world development report 2016

BACKGROUND PAPER

Digital Dividends

The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet

Johannes M. Bauer and William H. Dutton
Quello Center, Michigan State University

The New Cybersecurity Agenda:
Economic and Social Challenges to a Secure Internet[1]

Johannes M. Bauer and William H. Dutton

Quello Center, Michigan State University

2 June 2015

Abstract

This paper focuses on key economic and social factors underpinning worldwide issues around cybersecurity and, identifies a new agenda for addressing these issues that is being shaped by the Internet and related information and communication technologies, such as social media. All actors in the widening ecology of the Internet require a better social and cultural understanding of cybersecurity issues in order to effectively engage all relevant stakeholders in processes aimed at enhancing cybersecurity. The problems tied to cybersecurity are not new, but as the Internet becomes ever more essential to everyday life and work, and empowers users as never before, there are new social and economic aspects of the challenges to achieving a secure, open and global Internet that require much more focused attention. For years, computer scientists and engineers have recognized that cybersecurity is not merely an engineering and computer science problem, but also an economic and behavioral challenge. But recognition of the fact that cybersecurity cannot be successfully addressed with technical solutions alone, is not sufficient. It is critical that economists and other social and behavioral scientists engage in this area and address the practices of a wider range of actors in local and global arenas who need strategies that provide feasible and practical steps for securing the Internet and the incentives and mindsets to take them.

[1] This paper has been written as a briefing document in support of the World Development Report. The authors thank the World Bank and David Satola in particular, for requesting our views, and providing guidance, but we wish to emphasize that the views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the World Bank or any other organization.

Introduction

Cybersecurity concerns the "technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor" (Clark et al. 2014: 2). Efforts to bolster cybersecurity are facing a growing range of challenges as the Internet continues to play an increasingly central role in the social and economic development of nations across the world. This is true in every nation, but is particularly the case in the rapidly developing nations, where the Internet's role presents a newer and even more empowering potential for their global role (Dutta et al. 2011).

The range of problems tied to security in the online world is large and growing, and becoming increasingly acute, even though there have been many efforts over the years to enhance cybersecurity (see Box 1). This is in part due to the growing centrality of the Internet in economic and social development, making it a more valuable target, but is also due to the changing dynamics of the problem, such as the growing number of users who are not only vulnerable to cybersecurity threats, but also increasingly culpable even if not directly engaging in any malevolent online activities, from flaming to cyber-bullying.[2] Attempts to address these problems have had limited success in many cases, and have not been able to stop the innovativeness of attackers to come up with new strategies, and of users to fall victim to these strategies. Moreover, the same advances in the Internet that enable more users to more easily bank and shop online, for example, are also making it easier for more individuals to use the Internet for malevolent reasons, such as in virtually democratizing cybercrime.

Box 1. Cybersecurity Incorporates a Range of Separate but Interrelated Issues, including:

- Spamming, such as sending unwanted emails, and spamdexing, such as sending spam aimed at supporting search engine optimization
- Theft of intellectual property (IP theft), such as illegal downloading of copyrighted music or films;
- Cybercrime, such as breaking laws designed for the offline world, such as those against theft or fraud, using online tools, such as in fraudulent romance scams; or Webcam image extortions
- Ransomware, a particular form of malware that disables a computer or an email account until a ransom is paid for its removal
- Destroying or disrupting Internet systems and services, such as through a (distributed) denial-of-service (DoS) attack
- Vandalism, such as defacing a website
- Hacking a PC for use as a Web server for phishing, or spam; email attacks, to harvest email accounts; for bot use, such as click fraud zombie, Distributed DoS zombie, Spam zombie
- Phishing: sending emails or other electronic messages to acquire sensitive information, tricking a person into sending money, opening malware, or falling for a scam or other fraudulent confidence game
- Spear phishing, by targeting specific individuals with information that fools recipients, such as believing the attacker is a friend, in order to obtain information

[2] Users can be partly culpable through such actions as failing to protect their systems, unwittingly exposing them to bots, or not standing up for victims of cyberbullying.

- Distributing malware, that can install a virus or other malicious code on an unsuspecting user's computer, such as a botnet, worm or Trojan horse
- Data breaches, such as through loss or theft of computers or electronic storage devices
- Identity theft, through breaching a computer system or email to obtain information enabling the use of a person's identity for fraudulent access to credit card data, bank account, stock or mutual fund account, or reputation hijacking
- Misuse of social media in ways that can harm users, such as for cyber-bullying, cyber-stalking, and identity theft
- Insider threats, such as a disgruntled employee or other insider purposely undermining security protocols
- Cyber espionage, such as government or corporate spying or eavesdropping by illegally gaining access to email or computer systems
- Cyber warfare, attacking the software, data, or physical computing equipment of a nation to disrupt or destroy services or infrastructures; hostage attacks

So while concerns over cybersecurity have generated a wide range of initiatives, the problems are persisting, if not growing in frequency and significance. Efforts up to this point have been well conceived, but limited in their impact on the overall problem. Arguably, some issues such as spam have been addressed more effectively, often due to the potential for technical responses to be diffused widely. Yet even in this case, the problem must be constantly addressed: spammers create new ways to reach users, and the incentives behind spamming continue to evolve, such as "spamdexing," aimed at optimizing the visibility of a website to search engines.

Recognition of these growing problems has led many individuals, communities and institutions to raise the priority of cybersecurity. For example, the launch of the Global Cyber Security Capacity Centre at the University of Oxford was met with worldwide interest, and generated many commitments to participate in tackling a problem that was widely perceived to exist.[3] And there have been many other efforts undertaken by a multiplicity of stakeholders. While there are cases in which these initiatives have had temporary success in reducing particular problems of cybersecurity, they have not been able as yet to have a lasting impact on a wide range of problems that are rapidly morphing into contests ranging from cat and mouse games to cyber warfare. Perhaps the problems would be far greater had cybersecurity initiatives not been championed, but the problems continue and are perceived to be growing worse as the technology is valued more.

Not all responses have been effective, such as public awareness campaigns that rely only on fear, and do not provide remedies.[4] Another ineffective response has been to blame others. For example, technical experts in cybersecurity tend to view many actors outside their specialized area as relatively unresponsive to the problem, generating a politics of blaming the users, or blaming commercial enterprises for thinking that increasing security is a strategy for losing customers. Instead, there needs to be a reconsideration of approaches to cybersecurity that are more sensitive to, and aware of the economic and social aspects of the problems, such as why users do not always follow the best practices recommended by the technical security community.

[3] http://www.oxfordmartin.ox.ac.uk/research/programmes/cybersecurity/ [Last accessed May 11, 2015].
[4] See a working paper on the problems with public awareness campaigns: http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness%20CampaignsDraftWorkingPaper.pdf [Last accessed May 17, 2015].

What can be done to support more effective approaches to addressing global and multi-stakeholder actions to enhance cybersecurity for the digital age? Cybersecurity has been high on the agenda of governments, players in the IT industries, and in the many civic groups participating in Internet governance, but paradoxically, the problems are growing and becoming more urgent to address. Because some conventional approaches have not been effective ways of addressing the problem, it is important to challenge conventional wisdom and rethink the ways we address cybersecurity.

Outline of this Paper

The paper begins with a brief introduction to some new elements in an evolving cybersecurity landscape. While not a new issue, we argue that there are key challenges that are raising its significance around the world. This is followed by a broad overview of the widely distributed costs and benefits across the ever-changing and complex global ecology of actors shaping cybersecurity. With this introduction, the paper discusses the incentives of different actors, which might be a central focus of efforts to address the problem. This is followed by an empirically anchored perspective on the attitudes, beliefs and practices of users, a principal issue arising from the incentive structures and costs and benefits associated with cybersecurity. Based on the changes in the cybersecurity landscape, the distribution of costs and benefits, the need to change incentive structures, and the beliefs, attitudes and behavior of users, the paper identifies approaches to addressing cybersecurity in the digital age—suggesting a new agenda for moving forward. The paper ends with a brief summary and conclusion.

New Features of the Evolving Cybersecurity Landscape

The security of telecommunications has been a problem over the centuries, from the use of carrier pigeons to the coming Internet of Things. The Internet was designed to support the sharing of computer resources, including computers and data over networks, rather than to provide security. But with the rise of the Internet, and its use for more basic activities, such as banking and commerce, recognition of cybersecurity as a key problem for the Internet age has increased, albeit not a new issue (e.g., NRC 1991; NRC 2002; Clark et al. 2014: ix).[5] Technical developments, research, public policy initiatives, and practical steps for users have been evolving over the years to strengthen cybersecurity.

For example, the global Internet governance community has focused attention on security issues, and this has led to many regional and national initiatives. These include such organizational innovations as the Internet Corporation for Assigned Names and Numbers (ICANN) forming the Security and Stability Advisory Committee (SSAC) in 2002; development of the European Network and Information Security Agency (ENISA); the creation of national Computer Emergency Response Teams (CERTs), designed to improve the security of a country; and Computer Security Incident Response Teams (CSIRTS), which are typically organized with multiple stakeholders (DeNardis 2014: 90–95). In 2004, the London Action Plan (LAP), an international cybersecurity enforcement network, was founded. Focusing on spam, it grew to include 47 government organizations from 27 countries, 28 private-sector organizations from 27

[5] A full range of reports on cybersecurity by the Computer Science and Technology Board of the US National Research Council provides a sense of the history of rising concerns over this issue. See: http://sites.nationalacademies.org/CSTB/CSTB_059144 [Last accessed May 26, 2015].

nations, and six observer organizations.[6] There have also been initiatives mainly driven by business, such as the Messaging Anti-Abuse Working Group (MAAWG), formed by members of the messaging industry to address issues such as spam. And there have been global collaborations, such as the global Forum for Incident Response and Security Teams (FIRST.org), which has enrolled more than three hundred members from all continents. And there have been numerous intergovernmental initiatives such as the Council of Europe's Convention on Cybercrime adopted in 2001, ratified as of April 2015 by 45 countries including six non-European nations.[7]

However, the scale and severity of the problems appear to be rising along with the growing centrality and ubiquity of the Internet in an Internet-enabled, hyper-connected world. In parallel with the rise of the Internet, there has been a commensurate growth in cybercrime. Problems with spam continue to be a problem for Internet Service Providers (ISPs) and users (Krebs 2014). Threats to privacy have been growing with the development of social media and big data computational analytics, threats that were dramatically exposed by the revelations of Edward Snowden in 2014.[8] Corporate and government networks have been under attack, such as the cyber-attack on SONY and larger US retailers such as Target and Home Depot, and alleged attacks on the Internet infrastructure of the Democratic People's Republic of Korea.

