OECD Digital Economy Outlook 2015

Chapter 5

Trust in the digital economy: Security and privacy

Trust plays a vital role in social and economic interactions. It functions as a powerful tool in complex environments for reducing uncertainties and enabling reliance on others. Trust underpins business, institutional and personal relationships and is particularly important in the global online environment. The opportunities presented by the digital economy will not be realised in the absence of trust. This chapter examines two key elements of trust online: security and privacy. It covers a select number of trends, which taken together provide an overview of digital security and privacy, both in terms of the risks and responses.

5.1 The growing profile of digital security and privacy risks

The OECD began developing its policy framework for trust online in the 1990s with a view to helping governments realise the economic and social potential of the Internet. Two decades later, information communication technologies (ICTs) and the Internet are widely integrated into economic and social activities. The resulting dependence of all sectors of OECD countries on the digital environment makes addressing security and privacy risk essential.

Digital security and privacy routinely feature on the front page of newspapers and in government strategies and speeches by senior political figures and corporate executives. In a 2014 OECD survey on the digital economy, governments identified security as the second highest priority area and privacy as the third out of 31 possible priority areas, with only broadband coming higher (OECD, 2014).

Privacy has also joined cybersecurity on the US Government's "High Risk List", attributed to the challenges posed by advances in technology, which have dramatically enhanced the ability of both government and private sector entities to collect and process extensive amounts of personal information (US GAO, 2015). Although the disclosures in 2013 by former NSA contractor Edward Snowden have no doubt elevated the visibility of security and privacy, the increasing prominence of these issues is the result of a transformation in the way data is generated, shared and analysed, and the corresponding benefits that these developments have brought in terms of innovation, growth and well-being.

This chapter reviews a number of topics addressed in a 2012 OECD survey of the evidence base for security and privacy, which uncovered a rich diversity of empirical data that could potentially enhance policy making in this sector (OECD, 2012a). It examines the available evidence in a number of discrete areas across the security and privacy landscape. This evidence is suggestive of the growing attention paid to security and privacy, shown for example by the booming professional class of privacy and security experts, as well as an important if less dramatic strengthening of the government bodies charged with protecting privacy and security. At the international level, one important development underway is the revision of the 2002 OECD Security Guidelines to help stakeholders better address digital security risks.

At the national level, governments continue to release and update national cybersecurity strategies (see Section 5.4). Opportunities for skilled security professionals continue to grow (see Section 5.2) and the role of national Computer Security Incident Response Teams (CSIRTs) is highlighted as a key response (see Section 5.3). In terms of legislation, data security breach notification, which bridges privacy and security risks, is on the rise (see Section 5.4). On the technical side, implementation of Domain Name System Security Extensions (DNSSEC) promises to provide security in the domain name system (Section 5.4).

Consumers report growing privacy concerns

Surveys suggest that the evolving risk environment is causing concern for security and privacy. A 2014 CIGI-Ipsos survey of Internet users on Internet security and trust, found that 64% of respondents in the 24 countries surveyed were more concerned about privacy than they were in 2013 (CIGI, 2014). According to a 2014 Pew Research Center poll, 91% of Americans surveyed agree that consumers have lost control of their personal information and data (Madden, 2014). In a special 2014 Eurobarometer report on cybersecurity, the top two concerns reported by EU Internet shoppers were misuse of personal data and security of online payments. In both areas the level of concern has grown since 2013, with fear of personal data misuse increasing from 37% to 43% and security concerns rising from 35% to 42% (EC, 2015).

Significantly, expressions of concern are not always accompanied by a change in behaviour. For example, numerous studies document how individuals reporting privacy fears nevertheless engage in risky behaviour involving their personal data, a phenomenon dubbed the "privacy paradox" (Taddicken, 2014). Recent surveys, however, suggest that users are taking steps to address their concerns. The CIGI-Ipsos 2014 study found that out of the 60% of Internet users that had heard of Edward Snowden, 39% took steps to protect their privacy and security as a result of his revelations. Recent Eurobarometer numbers are more striking, with 88% of EU respondents claiming in 2014 to have changed the way they use the Internet because of concerns about security, up from 81% in 2013. Password management is among the actions reportedly taken, with 31% reporting that they use different passwords for different sites, and 27% reporting that they change those passwords regularly (EC, 2015).

Surveys like these cannot of course conclusively establish the importance of consumer trust in the current online environment. However, there is increasing recognition of the need for better metrics and other evidence to inform policy makers in government and organisations of the size of the problem and to develop strategies to address the challenges (OECD, 2011a, 2012a, 2013b). Nevertheless, the perception that consumer trust is at stake persists and is reflected in recent business practices. For example, the last few years have seen an increasing number of multinational Internet and communication companies release transparency reports (see Section 5.4), which indicates growing recognition among companies of the linkage between consumer trust (whose data and loyalty are essential to the bottom line) and the need for public steps to protect privacy and secure online services.

Impact of security breaches can be significant

In 2014, security incidents featured regularly in mainstream media. One observable trend is an increase in theft of card account and customer credentials, as highlighted in the Target and Home Depot cases – two major US retailers. The Target breach reportedly involved payment card and other data of 70 million customers. Target corporate filings for 2013-14 recorded expenses related to the breach of USD 252 million, which even after being offset by USD 90 million in insurance proceeds, leave charges of USD 162 million. Ongoing litigation and regulatory proceedings have added further costs, including an estimated USD 200 million to issue new cards, which still omits the more speculative reputational costs. The breach at Home Depot involved 56 million payment card accounts and 53 million customer email addresses (Home Depot, 2014). Another major breach in 2014 involved three Korean credit card companies and affected 20 million individuals – 40% of the Korean population. Some three dozen executives lost their jobs as a result (Choe

Sang-Hun, 2014). The beginning of 2015 has continued the trend, with Anthem Inc., a large US-based health insurance company, announcing that hackers broke into its servers and stole social security numbers and address, email and employment data across its business lines, which will by some estimates affect 80 million individuals.

