Introduction to the Economics of Cybersecurity

Johannes M. BAUER
Michigan State University

Michel VAN EETEN
Delft University of Technology

The challenges of cybersecurity

Cybercrime, cyberterrorism, and cyberwar are apocalyptic horsemen of the information age. Business leaders regularly name information security as the biggest challenge facing them in the future. Information security breaches entail direct and indirect costs to businesses and individuals that are affected and to society at large. But the negative effects of such violations go much further. Information security is critical to sustain trust in electronic transactions. Without such trust, only part of the productivity gains that could be achieved with the help of advanced information and communication technologies will materialize. Moreover, trust in the security and confidentiality of electronic means of communication is also an important precondition for realizing many of their potential benefits for invigorated civic life. It is difficult to estimate the extent of opportunities foregone by insufficient information security and it is the unknown magnitude of the associated opportunity costs that renders the formulation of good policies difficult.

Information and communications technologies have permeated all aspects of society. Embedded in all other critical infrastructures, including energy, transportation, as well as health and emergency services, they themselves form a critical nervous system of the economy, government and private life (SOMMER & BROWN, 2011; GALLAHER, LINK & ROWE, 2008). They have also become an indispensible component of research, development and innovation, the key drivers of change in knowledge-based economies. As general purpose technologies, they are used in an increasing range of business transactions, such a financial services, e-commerce, and global supply chains. Their wide diffusion has greatly enhanced the range of technological opportunities in sectors not least by enabling new forms of networked interaction. Many efforts to expand the frontiers of knowledge rely on collaboration and flexible sharing of information and data across time and space: e-research is increasingly based on massive, openly accessible

COMMUNICATIONS & STRATEGIES, no. 81, 1st quarter 2011, p. 1.

datasets; health services can be greatly improved by electronic information sharing; open innovation is built around fluid organizational boundaries, often mediated by information and communication technology; and social media derive a large part of their appeal from the sharing of information.

Reaching an appropriate level of information security is difficult. A first factor complicating matters is the increasing number of players required to provide advanced communication systems. In addition to hardware manufacturers and network operators, software vendors, a plethora of application and service providers, and different types of users populate this space (OECD 2009). As these players complement each other, the problem is compounded by the high interdependence among them. Increasing national and international broadband connectivity enhances the opportunities of cybercriminals to launch attacks with high trans-border agility, as the risk of being caught and prosecuted is lessened by the complications of orchestrating effective international law enforcement. At the same time, the sophistication of attacks increases continuously in a technology race between defenders, such as information security service providers, and increasingly specialized attackers. Heterogeneous communities of application developers – some open source, some proprietary, some hybrid – and user groups with greatly varying information security savvy open many potential inroads for attacks. The proliferation of new uses such as social networks, new mobile devices and applications, and the emergence of new services related to cloud computing all open new vulnerabilities.

The threat landscape is continuously shifting and attacks are becoming increasingly sophisticated. Early generations of "white hat" hackers were motivated by notoriety and fame but typically sought to reveal security problems to help fix them. During the past decade, a differentiated and skilled underworld of cybercrime has emerged whose primary motive is financial gain. Whereas computer viruses continue to be a problem, criminal attack strategies now more typically rely on malware, propagated in multiple ways via viruses, worms, trojans, and drive-by attacks from compromised websites (e.g., Symantec, 2011). Large numbers of infected computers are integrated in versatile botnets, which serve as platforms for sending spam, fraud, and other types of cybercrime (OECD, 2009; HOGBEN *et al.*, 2011). For the past few years, attacks have become more targeted. Nearly half the respondents in the latest CSI Computer Crime and Security Survey that had experienced security incidents reported targeted attacks, double the number from two years prior (CSI, 2010).

Information security has both private and public good characteristics. Given the complexity of the information and communications system, the question of whether a desirable level of security for individual players and society overall will be achieved by decentralized decisions of the players demands close scrutiny. Each of the players responds to incentives relevant to their own objectives. For example, application providers, such as Facebook, encounter trade-offs between providing high levels of security and privacy and their ability to earn revenues from advertisers and complementary business partners. Many incentives nudge players toward higher security but there are also many potential flaws that may cause a deviation between the private and the social costs and benefits of decisions. If this is the case, a sub-optimal level of security overall will result (VAN EETEN *et al*. 2008; BAUER & VAN EETEN, 2010). Moreover, in highly interconnected systems, the overall level of security may be strongly influenced by the weakest link (VARIAN, 2004).