Nevertheless, efforts to address the problems have not been sufficient to reduce what appears to be a rising array of cybersecurity problems. There are many reasons for the difficulties confronting cybersecurity initiatives. Many key actors, including users, have been slow to adopt practices that could enhance their security online. Motivating a wide range of actors across the globe, including over three billion users, to change the way they do things is not only a technical issue. It also requires an understanding of how each actor views cybersecurity, such as their level of awareness, and how they are incentivized to ignore or adopt practices that could protect themselves and others in the online environment. For example, the provision of cybersecurity is often difficult and costly, which might mean that accepting some level of insecurity is economically rational (Anderson and Moore 2006; Moore, Clayton and Anderson 2009), such as when individuals accept the potential risks of online commerce, or organizations decide to accept the costs of compensating victims rather than impose security precautions that may be perceived as cumbersome or off-putting by customers.

Several developments on the cybercrime side also contribute to the potentially wicked nature of the problem.[9] Increasing global connectivity allows criminals to launch attacks using servers and machines in other countries. While controlled remotely by criminals from around the world, the vast majority of malicious messages are sent via US Internet infrastructure, although other high-income countries also rank high. Likewise, the majority of malware is hosted by legitimate

[6] See: http://londonactionplan.org/ [Last accessed May 26, 2015].
[7] See http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG [Last accessed May 27, 2015].
[8] http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html [Last accessed May 17, 2017].
[9] The concept of "wicked" problems is meant to emphasize problems that are exceedingly complex, dynamic, and difficult, if not impossible, to solve.

providers such as Amazon, GoDaddy, or OVH Hosting (France), but this is aggravated by business models of ISPs and hosting providers that emphasize anonymous transactions.[10]

Anonymity raises another limitation on cybersecurity initiatives, which is the need to balance security with other valued objectives, such as privacy and freedom of expression. One real risk of the push for cybersecurity is the potential to undermine other key values and interests that can be enhanced over the Internet. There is a need to balance these sometimes compatible but sometimes competing objectives, such as the "tensions between cybersecurity and surveillance" tied to national security (Clark et al. 2014: 104–05).

Other things being equal, businesses and individual users in higher income countries are more appealing targets. As incomes in low- and middle-income countries increase, even if these increases are unevenly distributed, users in these countries become more appealing targets as well. Historically, while attacks may have been launched by criminals in countries that have poor income opportunities, they were orchestrated via nodes in countries with good connectivity (the largest number of botnet-infected machines continues to be in the United States). However, as global and regional connectivity improves, we can expect that pattern to change, with an increasing share of malicious activity launched in regions that currently only show weak activity, such as Africa.

One key trend in high-income countries is the increasing number of targeted attacks. In 2013, eight incidents each compromised data of more than ten million individuals. A total of 253 major security breaches exposed 552 million identities (Symantec 2014: 13). Similar developments characterized 2014. These attacks, such as the compromising of point-of-sales terminals, are difficult for users to avoid. Another growing phenomenon is ransomware, attacks in which users' access to information is blocked (e.g., by encrypting it) unless a ransom is paid. With the increasing use of mobile devices and social media, these platforms are used more often to launch attacks. As users in developing countries embrace smartphones, and more transactions take place online, it is only a matter of time before attack activities will also migrate to these regions.

Over the past decade, the cybercriminal underworld has developed an increasingly differentiated organization, with specialists emerging in the harvesting of addresses, the development of malware, assembly and leasing out of botnets, market places for stolen data, and multiple ways to monetize illegal transactions (Holt 2012). This division of labor among specialists has increased the sophistication and virulence of attack tools while reducing their price (Franklin et al. 2007). The emergence of online markets for these tools has made them widely available (Holt 2012; Ablon, Libicki and Golay 2014). Combined with the low probability of being caught or prosecuted, given the complexities of international law enforcement in this area, this has improved the ratio of expected rewards to expected costs as seen from a cybercriminal's vantage point.

One consequence of these developments has been an increasingly central focus on the role of social and behavioral issues in addressing cybersecurity. Too often, cybersecurity has been left to the computer experts in the computer sciences and engineering, or to the information technology team in an organization. While their technical knowhow and contribution to a secure organization as

[10] See CSIS and McAfee (2014) and the blog entry at http://www.calyptix.com/malware/top-malware-sites-and-unsafe-servers/ [Last accessed May 26, 2015.

well as to a secure, open and global Internet has been and will remain great, initiatives to address growing problems with cybersecurity face several new challenges that require contributions from many more disciplines and actors. These challenges include:

1. A New Range of Actors and Motivations

The Internet and related information and communication technologies (ICTs), such as social media, mobile Internet and the Internet of Things (IoT), are expanding the range of actors involved in protecting security, including users in particular, who are seldom focused on security except as a necessary step to moving ahead with what they wish to do online (Box 2). At the same time the range of actors who are capable and willing to attack information systems is also broadening, spanning a wide range of motives from attacks on national security to other criminal motives.

Box 2. The Range of Actors in the Cybersecurity Ecosystem include:

- Cybersecurity experts
- Internet users
- Insiders: people within an organization who can undermine security, from unintentionally leaving a laptop on a train, or intentionally leaking information
- Spammers
- Hackers: those who crack systems for well-intentioned purposes, "Whitehats", and those with malevolent intentions, "Blackhats"
- Criminals
- Terrorists
- States
- Businesses and industries providing infrastructures, devices, and software for cybersecurity, such as anti-virus software
- Internet governance communities focused on cybersecurity, including standards boards and committees

2. An Expanding Range of Platforms and Applications

Gone are the days of protecting security on an organization's mainframe computer. An expanding array of platforms, from social media to the World Wide Web, as well as mobile platforms, cloud computing, big data and the IoT, are creating a far more complex set of technological platforms and social settings that have somewhat different characteristics and require somewhat different approaches to security. Some are dependent on the weakest link in a system of connected nodes, such as the use of botnets, others on the efforts of particular actors, such as in the case of targeted attacks on a company or a state (Varian 2004).

The increasing availability of broadband Internet access since the late 1990s has greatly boosted Internet use but also multiplied vulnerabilities. Moreover, the rapid adoption of mobile phones and devices, as well as the networking of an increasing number of objects in IoT, has further increased the number of attack points and expanded the footprint of cybercrime to developing countries (Orji 2012; Shalhoub and Al Qasimi, 2010). According to a recent global survey conducted for Symantec, mobile users are much less security savvy than users of wireline Internet services. In

that survey, conducted in 2013, 57% of adult mobile users were unaware of security solutions for mobile devices (Symantec 2014: 69). This was up 13 percentage points from the previous year, probably reflecting the increasing proportion of users who had upgraded only very recently from feature phones to smartphones, which constitute a greater vulnerability to cybersecurity issues. These trends are aggravated by social media, which offer new attack pathways for phishing, malvertising, and other types of socially engineered intrusions.

Drive-by download attacks infect computers and mobile devices if users visit web pages on compromised or malicious web servers. Attackers install toolkits on these servers that contain exploits for multiple vulnerabilities that put users visiting the websites at risk for downloading infections (Microsoft 2014:.54). With the expanding uses of mobile and social media, new strategies are on the rise. Campaigns that promise free phone minutes, devices, or online surveys have become major vehicles on social networks. Malvertising uses online ads to disseminate malicious code. Cybercriminals often place legitimate ads but replace them with infected ones later on, making it difficult for the advertising networks to detect. The mobile application marketplace is also increasingly used, often using fake versions of popular apps. With the opening of the Android apps marketplace, there are increasing opportunities to trick users into downloading compromised apps. While mobile devices typically detail the permissions sought by an application, mobile users often accept an app without critical examination. Access to other functions such as Bluetooth, GPS, and a camera, in addition to personal data, offers a broader attack surface than traditional computers.

3. Balancing a Wider Range of Issues

Security can no longer be viewed discretely, as it is closely connected with other issues, such as privacy and surveillance, as noted above, and with the risks associated with the new media generally, such as threats tied to the use of social media. Given this interdependence, it is necessary to identify and consider trade-offs that may exist with other goals, such as when increasing security might compromise freedom of expression or personal privacy. This is difficult since users might well sacrifice some values, such as privacy, for security, or even convenience (Dutton and Meadow 1987). It is therefore important for governments and other stakeholders to ensure that rights and responsibilities are protected in the course of ensuring greater cybersecurity.

4. Interdependent Multi-Level Governance Issues

Governance issues are entangling firms, government agencies, nations, regions and global actors in an increasingly interdependent range of governance processes. Recognition of the global scale and interdependence of these issues is critical to avoiding the risks of a fragmentation of governance that could undermine local and global initiatives, not only around cybersecurity, but also around all the issues tied to the Internet, from the privacy of individuals to the vitality of global commerce. The Internet is bringing the developing and developed world into the same boat. The Internet does not have clear national boundaries, making the success of cybersecurity an increasingly worldwide challenge that cannot be contained within any single organizational or national boundary.

5. Awareness of Practices as well as Problems

Public-awareness campaigns have been undertaken for decades, but most often these are based on frightening users. Much more effort needs to be focused on giving users tips and best practice on how to protect their own security and help protect the safety and security of other users. To be successful, these campaigns need systems to be designed in ways that are usable by individuals. The difficulties this aim presents have led to some innovative ideas, such as Vint Cerf's concept of creating organizations analogous to the voluntary fire brigade (Box 3). This leads to the last point—the need for better user-interface designs for security.

Box 3. The Voluntary Fire Brigade Model Applied to Cybersecurity*

Vint Cerf has borrowed the concept of a voluntary fire brigade, common in the United States and other nations, to promote the idea of a "cyber fire department." Like a fire brigade, if there is evidence of a fire hazard or fire breaking out in a household or business, the brigade can enter and fix the problem rather than let the house or business burn down. Imagine an unsuspecting user, whose computer is infected by a virus or hosting a botnet, being interrupted at the door or online by the cyber brigade, letting him know that there is a problem and that they are there to fix it. An invasion of privacy, or a safety net for users?