The impact of these security incidents can be significant for the organisations in question. Perhaps the most prominent malicious breach occurred at the end of 2014, when Sony Pictures Entertainment suffered a cyber attack that exposed unreleased movies, employee data, emails between employees, and sensitive business information such as sales and marketing plans. The duration of the hack is as yet unknown, although evidence suggests that the intrusion was ongoing for more than a year, prior to its discovery in November 2014. Although the direct financial costs of the breach may be covered by cyber insurance policies (see Section 5.4), the damage to the firm's reputation, relationships in the industry and impact on employees may be longer-lasting and hard to measure.

Although only larger incidents tend to capture the headlines, research suggests that data security breaches are commonplace. A 2014 study commissioned by the UK government found that 81% of large UK organisations suffered a security breach in the past year (BIS, 2014). Although this figure seems high, it actually represents a reduction of 5% from the 2013 survey. However, the severity and impact of security breaches has increased, with the cost of individual breaches nearly doubling in a single year. Major breaches are estimated to cost large organisations between GBP 600 000 and GBP 1.15 million. As discussed in Section 5.4 below, a new report from the Attorney General in California singled out the retail and health sectors as the target of a disproportionate percentage of reported data security breaches. Data security breaches are increasingly the subject of litigation, with card issuers looking to the hacked companies to recover the costs of reissuing payment cards, while class-action lawsuits brought by affected individuals are a growing possibility (Section 5.4). Moreover, breaches are not limited to the private sector. In Canada, the Office of the Privacy Commissioner stated that the number of data breaches reported by other Canadian government agencies more than doubled during the 2013/14 fiscal year. Accidental disclosure was indicated by reporting organisations as the reason behind more than two thirds of breaches.

The digital security threat landscape continues to evolve, sustained by often profitable business models. For example, "ransomware" is a type of file-encrypting malware increasingly deployed by cybercriminals to encrypt the computer files of an organisation or individual, who must then make a payment (i.e. the "ransom") in exchange for decryption of their files. The most prominent strain of ransomware is "CryptoLocker", which is spread via email attachments. Experts estimate that CryptoLocker infected some 234 000 computers, extracting more than USD 27 million in ransom payments, during its first two months alone, before being disrupted by a multinational law enforcement effort, involving Canada, Germany, Luxembourg, the Netherlands, Ukraine, the United Kingdom and the United States (US DoJ, 2014).

New security vulnerabilities continue to be discovered with recent examples affecting the operation of key Internet protocols. "Heartbleed" involved the exposure of a critical vulnerability in Open SSL (Secure Sockets Layer), a security technology commonly used by websites to encrypt communications with users. By exploiting this vulnerability, an attacker was able to steal usernames, passwords and private encryption keys. The carefully chosen name "Heartbleed" illustrates the increasing efforts of security researchers who discover these vulnerabilities to publicise their findings. Heartbleed even has its own website: *http://heartbleed.com/*.

A similar vulnerability, dubbed “Shellshock”, was disclosed in September 2014. It affects websites using the Unix and Linux operating systems. Like Heartbleed, Shellshock affects numerous systems that require a patch. In October 2014, a flaw in one version of SSL used by most commercial sites to protect user privacy and security was disclosed. Attackers can also exploit the “Poodle” vulnerability to decrypt passwords or other data from an SSL-encrypted transaction and other security protocols.

Responses to the evolving security risk landscape have been many-faceted and samples of these are provided at the end of the chapter.

The privacy risk landscape is evolving

Privacy issues have also received a significant rise in attention, including at the political level. President Obama’s “State of the Union” speech to the US Congress referred to privacy on several occasions – a first for such an address (White House, 2015). In a speech announcing his legislative priorities on the eve of becoming President of the European Commission, Jean-Claude Juncker, committed to “swiftly concluding negotiations on common European data protection rules” (Junker, 2014).

No longer just the concern of specialists, privacy has attracted the attention of the scientific community as the subject of a special report in *Science* (2015). Concern about privacy has also spilled over into contemporary art, with the opening of the play *Privacy* in London’s West End in 2014. One commentator has compared the role of privacy in the digital economy to that of competition policy reacting to the excesses of the Industrial Revolution in the early twentieth century (Tene, 2015).

Post-Snowden, much of the focus of the privacy community and media is framed in relation to the activities of national security agencies involving communications and Internet data. But the increasingly data-driven character of economic and social activities has raised privacy concerns around a host of other developments. Big data, the Internet of Things and data brokers have joined Internet search and social networking as regular topics subject to commentary and debate at conferences. One cannot consider the evolving privacy risk environment without recalling that many of the data security breaches noted above involved personal data, and as such represent a breach of privacy.

Legislation continues to feature as a key response to privacy risk, with security breach notification requirements (see Section 5.2) typically found in privacy laws. A series of developments in privacy legislation have taken place across OECD countries. Legal reforms came into effect in Australia in 2014, enhancing the powers of the Office of the Australian Information Commissioner (OAIC), while updating the Australian Privacy Principles. Canada’s anti-spam legislation (CASL) came into effect in July 2014, requiring organisations to obtain consent before sending commercial electronic messages to an email, telephone or instant messaging account. Korea significantly revised its privacy law in 2012 to require data breach notification, with further revisions in 2014 to increase data breach fines and allow individuals to claim statutory compensation. Japan established its first independent data protection authority in 2014, with authority over personal information related to government-issued identification numbers for social security, taxation and disaster management.

Countries outside the OECD have also implemented changes in privacy legislation. China amended its consumer rights law, effective March 2015, to add a number of provisions regarding the protection of personal information. In 2014, Brazil adopted a long-awaited law on the rights of Internet users – the "Marco Civil da Internet" – that creates fundamental rights regarding personal data covering consent, data deletion and purpose specification (see Chapter 1, Box 1.3). In November 2013, South Africa adopted the Protection of Personal Information Act, parts of which came into effect in 2014, including the establishment of an information regulator. Singapore's new law governing the collection and use of personal data by private sector organisations came into force in July 2014. Other countries with legislative developments include the Dominican Republic and Dubai (NYMITY, 2014).