The Internet and the vibrant information services enabled by it have evolved largely in an environment free of government regulation. Many of the governance issues were addressed using bottom-up methods of self-regulation or, in some cases, co-regulation between government agencies and stakeholders. From these developments hybrid forms of governance emerged, in which alternative and traditional forms of regulation complement (and sometimes rival) each other. The collective-action problems of cybersecurity have led to several new initiatives at the national, regional, and international levels by government and non-government actors. They range from government-led international thrusts such as the Cybercrime Convention, promulgated by the Council of Europe, and the London Action Plan (LAP) to national legal and regulatory initiatives, such as the Australian Internet Security Initiative (AISI), often in public-private partnerships. Moreover, several private sector-led projects address cybersecurity, including the Messaging Anti-Abuse Working Group (MAAWG) and the Cloud Security Alliance (CSA). Currently, these measures amount to a patchwork rather than an integrated approach but they are steps in the right direction and will help designing more effective solutions. Recent work on the economics of cybersecurity, to which we turn in the next subsection, is an important source of knowledge for these initiatives.

Economics of cybersecurity

At the heart of the rapidly growing field of the economics of cybersecurity, we find this key insight captured by ANDERSON & MOORE (2006, p. 610):

> "[P]eople have realized that security failure is caused at least as often by bad incentives as by bad design."

Market players make their own tradeoffs regarding what kind of security measures they deem appropriate and rational, given their business model. Clearly, these business models are very different for actors in the different niches of the complex ecosystem surrounding information systems and networks. In other words, many instances of what could be conceived as security failures are in fact the outcome of rational economic decisions, given the costs and benefits facing the actors involved within the timeframe of those decisions.

As security comes at a cost, tolerating some level of insecurity is economically justifiable. From an economic perspective, the key question is whether the costs and benefits perceived by market players are aligned with social costs and benefits of an activity. In certain situations, the security decisions of a market player may be rational for that player, given the costs and benefits it perceives, but its course of action may impose costs on other market players or on society at large. These costs are typically not taken into account by the market player making the initial decision, causing an "externality." Externalities are forms of market failure that lead to sub-optimal outcomes if left unaddressed. In the presence of externalities, Internet-based services may be less secure than is socially desirable.

Security externality is a key concept, but economics offers a broader framework to make sense of security issues. As ANDERSON (2001, p. 1) wrote in an early, ground-breaking piece:

> "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 research, the incentives that stimulate efficient behavior are central.

The approach has been used, for example, to explain security issues in software markets (ANDERSON & MOORE, 2006). These markets tend to be dominated by a few firms. Dominance can be due to network externalities –

the more people use certain software, the more valuable it becomes, and the more users it attracts. These incentives have effects on security. First-mover advantages reward a short time to market, rather than longer development cycles that result in better security. Vendors of platform software, such as operating systems, have to attract vendors of complementary products for the platform. The more complementary products are available, the more valuable the platform. To become dominant, platform vendors may be reluctant in implementing security restrictions for those complementary products.

In the markets for Internet access, incentives drive how providers deal with security issues in their networks (VAN EETEN & BAUER, 2008). A dominant incentive is the often high cost of customer support, which works against contacting large numbers of customers with infected machines. On the other hand, providers that do not act against abuses can suffer a backlash from other providers who blacklist and block their traffic. In the interactions among providers, it was suggested that large providers are more or less immune to such forms of peer pressure and, therefore, have weaker incentives to act against security problems (MOORE *et al.*, 2009). Recent empirical research, however, revealed that the networks of large Internet service provider harbor, on average, fewer infected machines per subscriber than those of small providers (VAN EETEN *et al.*, 2010). Other incentives seem to be more powerful, such as whether telecommunication regulators are active in the area of security of providers.