*See: http://www.v3.co.uk/v3-uk/news/2292683/internet-needs-cyber-fire-department-to-protect-web-users-claims-vint-cerf [Last accessed May 28, 2015].

6. Improving User-Interface Designs for Security Applications

Many of the security systems designed by the technical community are becoming increasingly infeasible for users to apply. For example, it is unrealistic to expect most users to memorize numerous passwords and change them frequently. New designs need to be developed and implemented more widely to make it easier for users to protect themselves and their computers from security breaches, while not compromising other important values and interests of theirs, such as protecting their anonymity or convenience and speed in obtaining a service. Biometric identification shows some promise in usability, such as fingerprint identification for accessing a smartphone, but there are likely to be major risks of individuals hacking into digital fingerprint databases, and creating even greater problems.[11]

7. The Dual Effects of Technological Advances

A last and overarching issue that is not new but increasingly apparent is the dual effects of empowerment. Cyberthreats are evolving rapidly in a technology race pitching efforts to increase security against attempts to find new ways to breach it by malevolent actors. These hostile actors range widely as well, including malevolent hackers,[12] insiders, terrorists, states, and ordinary criminals, who use the Internet.

[11] http://www.popsci.com/article/gadgets/fingerprint-security-not-future-and-god-help-us-if-it [Last accessed May 17, 2015]

[12] A "hacker" was initially defined as a person who was obsessively focused on solving a programming problem, what Joseph Weizenbaum (1976: 111–31) referred to a "compulsive programmer." His worry was that such a compulsion would undermine humanistic knowledge of a problem and create technicians rather than programmers. Since Weizenbaum, the term has been used more often to define individuals who seek to break into, "hack," or crack computer systems, increasingly through the Internet.

The Distributed Costs and Benefits of Cybersecurity

To understand the dynamics of cybersecurity, it is critical to know who gains and who pays for greater or lesser levels of security. However, the actual costs and benefits of cybersecurity continue to elude efforts to develop reliable and valid quantitative indicators. Estimates of the costs of cybercrime abound, but many reports are based on weak evidence and/or overly simplified strong assumptions. Often the employed methods are not publicly available, complicating an assessment of the validity and reliability of the information. Damage is typically assessed at a highly aggregated level and difficult to link to specific incidents.

Recent developments of more robust methods of measurement focus on individual firms and organizations and not on the entire value network or costs to society at large, which would be the relevant metrics for public policy and law-enforcement decisions. The numbers reported are sometimes puzzling, and detailed explanations for their variations are lacking.

A joint study conducted by McAfee and the Center for Strategic and International Studies (CSIS) recently estimated the global costs of cybercrime at $445 billion, or about 0.6% of global GDP (CSIS and McAfee 2014). Indirect significant effects on employment related to information security breaches are also identified in that study, and are estimated to be in the range of 200,000 jobs in the US economy alone.[13] Several years earlier a study conducted for the International Telecommunication Union (ITU) also provided a rough first estimate of the potential direct and indirect global effects of malware as in the range of 0.5% of global GDP (Bauer, van Eeten, Chattopadhyay and Wu 2008). A recent Norton report put the figure of costs to consumers at $113 billion per year, with the costs per victim up by 50% from the previous year.[14] In a detailed analysis of cybercrime in the UK, Anderson and others (2013) found that the cost of preventing cybercrime exceeded the direct costs of information security breaches by several orders of magnitude.[15]

The Ponemon Institute has issued nine annual reports on the global cost of data breaches. Ponemon's (2014) report reflects the experiences of more than three hundred organizations in 10 countries (including the US, UK, Australia, Japan, India, Brazil, and the United Arab Emirates & Saudi Arabia). The sample is deliberately structured to exclude mega data breaches (incidents involving more than 100,000 compromised records) in order not to inflate figures with extreme cases. Findings show that the average per capita cost[16] of data breaches ranged from $51 in India to $201 in the United States (Ponemon Institute 2014: 5). With the exception of Germany, the average per capita cost in every country was higher than in the previous year. Since 2006, the average per capita cost of data breaches has increased by 46% from $138 to $201. The number peaked in 2011 at US$211, declined in 2012 and 2013, only to increase again in 2014. A similar pattern holds for the total cost per affected organization, which was estimated at $5.85 million in

[13] See: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf [Last accessed May 27, 2015]

[14] See: https://msisac.cisecurity.org/resources/reports/documents/b-norton-report-2013.pdf [Last accessed May 27, 2015].

[15] However, from this fact it cannot necessarily be concluded, as the authors seem to suggest, that fighting cybercrime is "inefficient," as the correct damage figure would have to be the potential damage and not the damage that actually occurred, as the latter figure already reflects the effort to prevent incidents.

[16] The per capita cost (perhaps better the "per record" cost) is defined as the total cost of an incident divided by the total number of affected records.

2014. The Ponemon reports also shed light on the relative costs of different types of security problems, with the average cost of malicious attacks the highest, followed by system glitches, and then by "human error." By sector the average cost of data breaches for the healthcare sector was the highest, followed by education, the pharmaceutical industry, and communications (Ponemon Institute 2014: 7).

Regular reports generated by major security firms, such as Symantec, McAfee, Verizon and Sophos, allow detailed insights into dynamic aspects of cybersecurity. While there is concern that industry data may be inflated due to the interests of these players in exaggerating the problem, the overall pattern that emerges from them is surprisingly consistent and lends more credibility to the information. One important aspect is the coexistence of stability and change, such as a fairly stable core of global malicious activity. For example, the United States and China, each with the largest Internet population in their respective regions, have the highest number of bot populations as well. Countries that rank high, but often shift in their ranking one or two levels, include Italy, Brazil, Taiwan, Japan, Canada, Hungary, and Germany (Symantec 2014: 45; Symantec 2015: 97). A similar pattern of relative stability was also found at the level of ISPs (Van Eeten et al. 2009).

There is no clear pattern with regard to the role of emerging and developing countries in the cybercrime landscape. Given the poor ICT infrastructure, countries in the Global South play a relatively minor role as places where malicious activity is hosted as opposed to launched (McAfee Labs 2014). They play a stronger role as places from where cyberattacks and criminal activity are being launched as, for example, email scams aimed at obtaining money transfers, illustrated by the infamous "Nigerian spam," named for the nation in which they originated.[17]

In a similar vein, there is only limited evidence of cyberattacks in developing countries. However, this is likely to change as the Internet becomes increasingly central to these economies. Cybercriminals are aiming at targets that can be exploited with the tools used in the underground economy. Moreover, they are after targets with sufficiently high resources to be exploited. For the time being, this incentive structure tends to protect individuals and organizations in developing countries, who often do not offer the most attractive targets. As the cost of carrying out attacks continues to decrease and the diversity of malware continues to increase, this is likely to change in the near future.

Overall, despite the dynamic change in cybercrime, with improvements in some areas and additional challenges in others, all evidence points in the direction of increased attack activity. McAfee Labs estimated the total number of malware at over 300 million by the end of 2014 up from 200 million the year before; total ransomware was estimated at about 2 million; and total "rootkit malware" at 1.5 million (McAfee Labs 2014: 29).[18] Symantec (2014) estimated the cost per victim of malicious attacks at US$282 in 2013, up 50% from the previous year.

Because of the highly interconnected nature of the Internet, security incidents not only affect the immediate targets of an attack but also have second- and third-round effects on other stakeholders. From a policy perspective, the relevant cost is the total cost to society, which also includes the costs incurred by stakeholders other than those immediately affected. This is one rationale for

[17] http://www.scamwatch.gov.au/content/index.phtml/tag/nigerian419scams [Last accessed May 17, 2015]
[18] Rootkit is software that installs viruses and malware in ways that antivirus software cannot detect. See: http://www.pctools.com/security-news/what-is-a-rootkit-virus/ [Last accessed May 17, 2015]

justifying some kind of cyber security brigade (Box 3 above), as an individual's problem can have broader economic and social implications.

A comprehensive assessment of the costs and benefits of cybersecurity should therefore include the entire ecosystem of players including:

- Users (individuals, households, and businesses large, small and micro)
- Private-sector organizations involved in e-commerce (online merchants, financial services, insurance services, health, etc.)
- Public-sector organizations (e.g., e-government services)
- IT infrastructure providers (software vendors, ISPs, hosting providers, registrars)
- Incident response units (computer security incident response teams, law enforcement)
- Society at large (including opportunity costs, lost efficiency gains, diminished trust and use of the Internet, etc.)
- Criminals and malevolent actors, including cybercriminals, malevolent hackers, and all those seeking to profit from undermining the security of the Internet

When assessing the impact of a particular security incident, for example, it is helpful to distinguish between these direct and indirect costs (Gordon and Loeb 2005). Direct damages are costs that are caused by a specific security breach. Indirect costs, while certainly caused by the fact that a security breach occurred, are not simply the consequence of a specific breach. Rather, they reflect more generic costs, such as the cost of measures to prevent security breaches or the cost of training personnel to adopt security practices.

Direct and indirect costs can be either explicit or implicit (Gordon and Loeb 2005). Explicit costs, such as security expenditures, are well defined and, in principle, directly visible from cost-accounting data. Implicit costs are known impacts of security breaches that often elude unambiguous measurement, although it may be possible to find proxies. Implicit costs at the level of society at large occur, for example, if security problems slow down the adoption of online services by market players and end users, thus retarding society-wide benefits extending from use of the Internet.

Based on this categorization, different specific costs can be identified. Table 1 summarizes main cost categories as well as the main actors that are affected. Using this framework, systematic assessments of the total cost of cybersecurity can be put together in a step-by-step process. Individual steps are repeated until all cost categories have been scrutinized as to whether they are relevant for each of the actors and, if they are, the magnitude of the direct, indirect, or implicit impact can be estimated. Adding each type of cost across all players and cost categories yields an estimate of the total direct, the total indirect, and the total implicit costs.