In terms of major legislative initiatives, proposed privacy legislation in Europe and the United States remain works in progress. Negotiations are still underway in Brussels and EU member state capitals to complete a major overhaul of Europe's data protection framework, with work continuing to finalise proposals first announced by the European Commission in January 2012. The Obama administration has released a discussion draft of legislation to implement the Consumer Privacy Bill of Rights, and is supporting more targeted measures to address data breach notification and student privacy. Elsewhere, a process to reform Canada's private sector law "PIPEDA" remains underway and Japan is currently reviewing its Personal Data Protection Law to ensure its suitability for a world of "big data" and to improve its global compatibility (Cabinet Office of Japan, 2014)

Although privacy issues are seldom considered in a vacuum, a number of efforts to link privacy to other policy domains are noteworthy. Attempts to link trade and privacy are on the rise, in particular in the context of negotiations between the EU and the US towards a Transatlantic Trade and Investment Partnership. The European Data Protection Supervisor has taken steps to establish closer links between data protection and competition policy (EDPS, 2014), as personal data replaces natural resources as a key source of market power (Tene, 2015). In the research community, efforts continue to apply insights from behavioural economics to privacy policy.

In terms of international developments, the Council of Europe is working to update its primary data protection instrument, Convention 108. Meanwhile, Asia-Pacific Economic Co-operation (APEC) has begun a review of its 2004 Privacy Framework, with a view to possibly drawing on elements from the 2013 update to the OECD Privacy Guidelines. APEC is also working to implement its Cross-border Privacy Rules (CBPR) system, whose members include Japan, Mexico, the United States and most recently, Canada. Officials from APEC economies and representatives of the EU Working Party 29 are also continuing their collaboration to improve interoperability between the CBPR system and the EU's Binding Corporate Rules system. Lastly, the Organization of American States is working on a model law on personal data protection.

Encryption to protect user data is going mainstream

On the technology front, Apple, Google and other companies have increased the default use of encryption in respose to the Snowden disclosures. Apple's latest mobile operating system encrypts nearly all data on iPhones and iPads by default. Google's Gmail now uses an encrypted connection when checking or sending email via a browser. The company has also released a new browser extension to simplify the use of Open PGP, a common encryption tool (Somogyi, 2014). The popular messaging tool, WhatsApp, announced its own end-to-end encryption. Apple, now the world's most valuable publicly traded company, has also begun to explicitly market its privacy practices at the CEO level, emphasising security and privacy as fundamental design elements in Apple products and services. Such developments offer encouragement to policy makers who have long hoped that businesses would treat privacy protection as a business differentiator.

Other developments that address privacy risks are covered throughout the remainder of this chapter. Of particular note is the increasing role of courts, in particular the *Costeja* decision of the European Court of Justice, which established an individual's right to have a search engine de-list certain results (commonly referred to as the "right to be forgotten") (Section 5.4). Another development is the upward trend in the number of privacy professionals working in the private sector. Growth in the privacy profession has been particularly striking, with one estimate putting overall expenditure on privacy programmes among Fortune 1000 companies at USD 2.4 billion per year (Section 5.2).

However, the growing profile of privacy and security issues has not been matched by an equivalent acceleration in the development of metrics and other evidence needed by policy makers in government and organisations, to help them evaluate the size of the problem and address challenges posed by the current environment (see OECD, 2011a, 2012a, 2013b). Furthermore, unlike cybersecurity, governments have not yet started to develop national privacy strategies, as called for in the OECD Privacy Guidelines, to address privacy issues in a coordinated, holistic manner, which would enables stakeholders to clarify the depth of protection to be afforded to individuals and the limitations society is willing to accept to serve collective public interests.

5.2 The job market for security and privacy professionals

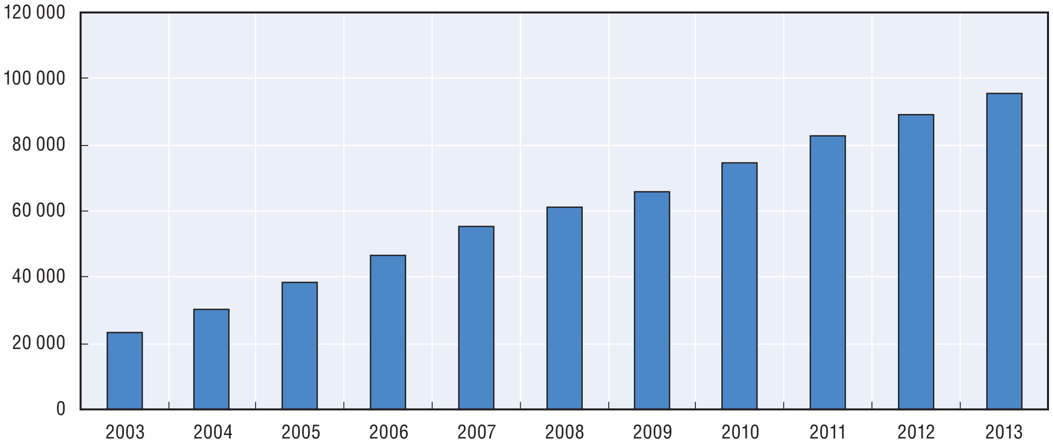
The growing importance and visibility of security and privacy risks has increased professional opportunities for experts in these areas. Demand for security expertise is characterised by a continuation of the steady growth evident over the last decade, while growth in demand for privacy professionals has accelerated rapidly in recent years. A new website devoted exclusively to jobs for privacy and cybersecurity professionals (*www.dataprivacycareers.com*) has emerged, with new opportunities posted daily. However, locating available professionals with the required skills and expertise in privacy and security remains a challenge for organisations looking to strengthen capacities in these areas.