The incentives of financial service providers, such as banks, lead them to often compensate customers for the damage they suffered from online fraud. In that sense, they internalize the externalities of sub-optimal security investments of their customers as well as the software vendors whose software is exploited to execute the attacks. The financial institutions bear these externalities, but they are also in a position to mitigate the size of these externalities, i.e., they can manage the risk through the security measures around online financial services. For these providers, but also for society as a whole, it may currently be more efficient to keep losses at acceptable levels, rather than to aggressively seek to reduce them. A dominant incentive is the benefits of a growing online transaction volume. Any security measure that might reduce the ease of use of online financial services may impede this growth, which implies costs that are likely to be much higher than the current direct damage from malware-related fraud.

The behavior of many different market players has been examined from an economic perspective. Looking at security issues in terms of costs and

benefits also helps to put broader security questions in perspective. For example, in a technical sense, the number of phishing attacks may be rising, but this may in fact reflect a diminishing economic success of these attacks (HERLEY & FLORENCIO, 2008). The evidence indicating the actual losses of security incidents is ambiguous. The earlier cited CSI Computer Crime and Security Survey found that while reported losses of firms rose in recent years, they are still much lower compared to the losses reported in 2001 and 2002.

Where we have better evidence that economic damage is indeed rising, such as with financial fraud, fraud levels may actually be diminishing in relative terms, compared to the total volume of transactions. In 2009, the UK Payments Administration reported that card-not-present fraud – which includes Internet-based fraud – had risen by 350 percent in the period from 2000 to 2008 (APACS, 2009). In the same period, the total value of online shopping alone increased by 1,077 percent. As an aside, the figures for 2009 and 2010 actually show a decrease compared to 2008, even in absolute terms (UK Cards Association, 2011).

Main themes of this special issue

Research in the area of the economics of cybersecurity is still expanding. This special issue aims to contribute to a blossoming field that has changed our understanding of security issues. The papers in this special issue reflect state-of-the art thinking on the economics of cybersecurity and responses by public policy and non-governmental action.

The unabated use of public awareness campaigns to stress the ability and responsibility of consumers to protect themselves against cyberrisks receives both support and resistance. Supporters see consumers as clueless facilitators of crime, by publishing personal data online or otherwise disclosing it. Opponents stress that consumers are victims and that private and public organizations are diverting attention away from their own facilitating behavior. van der MEULEN addresses this tension, focusing on the issue of identity theft. She argues that neither side adequately appreciates how recent developments are eroding the consumer's ability to actively control the facilitation process and explores several alternatives to public awareness campaigns.

A classic and still critical question in cybersecurity is this: who benefits more from publicly available information on security incidents, the attackers

or the defenders? MOORE & CLAYTON bring an innovative empirical approach to bear on this issue. They study the impact of publicly available information on phishing web sites. If attackers benefit more from this information than defenders, then phising websites placed on a public blacklist should be re-compromised more often than phishing websites that are only known within closed communities. Their analysis forcefully demonstrates the opposite. Their conclusion is that strategic disclosure of incident information can actually help defenders, if properly designed.

BLUMENTHAL critically examines the security implications of cloud computing. Cautioning against the current hype surrounding the provision of platforms as a service (PaaS), infrastructure as a service (IaaS) and software as a service (SaaS), she reveals several potential security risks. Clouds could be used as new platforms for malice, offering both new ways to configure attacks and to evade criminal prosecution. Users of cloud services cannot easily assess the security policies and precautions of service providers, which often decline liability for data breaches in their service agreements. Given these potential risks, the paper discusses implications for organizations and individuals and suggests next steps for researchers and public policy that could help address the concerns raised.

The enduring problem of infected end user machines, most notably in the form of botnets, has demonstrated that this problem cannot be solved by end users alone. Increasing attention is paid to the role of critical intermediaries, such as ISPs. ISPs, however, have incentives that discourage them from dealing with large numbers of infected customers. CLAYTON explores a specific solution to overcome this incentive problem, namely government subsidies for cleaning up computers. In other words, we would treat infections as a public health issue. Based on certain assumptions, he estimates that the costs of such an initiative may be lower than is often assumed, and could be as low as one dollar per person per year.

BISOGNI, CAVALLINI & TROCCHIO discuss the role of information availability in enhancing cybersecurity. Their narrowly construed analysis is based in an economic model of information security investment, in which the effects of a lack of information are examined. After a brief overview of the prevailing European institutional and regulatory framework for cybersecurity, the authors discuss three actions at the European level that could contribute to better information security: (1) information sharing about threats, (2) information sharing about information security breaches, and (3) measures that increase information security competence.

