), *Science, Technology, and Industry Scoreboard*, 2005 edition, OECD Publishing, Paris.

OECD (2006), "OECD Anti-Spam Toolkit of Recommended Policies and Measures", report of the OECD Task Force on Spam, DSTI/CP/ICCP/SPAM(2005)3/FINAL, www.oecd-antispam.org/, accessed 13 December 2007.

OECD (2007a), *OECD Communications Outlook 2007,* Information and Communications Technologies, OECD Publishing, Paris.

OECD (2007b), "APEC-OECD Malware Workshop: Summary Record", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)15, 15 June, *www.oecd.org/dataoecd/37/60/38738890.pdf*.

OECD (2007c), "The Development of Policies for the protection of Critical Information (CII): A comparative analysis in four OECD countries: Canada, Korea, the United Kingdom and the United States", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2006)15/FINAL, 6 February, *www.olis.oecd.org/olis/2006doc.nsf/ENGREFCORPLOOK/NT00007766/$FILE/JT03221273.PDF*.

OECD (2008a), "The Development of Policies for the protection of Critical Information (CII): A comparative analysis in three OECD countries: Australia, Japan, and the Netherlands", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)16/FINAL, 9 January, *www.olis.oecd.org/olis/2007doc.nsf/ENGREFCORPLOOK/NT00005A5E/$FILE/JT03238526.PDF*.

OECD (2008b), "Scoping Paper on Online Identity Theft", unclassified document, DSTI/CP(2007)3/FINAL, 15 May, *www.olis.oecd.org/olis/2007doc.nsf/ENGREFCORPLOOK/NT00005CAE/$FILE/JT03240674.PDF*.

OECD (2008c), "The Development of Policies for the Protection of Critical Information Infrastructures (CII): A Comparative Analysis in Seven OECD Countries: Australia, Canada, Korea, Japan, The Netherlands, The United Kingdom and the United States", unclassified document of the Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)20/FINAL, 8 April, *http://www.olis.oecd.org/olis/2007doc.nsf/ENGREFCORPLOOK/NT00005A8A/$FILE/JT03243745.PDF*.

ORF (2007), *Spamhaus antwortet auf nic.at*. futurezone, *http://futurezone.orf.at/it/stories/201738/*, accessed 25 November 2007.

Outlaw.com (2007), "Phishing attack evades ABN Amro's two-factor authentication", OUT-LAW News, 18 April, *www.out-law.com/page-7967*, accessed 11 December 2007.

PayPal (2007), "Key Financial Facts", Paypal website, *www.pppress.co.uk/* .

Pigou, A. C. (1932), *The Economics of Welfare*, Macmillan, London.

Poindexter, J. C., J. B. Earp and D. L. Baumer (2006), "An experimental economics approach toward quantifying online privacy choices", *Information Systems Frontiers*, 8(5): 363-374.

Poulsen, Kevin (2003), *Slammer worm crashed Ohio nuke plant network,* Security Focus, *www.securityfocus.com/news/6767*, accessed 11 December 2007.

Register (2007), "Phishing attack evades bank's two-factor authentication", *www.theregister.co.uk/2007/04/19/phishing_evades_two-factor_authentication/*.

Rescorla, E. (2004), "Is finding security holes a good idea?", Workshop on Economics and Information Security 2004, *www.rtfm.com/bugrate.pdf*.

Rifon, N., E. T. Quilliam and R. LaRose (2005), "Consumer Perceptions of Online Safety", paper presented at the International Communication Association, Communication and Technology Division, New York, 27 May, *www.msu.edu/~isafety/papers/ICApanelfg.htm*.

Rowe, B. R. and M. P. Gallaher (2006), "Private Sector Cyber Security Investment: An Empirical Analysis", Fifth Workshop on the Economics of Information Security, Cambridge, March, *www.weis2006.econinfosec.org/docs/18.pdf*.

RSA Security (2006), "Internet Confidence Index Shows that – for Businesses and Consumers – Transactions are Outpacing Trust", *www.rsa.com/press_release.aspx?id=6502,* accessed 14 December 2007.

Schechter, S. E. (2004), *Computer Security Strength & Risk: A Quantitative Approach*, thesis presented to the Division of Engineering and Applied Sciences, Harvard University, May, *www.eecs.harvard.edu/~stuart/papers/thesis.pdf*.

Schneier, B. (2000), *Secrets and Lies: Digital Security in a Networked World*, John Wiley, New York.

Schneier, B. (2005), "A Real Remedy for Phishers", *Wired News*, *www.wired.com/news/politics/0,1283,69076,00.html*.

Schneier, B. (2007), "Information Security and Externalities", NSF/OECD Workshop on Social & Economic Factors Shaping The Future of the Internet, Washington, DC, *www.oecd.org/dataoecd/60/8/37985707.pdf*.

Shifrin, T. (2007), "Lose an unencrypted laptop and 'face criminal action'", *Computerworld UK*, 15 November, *www.computerworlduk.com/management/security/data-control/news/index.cfm?newsid=6241*.

Shin, A. (2007a); "Is Identity Theft Decreasing?", The Checkout Washington Post Blog, 6 February, *http://blog.washingtonpost.com/thecheckout/2007/02/is_identity_theft_decreasing.html*.

Shin, A. (2007b), "Looking for a Job? Phishers Are Looking for You.", The Checkout Washington Post Blog, 12 February, *http://blog.washingtonpost.com/thecheckout/2007/02/looking_for_a_job_phishers_are.html*.

Shostack, A. (2005), "Avoiding Liability: An Alternative Route to More Secure Products", Fourth Workshop on the Economics of Information Security, Harvard University, *infosecon.net/workshop/pdf/44.pdf*.

Snyder, W. (2007), "Time to Deploy improvement of 25 %", Mozilla Security Blog, *http://blog.mozilla.com/security/2007/06/18/time-to-deploy-improvement-of-25-percent/*.

Sokolov, D. A. (2007), "Spamhaus.org setzt Österreichs Domainverwaltung unter Druck", Heise online, *www.heise.de/newsticker/meldung/91417*; last accessed 25 November 2007.

Sophos (2006a), "The Growing Scale of the Threat Problem", *www.sophos.com/sophos/docs/eng/papers/Growing-threat-wpus.pdf*, accessed 7 December, 2007.

Sophos (2006b), "Devious Arhiveus ransomware kidnaps data from victims' computers", *www.sophos.com/pressoffice/news/articles/2006/06/arhiveus.html*, accessed December 7, 2007.

Sophos (2006c), "Married couple formally charged over spyware Trojan horse", *www.sophos.com/pressoffice/news/articles/2006/03/israeliesp2.html*, accessed 13 December 2007.

Sophos (2007a), "Security Threat Report", Sophos Security white paper, *www.sophos.com/security/whitepapers/*, last accessed 12 December 2007.

Sophos (2007b), "Security Threat Report Update July 2007", Sophos Security white paper, *www.sophos.com/security/whitepapers/*, accessed 12 December 2007.

South, G. (2007), "Web issues over banking code", *The New Zealand Herald*, *www.nzherald.co.nz/topic/story.cfm?c_id=126&objectid=10458545*.

Spamhaus (2007), "Report on the criminal 'Rock Phish' domains registered at Nic.at", Spamhaus statements, 21 June, *www.spamhaus.org/organization/statement.lasso?ref=7*, accessed 25 November 2007.

Table of Contents

Figures

Boxes