Security professionals are in short supply as demand rises

The issue of cybersecurity now features prominently on national policy agendas. One of the most critical aspects is the availability of skilled professionals capable of helping organisations manage cybersecurity risks. However, the number of professionals worldwide continues to rise steadily. Bodies issuing professional certifications for cybersecurity skills provide a useful source of data on the growth of professionals this sector. For example, the International Information Systems Security Certification Consortium, otherwise known as (ISC)^2, issues a range of cybersecurity certifications. By end-2013, (ISC)^2 had certified 95 781 individuals worldwide (Figure 5.1), representing a four-fold increase in the last decade.

Despite this increase, the supply of skilled cybersecurity professionals falls well short of demand. A 2013 report by Japan's National Information Security Center suggests a shortage of 80 000 information security engineers in the country. Moreover, the report noted that most practising cybersecurity professionals lack the necessary skills to counteract online threats effectively (Humber and Reidy, 2014).

Figure 5.1. **Number of (ISC)² certified individuals worldwide, 2003-13**



Source: (ISC)², 2011 and e-mail correspondence with company.

StatLink http://dx.doi.org/10.1787/888933225200

In the United States, the Bureau of Labor Statistics forecasts a 37% rise in demand for graduate-level cybersecurity workers over the next decade – more than twice the predicted rate of increase for the overall computer industry (Coughlan, 2014).

In the United Kingdom, an analysis of government statistics on students leaving higher education in 2012-13, showed that less than 0.6% of recent computer science graduates work in cybersecurity (Barrett, 2014). The UK's National Audit Office has warned that it could take 20 years to fill the skills gap in trained cybersecurity staff (Coughlan, 2014). The National Cyber Security Programme, the Department for Business Innovation and Skills, the Government Communications Headquarters and the Cabinet Office have since partnered to lead and support activities to increase cybersecurity skills at all levels of education (HM Government, 2014).

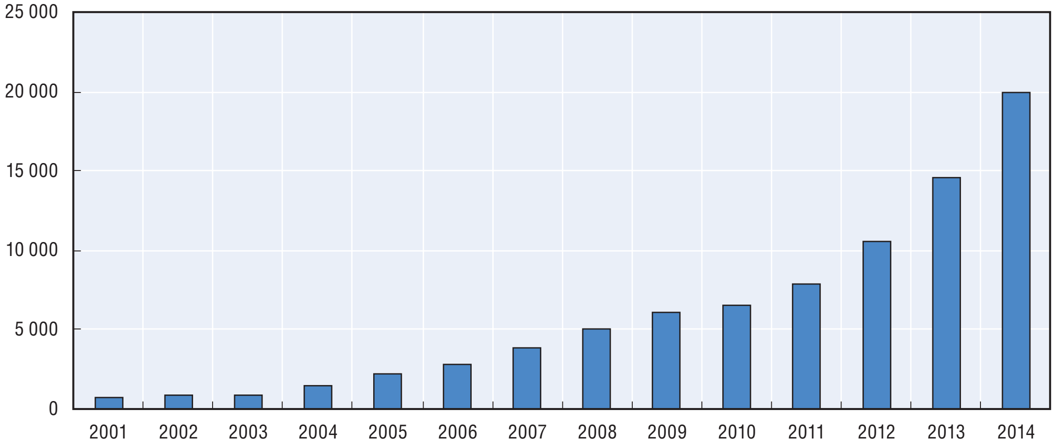
In summary, available evidence suggests that despite growth in the cybersecurity profession, organisations still face a severe skills shortage in both the public and private sectors.

Privacy professionals are in demand

One of the most important developments in effective privacy protection measures has been the emergence of a professional class of privacy officers and experts in organisations. (Bamberger and Mulligan, 2010). In some countries, there is a statutory basis to support or encourage the role of privacy professionals. For example, Germany's Bundesdatenschutzgesetz (Federal Data Protection Act) sets out specific requirements concerning data protection officials in organisations. Canada's federal private sector legislation, PIPEDA, requires organisations to designate an individual(s) responsible for personal data-handling activities, and the EU Directive also contains a reference to a personal data protection official. New Zealand's Privacy Act requires every agency in both the public and private sectors to appoint a privacy officer and various pieces of US legislation require federal agencies to have chief privacy officers or senior agency officials for privacy. Both of Korea's privacy laws require companies to designate a person responsible for the management of personal information. Lastly, the proposed EU data protection regulation would require the appointment of data protection officers for all public authorities and for companies processing more than 5 000 data subjects, which would further elevate the numbers of professionals.

These developments have been encouraged and supported by professional associations, setting the parameters for the development of a privacy workforce, including chief privacy officers (CPOs) and their staff (Clearwater and Hughes, 2013). These associations provide training, certification, conferences, publications, professional resources and industry research to a growing membership. The largest and most global in reach – the International Association of Privacy Professionals (IAPP) – now has more than 18 000 members (a 24% increase from September 2013) in 83 countries around the world (Figure 5.2). Others include the Privacy Officers Network, through which senior privacy officers involved in the practical implementation of privacy initiatives meet and exchange ideas through a professional support network,[1] and national bodies such as the Association Française des Correspondants à la Protection des Données à Caractère Personnel in France,[2] and the Asociación Profesional Española de Privacidad in Spain.[3]

Figure 5.2. **Total number of IAPP members, 2001-14**



Note: The figure for 2014 is a projection. As of October 2014 the number of members was 18 000.

Source: IAPP (2014). https://privacyassociation.org.