Table 1: A Basic Framework for Assessing the Costs of Security Incidents*

Market players / *Damage from security incidents*	End users		E-Commerce companies	Infrastructure				Incident response and law enforcement		Society at large
	Home	Business		Software vendors	ISPs	Hosting providers	Registrars	CSIRTs	Law enforcement	
Repair cost	x	x								
Cost of lost productivity	x	x								
Revenue loss		x	x							
Cost of data loss	x	x								
Cost of confidentiality breach	x	x								
Revenue losses related to reputation effects		x	x	x	x	x	x			
Cost of security measures	x	x	x	x	x	x	x			
Cost of infrastructure		x	x		x	x				
Cost of fraud	x	x	x							
Cost of patch development and deployment	x	x		x						
Cost of customer support					x	x	x			
Cost of abuse management					x	x	x			
Collateral cost of security countermeasures	x	x			x	x	x			
Cost of investigation at the organizational level								x		
Cost of law enforcement									x	
Cost of slower ICT adoption										x
Cost of slower ICT innovation										x

**Source*: Van Eeten, Bauer and Tabatabaie (2009).

Recent research has found an interesting relationship between increasing connectivity and threats to information security. As connectivity in a country increases, problems with cybersecurity initially increase. However, this is not linear. As adoption rates further increase, this trend is reversed and security performance increases again (Burt et al. 2014). This observation highlights the challenges faced by developing countries. At the same time, as capacity building and education as well as enlightened policies are important factors in reversing the trend, these findings also offer encouragement and a way forward, as things might get worse before they get better.

(Dis)Incentive Structures across the Multiple Stakeholders

The distributed costs and benefits of cybersecurity can create major incentives for some users to engage in malevolent activities, such as phishing. A malevolent site might try many (20 or more) times to get access to a particular computer, such as through phishing. In contrast, the incentives are relatively low for many users, leading them to lack caution now and then in seeing a suspicious email or message.

Understanding the Diversity of Incentives

The multiplicity of motives across users needs to be considered in understanding their behavior. For example, the motivations of hackers vary widely, from "white hat" hackers (mainly motivated by beneficial goals), and "black hat" hackers (i.e., mainly motivated by malevolent motives). Just as the Internet has tended to democratize access to information, it has also tended to democratize

some criminal activities by making it easier for non-computer experts to use the Internet to commit crimes, such as fraud, leading some to talk about the "democratization of cybercrime."[19]

For example, "white hat" hackers may be engaged to attack systems with the aim of making them safer, or to hold organizations more accountable, such as by exposing fraud. Governments may have an interest in keeping vulnerabilities to be able to penetrate systems operated by adversaries, an example of how cybersecurity can be in tension with national security, as shown by the continuing controversies over encryption. In this interaction, efforts to secure systems and devices and educate users to adopt safe online behaviors are regularly undermined with new and innovative technical and social means. Reducing the threats from one generation of attack vectors may be a temporary success until new forms emerge. The threat landscape also varies in response to the deployed communication platforms and devices, and the services used by businesses and individuals, as well as the economic, legal and institutional framework of a place.

Threats have changed from a time of highly visible attacks by intruders in search of fame, glory and notoriety to largely invisible attacks driven by fraudulent and criminal motives. For a time, viruses were a main concern and email spam was a major vehicle for the dissemination of malicious code. As hardware manufacturers, software developers, ISPs, and users have adapted to these challenges, attack strategies have also changed. For example, the global spam rate, the share of spam in all email traffic, has been gradually declining from 72% in 2012 to 64% in 2014. Nevertheless, email spam and phishing continue to be major activities.

Likewise the number of emails with malicious attachments fell slightly to 3.2%.[20] However, these attacks are increasingly sophisticated and often difficult even for experienced users to detect. The main dissemination vehicles for these messages remain botnets, large assemblies of remote-controllable computers. Recent data confirm that the largest number of infected computers that are parts of botnets continue to be in the global North (United States and Europe), with South and East Asia and parts of South America (Brazil) regions with an increasing presence of infected machines (Microsoft 2014: 31).

The Political Economy of Cybersecurity[21]

One of the major reasons why efforts by multiple stakeholders to address problems of cybersecurity have not had a more sustained impact has to do with the particular "problem structure" of information security challenges (Asghari, Van Eeten and Bauer, forthcoming). The Internet is a dense network with numerous technological and economical interdependencies between key players. Information security has strong public-good characteristics in that its benefits accrue to the community of users at large. Both costs and benefits often affect multiple players without market transactions to compensate for them. In other words, information security is typically

[19] See a blog by this title by Frank Ip: http://blog.blacklotus.net/2015/02/the-democratization-of-cybercrime.html [Last accessed April 9, 2015].
[20] See "Worldwide spam rate falls 2.5 percent but new tactics emerge", http://www.zdnet.com/article/worldwide-spam-rate-falls-2-5-percent-but-new-tactics-emerge/#! [Last accessed May 28, 2015]; and "2014 Estimated Global Email Spam Rate is 64%. That's Almost 2 Out of 3 Emails!" http://www.business2community.com/email-marketing/2014-estimated-global-email-spam-rate-64-thats-almost-2-3-emails-0875585 [Last accessed May 28, 2015].
[21] This section relies heavily on the research reported in Van Eeten et al. (2010) and Van Eeten and Bauer (2013).

afflicted with positive and negative externalities. Furthermore, markets for security as well as markets for many media and information services suffer from problems of incomplete and asymmetrically distributed information. Users are often not in a position to evaluate the security performance of an ISP, a device, software, or an application. The exact nature of how externalities and information asymmetries affect security varies depending on the type of security risk, the nature of attacks, and the best defenses.

For instance, take the case of untargeted attacks. If a user forgoes investment in security software for an Internet-connected device and this machine becomes infected, this may affect the performance of the device, but the main cost of security incidents will be borne by others to whom the machine sends malware. Hence, an unprotected or under-protected user causes a negative externality for others. If, on the other hand, a user invests in cybersecurity, some of the benefits will accrue to other users, whose machines will be less likely to be infected. The user causes a positive externality. Because only part of the costs associated with a negative externality are borne by the user causing it and only part of the benefits of a positive externality are enjoyed by the user causing it, decentralized decision-making by individual users will systematically not reflect these broader spillover effects on the larger ecosystem.

The opposite is true for targeted attacks. An organization fortifying its defenses against targeted attacks inadvertently exerts a negative externality on other organizations that did not undertake similar security measures and consequently face a higher risk of an attack.

An increasing volume of research argues that many cybersecurity problems are caused by misaligned incentive structures, which (dis)incentivize individual actors and therefore, given these interdependencies, result in greater security problems for all. Literally all participants in the Internet ecosystem work under mixed incentives, some contributing to enhanced security efforts, other weakening them. The net effect of these conflicting forces is often ambiguous, but they need to be the focus of study. The following paragraphs briefly illustrate the key incentives for important players in the Internet ecosystem.

Hardware Vendors

Hardware manufacturers operate in a highly competitive marketplace. Testing hardware and its components for possible vulnerabilities may increase time to market and, in the presence of first-mover advantages and network effects, delay could result in lasting disadvantages. At the same time, equipment manufacturers need to be concerned about their reputation. The first factor reduces attention to security and the second increases it, at least if reputation is also dependent on security performance. If reputation effects are stronger, the net effect will be increased security. However, if time to market pressure is stronger, security performance may be harmed.

There are several ways to overcome this dilemma, many of them requiring some coordinated action. For example, secure equipment design practices could be adopted and certified by an industry body. Also, government bodies could establish minimal standards for equipment, or for liability rules that will expose manufacturers with poor security practices to lawsuits and greater claims for compensation.

Another vulnerability introduced into the Internet ecosystem is the practice of bundling hardware with trial security and other software. Since a large number of users do not renew the subscription to their security software after the initial trial period, this could be a time bomb for the user. Changing the default to automatic renewal, as some vendors have done, would make a big difference, and some vendors have done this. Similarly, software that comes preinstalled may become a vulnerability if it is not regularly updated with security patches. For years, Microsoft's default setting was to turn off auto updates. The simple change to turn on automatic updates made a noticeable difference. However, this strategy is not without risks. For example, in the application of a large number of updates by multiple hardware (and software) providers, it is possible that updates might be compromised and thereby introduce new security risks.

Software Vendors

Like hardware vendors, software vendors work under ambiguous incentive structures. The cost and time (time to market) of software testing constitutes a potentially security-reducing factor. The user's desire for high levels of functionality, compatibility, and discretion often comes at the cost of security features. Moreover, software licensing agreements that contain hold-harmless clauses shield the vendor from any legal action and hence, all other things being equal, weaken the incentive for software vendors to invest in security.

On the other hand, flawed software will require security patching. As typically multiple versions of software are installed, such patching can be costly for the vendor and the user. This increases the incentive of vendors to bolster security in the first instance. (On the user side, the cost and disruption caused by updating and patching software may actually cause additional delays in implementation.) Potential loss of reputation and brand damage work in the same direction of increasing the incentives to design secure software. While reputation effects may only work slowly, they do work, as the transition from Windows XP to Windows XP Service Pack 2, and subsequent operating systems demonstrates.

Software is developed in a diverse range of institutional forms, from commercial enterprises to peer production to individual amateur programmers. The free and open software movement has greatly expanded the availability of software, plugins and applications. In particular, application markets have greatly expanded the scope of participants in the development of software. While this has been a major source of innovation, and created a potential for more decentralized and competitive software development, not all apps, plugins and programs are developed with security in mind, thus opening a new source of potential security risks.

Internet Service Providers (ISPs)

ISPs are key players in the Internet ecosystem, with numerous options to enhance information security. In a detailed analysis of a vast spam database that provided clues to the location of infected machines, Van Eeten and Bauer (2008) found that 50 ISPs globally hosted 60% of the machines that originated spam, a pattern that has not changed much over time. Furthermore, the study found considerable differences in the security performance of these ISPs, often in the range of one or two orders of magnitude, even within one country. This evidence suggests that ISPs do have the means to improve their security performance and that they are important choke points

that could contribute to reducing problems of spam and other more serious types of cybercrime and cybersecurity.