Challenges of securing the vast, decentralized Internet infrastructure are addressed by KUERBIS & MUELLER. Early routing protocols were designed without particular attention to security. The paper focuses on Resource Public Key Infrastructure (RPKI), an effort to reduce the resulting vulnerabilities. RPKI changes the relations among stakeholders, increasing the influence of centralized players at the expense of Internet Service Providers (ISPs). Describing in detail the mixed incentives of the various players (ICANN, regional registries, and ISPs), the paper examines conflicts of interest. The authors show how, for the time being, consensus could be achieved by permitting voluntary actions by ISPs but anticipate continued tensions over the establishment of more centralized governance structures.

The special issue is rounded-off with two interviews about the challenges of information security and ongoing initiatives to meet them. Keith Besgrove is the First Assistant Secretary, Consumer Policy and Post division of the Australian Department of Broadband, Communications and the Digital Economy. He also serves as the Chairman of the OECD Working Party on Internet Security and Privacy (WPISP). Evert van Hummelen is the head of the team Internet Security at the Dutch regulatory agency OPTA. Both provide important perspectives by experts on the forefront of policy efforts to enhance information security.

Putting together this special issue involved the collaboration of many individuals. We would like thank the contributors for their submissions and their prompt responses to editorial requests. We also would like to thank reviewers for their critical reading and helpful comments on the original manuscripts. Special thanks also to Keith Besgrove and Evert Jan Hummelen who found time in their busy schedules to respond to our questions. Sophie Nigon at IDATE was a good cheerleader who kept us motivated and on track and Yves Gassot lent his support to pursue the topic of cybersecurity. We received a larger number of good papers than could be accommodated; several will be published in future issues of *COMMUNICATIONS & STRATEGIES*.

References

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. http://www.acsac.org/2001/papers/110.pdf.

APACS (2009): Fraud – *The facts 2009. The definitive overview of payment industry fraud and measures to prevent it*. http://www.theukcardsassociation.org.uk/files/fraud_the_facts_2009.pdf.

BAUER, J.M. & VAN EETEN, M., J.G. (2009): "Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options", *Telecommunications Policy*, 33(10/11), 706-719.

CSI (2010): *2010/2011 CSI Computer Crime & Security Survey*, New York: Computer Security Institute.

HERLEY, C. & D. FLORENCIO (2008): "A Profitless Endeavor: Phishing as Tragedy of the Commons". http://research.microsoft.com/apps/pubs/?id=74159.

GALLAHER, M.P., LINK, A.N. & ROWE, B.R. (2008): *Cyber Security: Economic Strategies and Public Policy Alternatives*, Cheltenham, UK; Northampton, MA: Edward Elgar.

HOGBEN, G., PLOHMANN, D., GERHARDS-PADILLA, E. & LEDER, F. (2011): "Botnets: Detection, Measurement, Disinfection & Defence", Heraklion, Crete, Greece: European Network and Information Security Agency (ENISA).

OECD (2009): *Computer Viruses and Other Malicious Software*, Paris: Organisation for Economic Co-operation and Development.

SOMMER, P. & BROWN, I. (2011): "Reducing Systemic Cybersecurity Risk", OECD/IFP Project on Future Global Shocks, IFP/WKP/FGS(2011)3. Paris: Organisation for Economic Co-operation and Development.

Symantec (2011): "MessageLabs Intelligence", February. http://www.messagelabs.com/globalthreats.

UK Cards Association (2011): "Fraud losses drop on UK cards, cheques and online banking". http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/1323/

VAN EETEN, M. & BAUER, J.M. (2008): "The Economics of Malware: Security Decisions, Incentives and Externalities: Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy", DSTI/ICCP/REG(2007)27, Paris: OECD.

VAN EETEN, M., J. BAUER, H. ASGHARI & S. TABATABAIE (2010): "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data", STI Working Paper 2010/5, OECD. http://www.oecd.org/officialdocuments/displaydocument/?doclanguage=en&cote=dsti/doc(2010)5

VARIAN, H. (2004): "System Reliability and Free-Riding", in L.J. CAMP & S. LEWIS (Eds), *Economics of Information Security* (pp. 1-15), Berlin, New York: Springer.