StatLink http://dx.doi.org/10.1787/888933225215

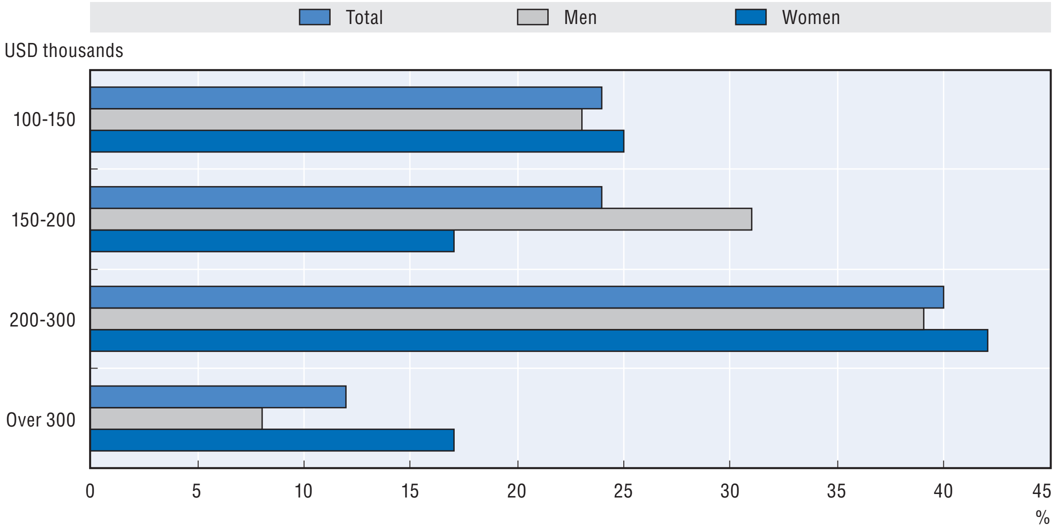
The steep growth in IAPP's membership numbers – from over 10 000 in 2012 to almost 20 000 projected by the end of 2014 – highlights increasing recognition of the importance of sound data governance practices. While budgets vary widely across Fortune 1000 companies, IAPP's "Fortune 1000 Privacy Program Benchmarking Study" found that the average privacy budget is USD 2.4 million, of which 80% is spent internally on areas ranging from developing policies, training, certification and communications, to audits and data inventories. Fortune 1000 companies spend an average of USD 76 per employee on privacy (IAPP, 2014). According to IAPP, overall expenditure on privacy among these companies is estimated at USD 2.4 billion per year.

A majority of respondents (59%) reported that they had personally established their company's privacy programme. This indicates that the privacy industry is still nascent with significant growth opportunities. Indeed, privacy budgets are likely to grow, with nearly 40% of privacy professionals predicting an average increase in their budget of 34% in coming years, and 33% of professionals intending to hire new privacy staff.

The IAPP's annual salary survey corroborates the results of the benchmarking study. The survey demonstrates a steady increase in privacy officers' pay (Figure 5.3), with CPOs earning an average of USD 180 000 per year in the United States, while privacy leaders (who do not hold the title of CPO) earn an average of USD 131 000 in the United States and USD 125 000 worldwide (IAPP, 2013).

Figure 5.3. **Annual income of a privacy professional in a Fortune 1000 company**

USD thousands



Source: IAPP (2013). *https://privacyassociation.org*.

StatLink http://dx.doi.org/10.1787/888933225226

For data-centred organisations, meeting privacy expectations requires more than legal compliance and sound security practices. Under the 2013 revisions to the OECD Privacy Guidelines, accountable organisations need to put in place multifaceted privacy management programmes, and be ready to demonstrate them on request from a privacy enforcement authority (OECD, 2013a, para. 15). Implementing such programmes requires legal, technical, communications, governance and public relations skills, among others. This has resulted in an increased focus on training, education and certification activities.

The growth in data-driven innovation, fuelled in part by data analytics, is also highlighting the importance of data ethics as a key element in protecting privacy (OECD, 2015a forthcoming: Chapter 6). Companies will need to adjust their perception of privacy as a compliance matter to be addressed by legal departments or as a technical issue to be handled by IT departments, and put in place ethical review processes. They must also ensure that privacy-literate employees are designated throughout the organisation to identify possible issues. Developing the skills and insights needed to meet these evolving needs should ensure continued demand for professional networks and associations for privacy professionals. However, this demand may have an adverse effect on privacy enforcement authorities – from whose rosters the private sector may increasingly look to recruit staff with the needed expertise and experience.

Although the growth in security and privacy professionals documented here is both impressive and important, it does not fully capture the shift in some organisations towards integration of these topics across workflows. For these companies responsibility for privacy/security issues is not limited to designated staff; instead it is shared among of all parts of the organisation dealing with personal data and matters impacting security.

5.3 Privacy enforcement and security response

The importance of privacy enforcement authorities is recognised in the 2013 revision of the OECD Privacy Guidelines, which includes a new provision calling specifically for the establishment of privacy enforcement authorities with the "governance, resources and technical expertise necessary to exercise their powers effectively" (OECD 2013a, para. 19). Approximately one third of OECD countries had such an authority in 1980 when the Privacy Guidelines were first adopted. Today, virtually all OECD countries report having established one or more privacy enforcement authorities.