However, ISPs also operate under mixed incentives. Several security-enhancing incentives exist, although their effectiveness is mediated by the business model of ISPs. Commercial ISPs will take security into account when it affects their revenue stream and bottom line. This is vividly illustrated by the example of viruses and spam. Early on, ISPs argued that emails were the personal property of recipients and that an inspection of the content of mails was a violation of privacy. Consequently, the responsibility for protecting their own machines and for dealing with spam was placed in the hands of end users. With the exorbitant growth of spam, which in the second decade of the twenty-first century, constitutes nearly two-thirds of all emails, the financial implications for ISPs also changed. Not only did the flood of spam become a burden for network infrastructure that would have required additional investment to cope with, but also the malware imported onto the network had indirect effects on the ISP's costs. Users of infected machines started to call the help desk or customer service at a fairly high cost per call to the ISP. Malicious traffic sent from infected machines triggered abuse notifications from other ISPs and requests to fix the problem, typically requiring even more expensive outgoing calls to customers. In extreme cases, the whole ISP could be blacklisted, causing potentially serious customer relations and reputation problems. Facing this altered economic reality, ISPs reversed their stance with little fanfare and started to filter incoming mail (about 40–65% of all incoming traffic is filtered out), and to manage their customers' security more proactively, while normally giving users more control over levels of spam filtering.

Now, in 2015, ISPs operate under several more or less potent incentives. Costs of customer support and abuse management, as well as the cost of additional infrastructure that might be required to handle malicious traffic, all have an immediate effect on the bottom line and have increased their incentives to undertake security-enhancing measures. Loss of reputation and brand damage work indirectly (and probably work more slowly) but exert pressure in the same direction. ISPs are embedded in an interdependent system of service providers. If contacts via the abuse management desk are ineffective, other ISPs have a range of escalating options to retaliate for poor security practices with regard to outgoing malicious traffic, even if the origin is an individual user.

For example, blacklists are regularly used by ISPs to filter and block incoming traffic. Substantial presence on one or more of these lists, reflected in the listing of many IP addresses belonging to an ISP for an extended time period, will drive up customer support and abuse management costs because, for example, emails originating from blacklisted ISPs may not be delivered, resulting in customer dissatisfaction and complaints. It may also trigger subsequent reputation and revenue losses for an ISP. Both effects create an incentive to improve security measures, and at the very least, to respond in a timely fashion to abuse requests. In extreme cases, an entire ISP (and not just IP addresses or address ranges) may be blocked by blacklists and de-peered by other ISPs, raising the costs of this ISP significantly, possibly to the point where its business model becomes unsustainable.

However, in contrast to these security-enhancing incentives, the costs of increasing security, legal provisions that shield ISPs from legal liability, and the costs of customer acquisition, all work in the opposite direction. Other things equal, they constitute incentives to adopt a lower level of information security. The net effect on ISPs is hence dependent on the relative strength of the components of this web of incentives. The high cost of customer calls (typically in the range of

the cost of a monthly subscription), while providing an incentive to find alternative solutions to enhance the security of end users, also may provide an incentive to ignore individual cases that have not triggered notifications to blacklisting services or abuse requests from other ISPs. Most ISPs estimate that only a small percentage of the infected machines on their network show up in abuse notifications.

Considerable technical advances and declining costs of security technology, on the other hand, have enabled ISPs to move their intervention points closer to the edges of their network and thus automate many functions in a more cost-effective way. In an escalating response, machines on the network may initially be quarantined with instructions to the user to undertake certain measures to fix a problem. Only in cases that cannot be solved in this fashion may customer calls become necessary. Overall, while the interdependencies among ISPs result in the internalization of some of the external effects, this internalization is partial at best. Hence, it is likely that the highly decentralized system of decision-making yields effort levels that, while higher than often assumed, nevertheless fall short of a social optimum.

Users

Large businesses (firms with 250 and more employees) are a heterogeneous group. Many large business users have adopted risk assessment tools to make security decisions. The diligence they exercise will vary with their size and other factors, such as the specific products and services provided. Their scale enables them to have a greater capacity of cybersecurity.

Other groups of actors that deserve even more focus, given their relative lack of scale, are small and medium enterprises (SMEs, typically defined as enterprises with fewer than 250 employees, and also micro-enterprises) and residential users. Although this is a large and diverse group, these players have some important similarities.

Like other participants, they work under multiple and potentially conflicting incentives. Unlike larger businesses that may be able to employ information-security specialists, either in-house or via outsourced services, many SMEs, micro-businesses, and residential users have insufficient resources to create a cybersecurity capacity to prevent or respond to sophisticated types of attacks. Whereas awareness of security threats has increased, there is mounting evidence that many households and individual residential users underestimate their exposure and overestimate their efficacy in dealing with these risks.

Although these constitute similarities between SMEs and residential users there are also differences. In general, one can assume that businesses employ a more deliberate, instrumentally rational form of reasoning when making security decisions. But this is not always the case. For example, many small businesses are not even online, preventing them from enjoying the benefits or the risks of Internet access. However, in both cases, for those users online, the benefits of security expenses will flow largely to other users.

Individual businesses and users may suffer from the perception that their own risk exposure is low, especially if other users protect their machines—the well-known “free rider” phenomenon. On the other hand, given increased information, a growing number of users in this category are aware of the risks of information security breaches. Thus, they realize to a certain extent that they are the

recipients of ‘‘incoming’’ externalities. Overall, one can expect that on average these classes of users will not be fully fledged free riders and will invest at some level in security. Whereas some individuals and SMEs may over-invest, there is evidence that most will not invest in security at the level required by the costs of information security breaches. This rational expectation is corroborated by the observation that many individual users do not purchase security services, do not even use them when offered for free by an ISP or a software vendor, and often turn off their firewalls and virus scanners regularly if they slow down certain uses, such as gaming.

Governments

Governments and government agencies are, in principle, actors who could align these incentives of different actors by developing effective policies. For example, the recent experience with "Cyber Essentials,"[22] a policy adopted in the UK that incentivizes contractors who wish to work on government contracts to implement certain minimal security practices, suggests that such policies for contracting can contribute to security improvements. Likewise, the theoretical literature on security economics suggests that hybrid policies combining minimal security standards with liability rules for both vendors and users yield better security outcomes. Yet governments are not always the neutral and beneficial actor they could be. For example, government agencies are the largest purchasers of "zero day exploits"—vulnerabilities of software, for example, that are not yet known to the vendor—as it enables them to gain access to the strategic assets of rival forces.[23] Hence, conflicts of interest may exist within secret service organizations, the military and other government organizations that result in uneasy tensions and ambiguous overall incentives.

The Diverse Attitudes, Beliefs and Practices of Users

The worldwide diffusion of the Internet along with the rise of social media and other applications can put more communicative power in the hands of users. At the same time, this widely distributed empowerment means that the user is a new and major dimension of cybersecurity. Increasingly, those designing cybersecurity initiatives need to ask:

1. Are users aware of risks to their privacy and security online?

2. Have concerns over privacy and security online undermined the user's trust in using the Internet for governmental, commercial and social purposes?

3. Do users take such threats seriously, and know what actions can be taken to protect themselves?

4. Do users take reasonable actions to protect themselves online, and if not, can they acquire a more appropriate cybersecurity mindset?

Based on surveys of users conducted online by the Oxford Internet Institute in collaboration with ComScore and the World Economic Forum (Dutta et al. 2011; Dutton et al. 2014), there is some

[22] https://www.gov.uk/government/publications/cyber-essentials-scheme-overview [Last accessed May 17, 2015].
[23] http://www.pctools.com/security-news/zero-day-vulnerability/ [Last accessed May 17, 2015].

evidence to address these questions, but a need for more systematic and longitudinal data to track what is a very dynamic area.

Awareness: Concern over Privacy and Security

Most Internet users are aware of privacy and security issues, but awareness is far from universal and requires more of a focus by all providers and government and industry as a whole. Cybersecurity is far from a universal "mindset" that might be the ultimate goal for a secure Internet community (Dutton 2014), where users do not need to consider each action to protect their security online, since it becomes routinized as part of their everyday life and work.

Most users believe that their privacy and security are at risk online, but many do not. At a general level, 61% of users believe that the Internet puts their privacy at risk. Two aspects of this belief are, first, that over two-thirds (67%) of users we surveyed believe that, on the Internet, organizations ask for too much information. Most users also believe that information about them is collected on the Internet and used for reasons that they do not know. And most believe that people they do not know have access to personal information about them through the Internet. Likewise, nearly as many (63%) indicate that they are concerned about being monitored online, with 50% believing that the government monitors what people do on the Internet (Table 2). While this data is recent, it is pre-Snowden, and therefore concerns are likely to have risen since it was collected.

Table 2. Beliefs and Attitudes of Users*

Item	***Percent of Users***
Organizations, companies ask for too much personal information online	67
People who go online put their privacy at risk	61
There is personal information about me that is collected on the Internet for reasons I do not know	58
People I do not know have access to my online personal information	57
The government monitors what people do on the Internet	50

*N = 8,793. Adapted from Dutton et al. (2014).