Box 5.1. **What is a Privacy Enforcement Authority?**

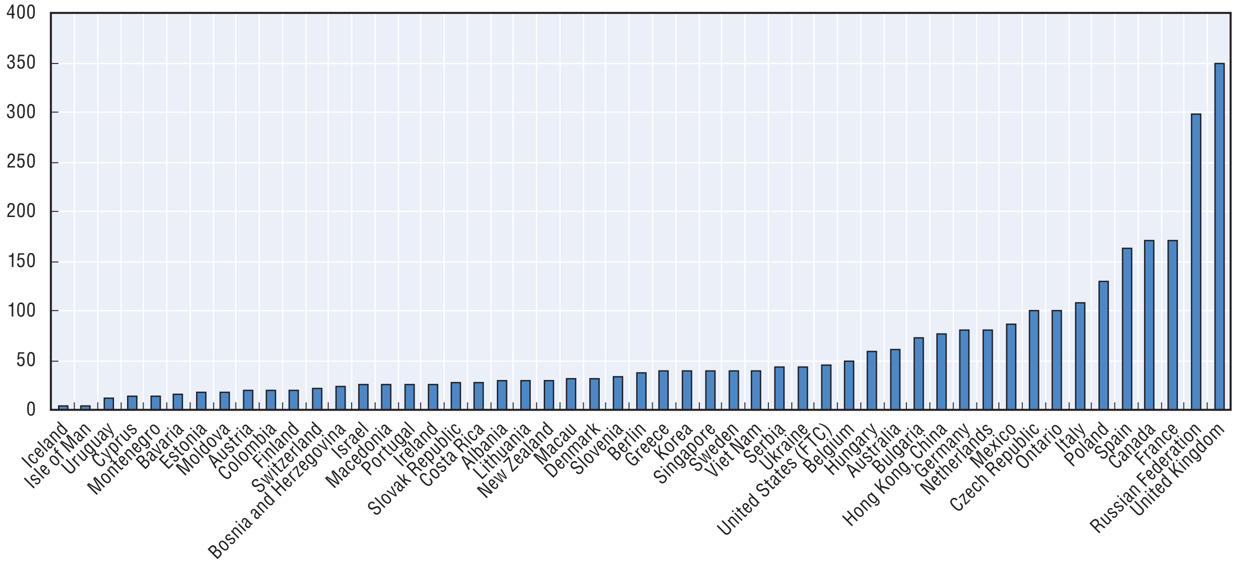
"Privacy Enforcement Authority" means "any public body, as determined by each Member country, that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings." Federal countries may have regional or local authorities that fall within the definition.

Source: OECD (2013a, para. 1)

Budgetary resources

In 2013, the European research consortium PHAEDRA, established to improve co-operation among data protection authorities, surveyed 79 data protection authorities and privacy commissioners around the world. The survey included one question on staffing: How many full-time employees does your organisation have?" The results indicate that staff size varies widely across countries, from quite small to relatively large (Figure 5.4). With 350 full-time employees, the United Kingdom reports the highest number of full-time employees (FTE).

Figure 5.4. **Number of full-time employees in privacy enforcement authorities worldwide, March 2014**



Source: PHAEDRA (2014).

StatLink http://dx.doi.org/10.1787/888933225238

However, it is important to take note of the difficulties some countries face in answering questions regarding staffing levels. In Japan, for example, there was no dedicated authority for privacy protection until 2014. Prior to this date, sixteen different ministries took on the role of privacy enforcement authority in the sectors overseen by their government administration. Likewise, in some countries the number and role of sub-national level authorities can be quite significant. Generalising about staffing levels for privacy enforcement matters is therefore challenging.

Technical resources

Privacy concerns typically follow on from technological developments. In recent years, the rapid evolution in technology-driven business models and practices has posed challenges for enforcement authorities working to understand the implications of these changes for privacy. The integration of data-driven innovation more fully within firms will exacerbate these challenges (OECD, 2015a).

The explanatory memorandum to the revised OECD Privacy Guidelines underlines the importance of technical expertise in light of the increasing complexity of data usage, and supports the emerging trend within privacy enforcement authorities of retaining staff with a technical background. A small sampling of countries is suggestive of an increasing trend within privacy enforcement authorities of bring technical expertise in house. However, among the nine countries reporting on this issue for the period 2011-13, the ratio of technological experts to staff remains relatively low (Table 5.1).

Table 5.1. **Ratio of technological experts to total staff in privacy authorities for selected countries**

Country	2011	2012	2013
Belgium	1/52	1/52	1/52
Canada	3/160	5/161	5/173
Hungary	No data	3/47	3/56
Ireland	0/21	0/27	1/28
Italy	4/123	4/122	4/122
Lithuania	4/30	4/30	4/30
New Zealand	0/30	0/30	0/30
Sweden	1/40	1/40	4/41
United Kingdom*	2/256	3/280	3/288
Total technologists	*15*	*21*	*25*

Note: * The UK staffing figures are higher in Figure 5.4 because they include staff working on freedom of information issues.

Source: OECD DEO survey 2014.

These numbers do not reflect the situation in Korea (not shown) where numbers of technical staff are much higher, accounting for more than half of privacy employees; or in the United States, which also attaches importance to ensuring decisions are informed by sufficient technical expertise. This importance is reflected by the establishment of the position of Chief Technology Officer at the Federal Trade Commission (FTC) in 2010, a senior post held by prominent computer scientists. The FTC also reported a wide range of investigators and attorneys with technical skills in the United States, but was unable to identify a precise number. Likewise, with 16 ministries involved in privacy enforcement, the situation in Japan is complex. Each ministry devotes 2 to 13 employees to privacy enforcement, many of whom co-operate with outside agencies to benefit from additional expertise.

Co-operation among privacy enforcement authorities is growing

Since the adoption of an OECD recommendation in 2007, co-operation among privacy enforcement authorities has become a priority (OECD, 2007). A 2011 OECD report highlights a number of areas in which progress is being made, including the formation of the Global Privacy Enforcement Network (GPEN) (see below). The report also highlights challenges and obstacles to more effective co-operation, particularly in the area of information sharing (OECD, 2011b). Recognising the need to take additional steps, privacy enforcement authorities have developed a "Global Cross Border Enforcement Cooperation Arrangement", which

> *encourages and facilitates all [privacy enforcement authorities'] cooperation with each other by sharing information, particularly confidential enforcement-related information about potential or on-going investigations, and where appropriate, the Arrangement also coordinates [privacy enforcement authorities'] enforcement activities to ensure that their scarce resources can be used as efficiently and effectively as possible (OPC, 2014b).*

In October 2014, the International Conference of Data Protection and Privacy Commissioners adopted a resolution endorsing the new Arrangement as a basis for facilitating enforcement co-operation among its members, and encouraged participation among all privacy enforcement authorities (OPC and ICO, 2014). While not legally binding, the Arrangement takes a number of important steps forward in strengthening the framework for cooperation among authorities. It aims to operationalise many of the good practices from the 2007 OECD Recommendation, including detailed provisions related to reciprocity and confidentiality. It also goes beyond the OECD recommendations, particularly in the area of coordination of international activities, and empowers the Conference's Executive Committee to help administer the Arrangement.