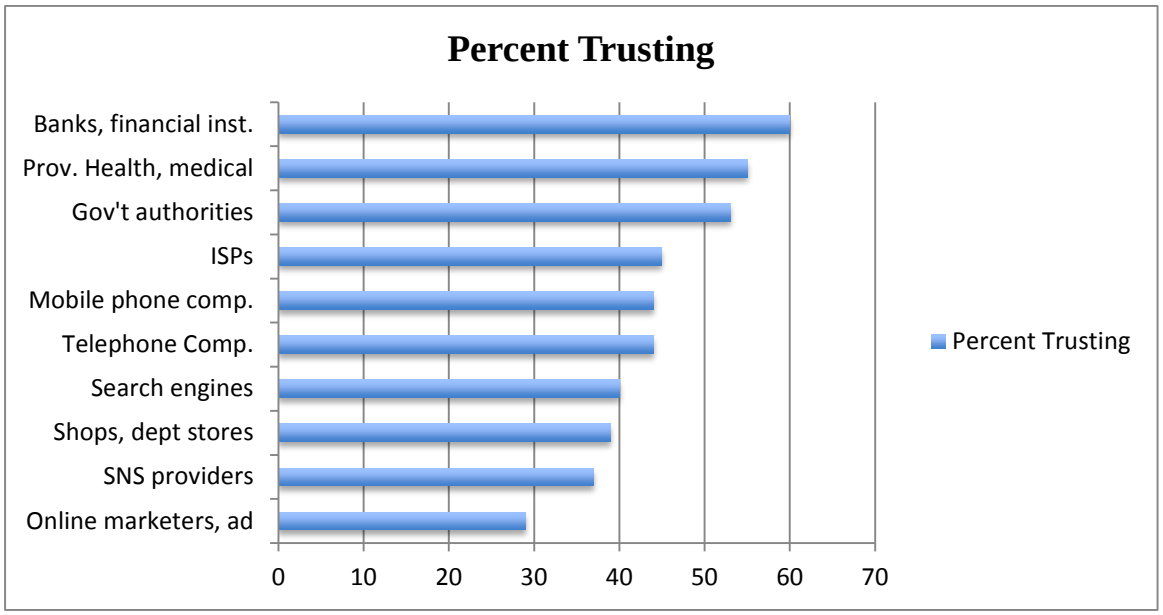
These concerns are spread worldwide, but in general, users in emerging nations are somewhat less aware of risks, and commensurably somewhat more trusting in the online environment (Dutton et al. 2014). This could be a function of being more recent users, and therefore experiencing fewer problems, or of being less often the focus of malevolent users, who are likely to focus more on users from more developed nations and regions. Some maps of the flow of attacks, for example, suggest that the United States and other developed nations are more often the target.[24]

[24] While measurement of such patterns are a focus of controversy, one dramatic mapping project includes the NORSE dynamic map: http://map.ipviking.com [last accessed May 28, 2015].

Undermining Trust in the Internet and Institutions

There is some evidence from our surveys of users that we might well be within an Internet "trust bubble" that could undermine use of the Internet in many contexts (Dutton et al. 2014). Of course, trust in the Internet is also a matter of trust across different institutions, from governments, ISPs, commercial enterprises, and SMEs. Our global survey found that banks and financial institutions, health and medical organizations, and governmental authorities are among the most trusted in protecting personal data (Figure 1). The ICT industries, including ISPs, mobile and telecommunication companies, are somewhat less trusted, and search engines are even somewhat less trusted, about the same as shops and department stores, and social media platforms. The least trusted in caring for personal data are online marketing and advertising firms (Figure 1).

Figure 1. Trust in Different Institutions for Protecting Personal Data



As with privacy, there are also widespread beliefs and attitudes that indicate that users are wary of their security online. While nearly two-thirds of users believe they "have control over information" they disclose about themselves online, less than half (45%) believe that the information they put online is "kept safe" and even fewer (41%) "feel safe providing some personal information" on the Internet (Table 3).

Table 3. Beliefs and Attitudes of Users about their Security Online

Item	***Percent of Users***
I have control over the information I disclose about myself online (62%)	62
The personal information I put online is kept safe	45
I feel safe providing some personal information such as my name, birth date, or phone number on the Internet	41

Translating Security Concerns to Actions

The protection of personal information is only one of a number of concerns individual users have about their online security. Almost three-fourths (72%) of users say they are concerned about "someone breaking into" their Internet or email account (Table 4). More than two-thirds (67%) are concerned about information that they provide online for one designated purpose being used for another purpose (Table 4).

Table 4. Security Concerns and Practices

Item	*Percent of Users*
Concerns about Online Security	
Someone breaking into your Internet account or email	72
Information you provided for one purpose is being used for another purpose online	67
Cyber Security Practices	
Scan your computer or mobile devices for viruses or spyware	65
Check your privacy and security settings online	54
Read privacy policies before using a website or service	41

Despite these concerns, many users do not demonstrate great concern in their actual security practices. Only two-thirds of users say they scan their computer or mobile devices for viruses or spyware (Table 4). Just over half (54%) of users say they check their privacy and security settings online (Table 4). Only 41% of users say they "read privacy policies before using a website or service" (Table 4).

What Can Be Done?

There is a clear need for more awareness campaigns in the area of cybersecurity, and such campaigns need to provide information about how users can protect their security, and not simply focus on creating a fear of the Internet and its use. It is clear than learning and education around the Internet and social media are key priorities for moving forward.

However, what appears to be a lack of adequate security practices cannot be attributed solely to an absence of concern, as shown above. This might well be a function of the poor design of security online, such as not being well tailored to the general user. Rather than blame users for not following safe practices online, it is important to look to computer science and software design to develop more user-friendly applications to enable users to protect themselves. For example, creating dozens of complex passwords, memorizing them, and changing each periodically is simply not feasible for average users.

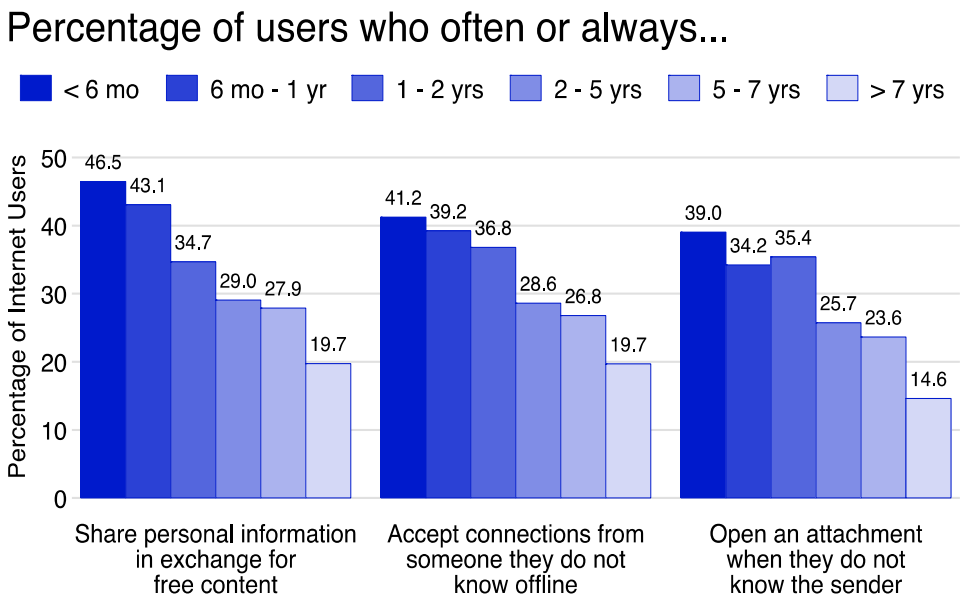
However, there is some evidence that being online for a time enables individuals to learn more about secure practices. For instance, you can see from the international data that newer Internet

users are less likely to engage in secure practices online (Figure 2). Those with less experience online are more likely, for example, to share personal information in exchange for free content, accept connections from someone they do not know, and open an attachment when they do not know the sender (Figure 2). Internet users learn from experience and their mistakes, but it would be far better to enable users to learn more quickly to avoid the problems they are likely to encounter if they do not follow some simple and reasonable practices.

The New Agenda for the New Cybersecurity Landscape

The theme running through our review of the social and economic aspects of cybersecurity is the need of a wider array of actors to reconsider approaches to achieving greater cybersecurity. The context, shaped by the growing significance of the Internet and the rise of a New Internet World, requires it. Conventional approaches evolving from the era of mainframe, and then personal computers, were dominated by the computer-security technical community and relatively centralized in the computer-support teams of governments, business and industry, and service providers, such as banks. The twenty-first century Internet has put users increasingly at the center of approaches to cybersecurity, while the role of the computer expert is being limited by their understanding of users.

Figure 2. Newer Internet Users More Frequently Engage in Less Secure Practices



World Internet Values Survey 2013: N(10,857), N(10,940), N(10,915), respectively.

Internet users are diverse and might have overly simplistic or even erroneous mental models about secure and insecure behaviors online, but these must be understood by the security community, such as network operators, who are another key actor in increasing security (Wash and Rader 2011). Likewise, app designers and software developers play a critical role but often do not follow secure design practices, or understand the knowledge and practices of their users. Developing approaches are being organized in the Internet age of decentralized, user-centric computing, where the role of

computer experts is increasingly limited and the role of the user and a wide array of other actors is greatly expanded in the new Internet ecosystem.

In light of such developments, there are new ways to address the rising challenges facing cybersecurity by focusing more on the economic and social dimensions of the problems. These will include:

- understanding of the role of a multiplicity of users in the new Internet landscape;
- knowing more about the real and perceived costs and benefits shaping the behavior of these actors;
- mapping the incentive structure underpinning responses to cybersecurity in ways that can guide policy initiatives designed to restructure incentives; and
- describing the attitudes, beliefs and practices of users to enable software and systems for cybersecurity to be designed to be in sync with user expectations and behavior.

More generally, this review suggests a set of topics that should rise on the cybersecurity agenda. The new agenda will include:

Cybersecurity Capacity Building

At every level—nation, organization, and individual—there is a need to build a capacity to maintain security online. The elements of cybersecurity capacity-building are being identified through a number of projects and collaborative efforts, such as the Oxford Cybersecurity Capacity Building Model. This group advocates an approach at multiple levels, including the use of technologies to control risks; building cyber skills, from the workforce to leadership; creating effective legal and regulatory frameworks, including cyber policies and defenses; and encouraging responsible cyber culture within society.[25]

For example, there is a growing recognition of a lack of cybersecurity expertise. Many computer science departments in North America and Western Europe have had a cybersecurity or computer security program in place for years, and an increasing number of courses are focused on this issue. However, there remains a skills gap in most nations, a clear need to grow the numbers of cybersecurity experts worldwide, and a need to expand curricula to include a greater focus on users and the social and economic aspects of cybersecurity.

Similarly, the size of corporate and other organizational budgets directed to cybersecurity is generally insufficient. Not only is this function viewed too often as a low priority, it can sometimes be seen as a threat to the core business of the organization, and viewed as the "business prevention unit,"[26] There is a clear need to change the image of cybersecurity as it increasingly becomes a key aspect of a corporation or organization's reputation.

[25] These dimensions are described in detail on the project website at: http://www.oxfordmartin.ox.ac.uk/cybersecurity/dimensions/ [Last accessed May 28, 2015].
[26] A point made by a cybersecurity expert at a conference for which we cannot attribute the quote.

More Realistic User-centered Designs for Security

Instead of blaming users for not adhering to impossible guidelines on the protection of systems, such as the memorization of multiple passwords, etc., systems need to be designed in ways that users can better manage. Users, from students to retired persons, are seldom interested in cybersecurity per se. They want to get their job done online, whether that is listening to music, filing taxes, or contacting their family. If they have to deal with security, then they want something convenient, simple, easy to use, and that works everywhere. This goal might well be impossible to meet in its entirety, but that is the direction that designs should move towards.

Of course, each of these criteria involve judgment calls, and that judgment would vary across users. What is simple to one person is not necessarily simple to another. However, a number of innovations in security have tended to add complexity, such as Transport Layer Security/Secure Sockets Layer (TSL/SSL)[27] and Europay, MasterCard, and Visa (EMV) chip cards.[28] In contrast, fingerprint scanners are gaining a level of accuracy that might make them acceptable for a variety of authentication devices, such as in their use for mobile phones. Compared to passwords, for example, such biometric devices could be more practical for users by being convenient, easy and capable of working on multiple devices, but as noted in this report, they will raise new risks to identity theft and are therefore not likely to be the solution in the longer run. Most generally, more work needs to focus on human–computer interaction that is focused on the security area and that entails behavioral research on what users actually do.

Learning and Education: Moving From Fostering Fear to Educating Users

Cybersecurity initiatives have often had a public awareness component. However, these are most often focused on frightening individuals into being more protective of their security online. Fear campaigns do not generally work, in part because they do not give clear and practical instructions on what to do. This is difficult because there are only a few conventional strategies for users to follow (Box 4). Moreover, they might well have negative consequences, such as undermining trust in using the Internet for social and commercial activities, which could undermine use of the Internet generally, or differentially, leading to increasingly digital divides as users at the margins, such as the elderly, might be frightened, while more experienced users remain confident.

Box 4. Strategies Users Can Adopt to Protect their Security Online

- installing firewalls
- using strong passwords
- updating passwords, force 90-day password resetting
- mask passwords
- installing and running anti-virus software
- employing SPAM filters
- setting SPAM filters at appropriate levels

[27] https://technet.microsoft.com/en-us/library/cc783349(v=ws.10).aspx [Last accessed May 28, 2015].
[28] http://en.wikipedia.org/wiki/EMV [Last accessed May 28, 2015].

- replacing default setting on WiFi with strong passwords
- updating operating systems

A more effective approach would involve learning and education that is targeted on specific kinds of security risks, such as how to recognize a phishing attempt, and on providing information that helps users decide what to do, such as not opening an attachment sent by a stranger. Canada has a very well-designed 'Get Cyber Safe' campaign on the Web, Facebook and Twitter, including easy tips for 'protecting yourself', "your family," "your identity," money, devices, and "yourself while traveling."[29]

Of course, creating a useful trusted site can lead malevolent actors to pose as this site, such as your bank, leading the Canadian site to post a warning to users: "Beware of callers falsely claiming to represent Public Safety Canada or the Canadian Cyber Incident Response Centre (CCIRC)."[30] Similarly, the US Homeland Security Department has a "Stop.Think.Connect" site with useful information for users.[31] But having a web page of suggestions is not enough as there needs to be a continuously updated and creative information campaign to educate users across all age groups.

In addition, it is important to find ways to move beyond "campaigns" to make cybersecurity an essential part of more basic and lifelong learning and education. We teach people how to write, create a letter, speak to a group, but seldom train children and others to use email, social media and related technologies in a safe, ethical and appropriate way. Learning how to use the Internet in ways that are appropriate, that reduce potential harm to others, and respect the dignity of other users needs to be a central part of educational programs across the life span. Some risks tied to social media, such as cyber bullying and sexting require users to identify and understand potential risks and how to minimize them. All aspects of cybersecurity should be incorporated in this lifelong learning about the appropriate and safe use of the Internet and related ICTs. Often these lessons are best if kept simple: 'Don't talk to bad people.' 'Respect others.' 'Don't open things you don't trust.'

Ideally, learning and education, reinforced by social norms and pressures, could lead to the development of a 'cybersecurity mindset' (Dutton 2014). Just as individuals in some neighborhoods and communities get in the practice of locking their doors when they leave their households, or securing their bicycle when parking it in pubic, computer users might well develop a mindset that makes security an aspect of what they do without thinking about it each and every time. This is a cultural change, but it is possible and will be made easier if security is better designed for users.

In addition to individual users, such education and learning is increasingly important for small and medium and mico enterprise (SMME) businesses. A very large proportion of businesses fall into this category and their use of the Internet and online commerce is critical to economic development. Providing them with a genuinely stronger sense of security and an understanding of how to protect

[29] http://www.getcybersafe.gc.ca/index-en.aspx [Last accessed April 9, 2015]
[30] Message appearing when accessed on April 9, 2015.
[31] http://www.stcguide.com [Last accessed May 28, 2015].

themselves in the cybersecurity area could be a critical role of national and international organizations.

Restructuring Incentives

Some actors in the cybersecurity ecosystem have strong incentives. One recent claim cited the observation that 20 or more targeted emails are often sent for a malevolent actor to obtain access to a computer. Spammers have real financial incentives (Krebs 2014). An analogy is the telemarketer, who might get a positive response from a very small percentage of those receiving a marketing message, but given the low cost of reaching this market and the value of sales, the effort is highly profitable. Likewise, many spammers continue because of the economic incentives behind their activities. Of course, the IT team charged with protecting computer security is also incentivized as their jobs might be on the line.

However, as outlined in this paper, many actors in the ecology of the Internet do not have strong incentives to prioritize cybersecurity or they demand that others in the value network provide security (e.g., network operators argue users are responsible; users argue the opposite). Too often, the costs of a lack of security are externalized, as individuals perceive others to benefit and others paying the costs, such as their bank, or credit card Company, or society at large.

Also, experience often beats rational concerns. Our own research has found that the Internet is an "experience technology" (Dutton and Shepherd 2006; Blank and Dutton 2011). Users trust the Internet more as they gain experience with it. Nevertheless, bad experiences online can reduce that trust (Blank and Dutton 2011), and there is evidence of growing concerns over privacy and surveillance that could erode trust in the Internet (Dutton et al. 2014).

New mechanisms, such as cybersecurity insurance, need to be devised to restructure these incentives in order to lead more actors to see a stake in protecting their own cybersecurity. Insurance, for example, would make users more accountable for their security, such as if their premiums were dependent on their ability to protect themselves, creating an incentive for good behavior. There might be other incentives, beyond saving or losing money, such as the loss of a service tied to insecure practices, such as being forced to update a password in order to restore an email service. All of these strategies have potential risks, such as undermining the marginal users, and deepening the digital divide, but ways to restructure the incentives underpinning cybersecurity are critical to explore.

Making Cybersecurity an Aspect of Local and Global Internet Governance

Cybersecurity cannot be achieved unless policy and practice can be increasingly global. This is a cultural as well as a governance challenge in that nations do not place the same priority on key values and interests and practices, such as the importance of anonymity. There need to be venues for resolving these cultural differences and coordinating international responses.

Some moves toward "data localization" could be restrictive and undermine the benefits of a global Internet (Bauer et al. 2014), but some could also enable more flexibility locally and internationally. For example, the Internet does not require all nations to move to some lowest common denominator. For example, banks sometimes need to ensure their government and customers that they are subject to a particular regulatory regime, and therefore contract their cloud services in

ways to keep their data within their national boundaries. Governments might also localize some services that enable features that other jurisdictions might not allow, such as the right to anonymity for political speech. Rather than treat all data and information in the same ways, the Internet has tremendous malleability that would enable creative solutions to addressing local and international issues of privacy, freedom of expression and cybersecurity.

Balancing Cybersecurity with the Broader Ecology of Internet Policy Choices

It is impossible to deal with cybersecurity as a single issue when it is tied to many related issues in a broad ecology of policy choices, such as around privacy, surveillance and freedom of expression. Most stakeholders want to promote a global, open and secure Internet, but not only a secure Internet. A myopic focus on cybersecurity could undermine other values and interests. You can imagine the universities where the IT officers would prefer not to allow wireless access. Such a solution would be ridiculous and would undermine the use of perhaps the world's leading technology for informal education.

As has been mentioned, in some businesses, the IT security team has been jokingly referred to as the "business prevention unit," illustrating the degree that cybersecurity can be blind to the core missions of a company or other organization. This means that the mission and expertise of cybersecurity experts must be increasingly balanced by the goals and expertise of those with other roles and other types of expertise in law, policy and use of the Internet and related media. Some major online commercial enterprises, for example, have been able to provide easy access for online shopping and secure payments, in relatively easy to use and reliable ways.

In addition, the case must be more clearly made that cybersecurity is becoming a requirement or necessary condition to protect privacy, for example, as well as the financial vitality and reputation of a business. More often than not, cybersecurity needs to be perceived as an enabler of other goals, rather than in conflict with their achievement. But this requires system designs to address the skills, attitudes and behavior of their users.

Points of Summary and Conclusion

The Internet and related ICTs are becoming increasingly central to the economic prosperity of developing and developed nations. However, the benefits of the Internet and related technologies are contingent on maintaining a level of security, trust and openness of a global Internet. While the Internet can empower individuals, organizations and nations of the developing world in an increasingly global economy, the same technology also appears equally able to empower hostile and malevolent actors, who have strong economic and social incentives to pursue their attacks. Clearly, success depends on global efforts to address the challenges to cybersecurity, and a central global question becomes: How can the world reap the huge economic and social benefits of the Internet while at the same time ensuring its security?

There is no solution to cybersecurity—no *Deus Ex Machina* on the horizon. It is a constantly moving target that will entail a continually evolving set of processes to contain the security risks associated with the use of the Internet and related digital media. Moving forward on the development of these processes will inevitably be a matter of incrementally adapting and

improving existing approaches. In organizations, this is often called muddling through, rather than seeking to find a rational-comprehensive solution or silver bullet.