…as reflected in the activities of the Global Privacy Enforcement Network (GPEN)

As noted above, progress in enforcement co-operation is reflected in the activities of the Global Privacy Enforcement Network (GPEN), formed in 2010 on the recommendation of the OECD. GPEN aims to facilitate co-operation between data protection regulators and authorities throughout the world in order to strengthen personal privacy globally. GPEN currently consists of 51 data protection authorities across some 39 jurisdictions. One interesting development has been the addition of new authorities outside the usual data protection family; for example, the US Federal Communications Commission joined GPEN in October 2014 (FCC, 2014).

A collective GPEN survey, or "sweep", examined disclosure practices regarding the use of personal data by mobile apps. Over the course of a week in May 2014, GPEN's "sweepers" – consisting of 26 data protection authorities across 19 jurisdictions – participated in the activity by downloading and briefly interacting with more than 1 200 of the most popular apps released by developers. The purpose of the sweep was to increase public and commercial awareness of data protection rights and responsibilities, and to identify specific issues that may become the focus of future enforcement actions and initiatives (Box 5.2).

Box 5.2. **GPEN sweep results**

The sweep identified the following privacy challenges:

- 85% of apps failed to explain clearly how personal information would be processed.
- 59% of apps did not clearly indicate basic privacy information (with 11% failing to include any privacy information whatsoever).
- 31% of apps were excessive in their permission requests to access personal information.
- 43% of apps had not sufficiently tailored their privacy communications for the mobile app platform, often relying instead on full version privacy policies found on websites.

The sweep identified the following good practices:

- Many apps provided clear, easy-to-read and concise explanations about exactly what information would be collected, how and when it would be used and, in some instances, explained specifically and clearly what would not be done with the information collected.
- Some apps provided links to the privacy policies of their advertising partners and opt-out elections in respect of analytic devices.
- Some apps provided good examples of privacy policies specifically tailored to the app platform. These included use of just-in-time notifications (warning users when personal information was about to be collected or used), pop-ups and layered information, which allowed consumers to obtain more detailed information if required.

Source: UK Information Commissioner's Office.

On 10 September 2014, GPEN published the results of the sweep, which suggest that a high proportion of the apps downloaded did not sufficiently explain how consumers' personal information would be collected and used. Numerous instances were identified where apps which appeared to collect personal information did not have a privacy policy (or other up-front privacy information), thus removing the opportunity for individuals to be meaningfully informed when making decisions about the collection, use and/or disclosure of their personal information.

In December 2014, 23 privacy authorities from around the world signed an open letter to the operators of seven app marketplaces urging them to make links to privacy policies mandatory for apps that collect personal information (OPC, 2014a). The letter was sent to Apple, Google, Samsung, Microsoft, Nokia, BlackBerry and Amazon.com, but was intended for all companies that operate app marketplaces. It called on operators of app marketplaces to require each app capable of accessing or collecting personal information to provide users with timely access to the app's privacy policy.

..and in growing actions across Computer Security Incident Reponses Teams

Incident response is a fundamental part of cybersecurity risk management. In recognition of this fact, the 2002 OECD Guidelines for the Security of Information Systems and Networks ("Security Guidelines")[4] include a Response principle.

Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

A Computer Security Incident Response Team (CSIRT) is a group that acts as a trusted point of contact for computer security incident response. While all participants have a role to play in incident response, CSIRTs are dedicated to co-ordinating response activities. Their main responsibility is to handle and mitigate computer security incidents with the aim of protecting their constituencies (i.e. their customer base). A CSIRT may provide a range of services to its constituents, such as issuing alerts and advising on current and impending computer-related threats, or collecting and gathering data to analyse incidents in order to provide constituents with solutions and courses of actions to reduce risks and minimise the expected damage. CSIRTs may also issue advice on vulnerabilities and malware in the software and hardware running on their constituents' systems, allowing them to promptly patch or update their systems to prevent infection or further damage.

The Response principle of the OECD Security Guidelines also emphasises the co-operative nature of security incident response and the need for international co-operation in some instances. The spirit of this principle is reflected in numerous high-level policy statements and commitments at national, regional and international levels. For example, the United States *International Strategy for Cyberspace*,[5] the Association of Southeast Asian Nations (ASEAN) Regional Forum 2006 *Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space* and the International Telecommunication Union's *Resolution 130*[6] all emphasise the importance of international co-operation in incident response.

In 2013, the UN Group of Governmental Experts recommended enhanced information sharing and co-operation in security incident response as a confidence-building measure, noting the importance of:

> *enhanced sharing of information among States on ICT security incidents, involving the more effective use of existing channels or the development of appropriate new channels and mechanisms to receive, collect, analyse and share information related to ICT incidents, for timely response, recovery and mitigation actions. States should consider exchanging information on national points of contact, in order to expand and improve existing channels of communication for crisis management, and supporting the development of early warning mechanisms (UN, 2013: 9)*.