There are too many actors and security problems across the globe, and across platforms, for there to be a neat, one-size-fits-all global solution to cybersecurity. Given the dynamic nature and complexity of progressing this area, there is a need to accept a long-term process of incremental decisions that enable actors to muddle through to find better solutions over time. However, this paper has pointed to directions for moving current approaches to cybersecurity, such as revitalizing public-awareness campaigns by focusing on providing tips for addressing problems rather than generating fear on the part of users. These approaches suggest a new agenda for a changing cybersecurity landscape.

The economic and social potential of the Internet is great for all nations—developing and developed alike. Increasingly, however, these benefits are at risk of failing in light of risks tied to the lack of security and falling levels of trust in the Internet and those who manage and exploit this technology around the world. Elsewhere, the authors have asked if we are in an Internet "trust bubble" (Dutton et al. 2014).

However, there are clear ways in which cybersecurity can be better approached once we recognize the new aspects of cybersecurity in the digitally connected world, and the centrality of users in this new ecology of choices shaping the future of the Internet.

Appendix

Online Survey Data

The survey data presented in this report derives from a 2012 survey that was part of the Internet Values Project (IVP), for which Bill Dutton was the principal investigator. The 2012 survey built on an earlier 2010 survey by the project team.

Survey questions were based upon a collection of well-known Internet surveys including the World Internet Project (WIP),[32] the OxIS Surveys,[33] the Pew Internet and American Life Project,[34] comScore[35] and the BBC World Service Internet poll.[36] IVP researchers reworked the original IVP survey with teams from the World Economic Forum, removing certain questions that yielded little variance and refining others to gain more precision. New questions were also added to measure the most relevant themes of today.

The survey was conducted online almost simultaneously by comScore and Toluna, two world-leading market research firms, between July and September 2012. Toluna focused on collecting

[32] http://www.worldinternetproject.net [Last accessed May 28, 2015].
[33] http://microsites.oii.ox.ac.uk/oxis/ [Last accessed May 28, 2015].
[34] http://pewinternet.org [Last accessed May 28, 2015].
[35] http://www.comscore.com [Last accessed May 28, 2015].
[36] BBC (2010) "Four in Five Regard Internet Access as a Fundamental Right: Global Poll," *BBC News*, http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/08_03_10_BBC_internet_ poll.pdf <This link couldn't be found>

data from the Middle East and North Africa (MENA) region while comScore focused on collecting data from other regions of the world. The online questionnaire was programmed to randomize questions, force answers and to minimize non-response biases. “Don’t know” answers were treated as missing data.

A total of 11,225 cases were retained from users in 63 countries by combining the data collected from both firms. The survey was conducted in nine languages: Arabic, English, French, German, Italian, Japanese, Korean, Simplified Chinese, and Spanish, both Iberian and Latin American.

Samples aimed to represent online Internet populations and not the general population. Only countries with sample sizes of more than three hundred were retained for country-level analysis (in comparison with an earlier 2010 survey, in which countries with samples of more than 200 were retained). This meant that 20 countries could be analyzed individually—Argentina, Australia, Brazil, Canada, China, Colombia, Egypt, France, Germany, India, Italy, Japan, South Korea, Mexico, Peru, Saudi Arabia, South Africa, Spain, the United Kingdom and the United States—seven more than in the earlier 2010 survey (Dutta et al. 2011). Overall, sampling and methodology were improved from the 2010 IVP survey; yet, new results reinforced and extended the previous findings, confirming the validity and reliability of the initial study.

More detail on the full methodology is available in the appendix of (Dutton et al. 2014), available online at http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf [Last accessed May 28, 2015].

References

Ablon, L., Libicki, M. C., and Golay, A. A., 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Santa Monica, CA: RAND National Security Research Division.

Anderson, R., and Moore, T., 2006. The Economics of Information Security, *Science*, 314, 610–13.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., Moore, T, and Savage, S., 2013, "Measuring the Cost of Cybercrime," in R. Böhme (ed.), *The Economics of Information Security and Privacy*, pp. 265–300. Berlin, Heidelberg: Springer.

Asghari, H., Van Eeten, M. J. G., and Bauer, J. M., Forthcoming. "The Economics of Cybersecurity," in J.M. Bauer and M. Latzer (eds.), *Handbook on the Economics of the Internet*, *pp. forthcoming*. Cheltenham, UK and Northampton, MA: Edward Elgar.

Bauer, J. M., Van Eeten, M. J. G., Chattopadhyay, T., and Wu, B., 2008. Financial Implications of Network Security: Malware and Spam: Report for the International Telecommunication Union (ITU), Geneva, Switzerland.

Bauer, M., Lee-Makiyama, H., van der Marel, E., and Verschelde, B., 2014, *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, ECIPE Occasional Paper, No. 3. Brussels: ECIPE. See: http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf [Last accessed May 18, 2015]

Blank, G., and Dutton, W. H., 2011. "Age and Trust in the Internet: The Centrality of Experience and Attitudes toward Technology in Britain," *Social Science Computer Review*, 30(2): 135–151.

Burt, D., Nicholas, P., Sullivan, K., and Scoles, T., 2014. *The Cybersecurity Paradox: Impact of Social, Economic, and Technological Factors on Rates of Malware*, Microsoft Security Intelligence Report.

Clark, D., Berson, T., and Lin, H. S., 2014. *At the Nexus of Cybersecurity and Public Policy*. Computer Science and Telecommunications Board, National Research Council, Washington DC: The National Academies Press.

CSIS and McAfee. 2014. *Net Losses: Estimating the Global Cost of Cybercrime*. Washington, DC: Center for Strategic and International Studies; Santa Clara, CA: Intel Security McAfee.

DeNardis, L., 2014. *The Global War for Internet Governance*. New Haven and London: Yale University Press.

Dutta, S., Dutton, W. H. and Law, G., 2011. *The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online: The Gobal Information Technology Report 2010-2011*. New York: World Economic Forum, April. Available at SSRN: http://ssrn.com/abstract=1810005.

Dutton, W. H., 2014. "Fostering a Cybersecurity Mindset," Working Paper, Global Cyber Security Capacity Centre, University of Oxford. Available on SSRN at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2490010.

Dutton, W. H. and Meadow, R. G., 1987, in K. B. Levitan, (ed.), "A Tolerance for Surveillance: American Public Opinion Concerning Privacy and Civil Liberties," *Government Infostructures* (pp. 147–70). Westport, CT: Greenwood Press.

Dutton, W. H., and Shepherd, A., 2006. "Trust in the Internet as an Experience Technology," *Information, Communication and Society*, 9(4): 433–51.

Dutton, W. H., Law, G., Bolsover, G., and Dutta, S., 2014. *The Internet Trust Bubble: Global Values, Beliefs and Practices*. NY: World Economic Forum. http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf

Franklin, J., Paxson, V., Perrig, A., and Savage, S., 2007. *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants.* Paper presented at the CCS'07. Available online at http://www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf.

Goodman, S. E., and Lin, H. S., 2007. *Toward a Safer and More Secure Cyberspace.* Washington, DC: The National Academies Press.

Gordon, L. A., and Loeb, M. P., 2005. *Managing Cybersecurity Resources: A Cost-Benefit Analysis*. Columbus, OH: McGraw-Hill.

Holt, T. J., 2012. "Examining the Forces Shaping Cybercrime Markets Online," *Social Science Computer Review*, 31(2): 165–177.

Krebs, B., 2014. *SPAM Nation*. Naperville, Illinois: Sourcebooks, Inc.

McAfee Labs. 2014. *Threats Report*, November 2014.

Microsoft. 2014. *Microsoft Security Intelligence Report*, Volume 17, January through June 2014.

Moore, T., Clayton, R., and Anderson, R., 2009. "The Economics of Online Crime," *Journal of Economic Perspectives*, 23(3), 3–20.

NRC, 1991. System Security Study Committee, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, *Computers at Risk: Safe Computing in the Information Age*. Washington DC: The National Academies Press.

NRC, 2002. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Computer Science and Telecommunications Board, Division of Engineering and Physical Sciences, National Research Council. Washington, DC: National Academy Press.

Orji, U. J., 2012. *Cybersecurity Law and Regulation*. Nijmegen, The Netherlands: Wolf Legal Publishers.

Ponemon Institute, 2014. 2014 Cost of Data Breach Study: Global Analysis.

Shalhoub, Z. K., and Al Qasimi, S. L., 2010. *Cyber Law and Cyber Security in Developing and Emerging Economies*. Cheltenham, UK; Northampton, MA: Edward Elgar.

Symantec, 2014. Internet Security Threat Report 2014, Volume 19, accessed 4 April 2015 at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. <This page is not found>

Symantec, 2015. *Internet Security Threat Report 2015*, Vol. 20, accessed 8 May 2015 at http://www.symantec.com/security_response/publications/threatreport.jsp?themeid=threatreport.

Van Eeten, M. J. G. and Bauer, J. M., 2009. "The Economics of Malware," in OECD, *Computer viruses and other malicious software: a threat to the Internet economy* (pp. 79–148). Paris: Organisation for Economic Co-operation and Development.

Van Eeten, M. J. G., Bauer, J. M., and Tabatabaie, S., 2009. "Damages from Internet Security Incidents: A Framework and Toolkit for Assessing the Economic Costs of Security Breaches." Report for OPTA. The Netherlands.

Van Eeten, M. J. G., Bauer, J. M., Asghari, H. and Tabatabaie, S., 2010. *The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data.* STI Working Paper 2010/5. Paris: Organisation for Economic Co-operation and Development.

Van Eeten, M. J. G. and Bauer, J. M., 2013. "Enhancing Incentives for Internet Security," in I. Brown (ed.), *Handbook of Internet Governance* (pp. 445–484). Cheltenham, UK: Edward Elgar.

Varian, H., 2004. "System Reliability and Free-Riding," in L. J. Camp and S. Lewis (eds.), *Economics of Information Security* (pp. 1–15). Berlin, New York: Springer.

Wash, R., and Rader, E., 2011. "Influencing Mental Models of Security**,"** *Proceedings of the New Security Paradigms Workshop (NSPW)*. Marshall, CA. September.

Weizenbaum, J., 1976. *Computer Power and Human Reason: From Judgment to Calculation*. San Francisco, CA: W. H. Freeman and Company.