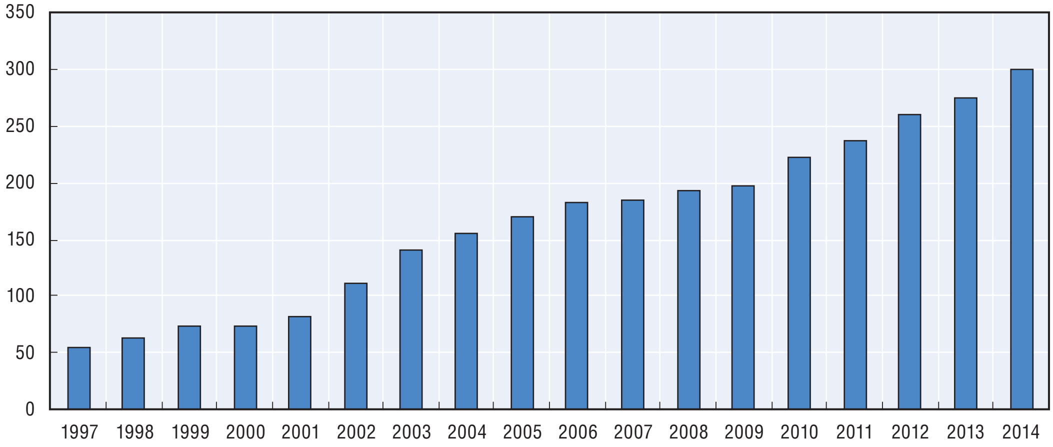
While there are currently no metrics for directly measuring international co-operation among CSIRTs, there are indications of interest in establishing closer links among teams globally. Statistics from the Forum of Incident Response and Security Teams (FIRST) reveal a steady increase in CSIRT participation at the Annual FIRST Conference – the premier international CSIRT event (Figure 5.5). At the 2014 conference in Boston, 299 teams participated. These statistics provide a good indication of increased interaction, information sharing, collaboration and co-operation among teams, which should lead to improved incident response and better cybersecurity risk management.

With increased recognition of the essential role that CSIRTs play in cybersecurity risk management comes increased expectations about the extent of their responsibilities, particularly from policy makers whose appetite is growing for reliable, trustworthy information about current and historical cybersecurity trends and the effectiveness of measures. There is mounting interest in CSIRT statistics among policy makers, but it is important that such statistics are of high quality and are internationally comparable if they are to inform decision making.

The 2012 OECD report on *Improving the Evidence Base for Information Security and Privacy Policies* found that many CSIRTs already generate statistics based on their daily activities, particularly statistics on the number of incidents handled (OECD 2012a). CSIRTs also collect data or potentially have access to data that could be used to generate statistics on other relevant phenomena if appropriate guidance were available. However, the quality and international comparability of these existing and potential statistics raise many challenges. The OECD is therefore working with the incident response community to develop guidance to improve the international comparability of statistics produced by CSIRTs (see OECD, 2015b, forthcoming).

Figure 5.5. **Attendants to the Annual FIRST Conference**

Number of Computer Security Incident Response Teams (CSIRT)



Source: Based on statistics from the Forum of Incident Response and Security Teams (FIRST).

StatLink http://dx.doi.org/10.1787/888933225245

5.4 Other selected trends impacting trust

Reliable trend data are difficult to obtain in this area. The following six subsections therefore examine very different aspects of the trust environment. The first considers the ongoing development of **national cybersecurity strategies** by OECD members and non-members. The second focuses on **data security breaches** involving personal data and the growth in **notification** requirements. One purpose of these notifications is to better position enforcement agencies to take appropriate measures in response. Likewise, notification is required in some circumstances to alert affected individuals who may then take steps to respond. Breach notification also enables authorities to gather statistical information to better understand the dimensions of the data security breach challenge. The third subsection explores the growth of **cyber risk insurance** markets. The fourth looks at the deployment of a promising new security measure: **DNSSEC**. The fifth subsection discusses the emergence of **transparency reporting** as a tool for better understanding the scale of government access to commercial data. The sixth and final subsection, highlights the increasing **role of the courts** in the governance of privacy and data protection.

A new generation of national cybersecurity strategies

In 2012, the OECD published a comparative analysis of the new generation of national cybersecurity strategies. The report found that in many countries, cybersecurity had become a national policy priority supported by high-level leadership. It also concluded that new national strategies were becoming integrated and comprehensive, approaching cybersecurity in a holistic manner encompassing economic, social, educational, legal, law enforcement, technical, diplomatic, military and intelligence-related aspects, and that "sovereignty" concerns were growing increasingly important (OECD, 2012c).

The 2012 report focused on the strategies of ten OECD member countries: Australia, Canada, Finland, France, Germany, Japan, the Netherlands, Spain, the United Kingdom and the United States. These strategies recognise that economies, societies and governments now rely on the Internet for many essential functions and that cyber threats are increasing and rapidly evolving. Most of the strategies aim to enhance government policy and operational co-ordination and to clarify roles and responsibilities, while calling for improved international co-operation.

Since the report was released, several other countries have pursued the development of national cybersecurity strategies. Across the OECD, new strategies have been published in Austria (2013), Belgium (2013), Hungary (2013), Italy (2013), Norway (2012), Switzerland (2012) and Turkey (2013). In addition, Japan (2013), the Netherlands (2013) and Estonia (2014) have published updates to their national strategies. In November 2014, Australia announced that it would undertake a six-month review of its strategy to identify strengths and weaknesses (Government of Australia, 2014).

In November 2014, Japan adopted its Basic Act on Cybersecurity. The Act states that cybersecurity policies shall be carried out according to the following principles: (i) ensuring the free flow of information, (ii) respecting citizen rights, (iii) taking a multistakeholder approach, (iv) co-operating internationally, and (v) promoting an advanced information and telecommunications network society. In January 2015, Japan established its Cybersecurity Strategic Headquarters, which will formulate the draft of the national cybersecurity strategy, working under the Cabinet. Japan has also established the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which functions as the headquarters' secretariat and the national cybersecurity operation centre.

Many non-OECD members have recently adopted or revised their national cybersecurity strategies, including India (2013), Kenya (2013), Latvia (2014), Qatar (2014), Russian Federation (2013), Singapore (2013), South Africa (2013), Trinidad and Tobago (2012) and Uganda (2013). Several other countries are currently in the process of developing national strategies.

In 2014, the Chinese government organised a high-level working group on cybersecurity and Internet management, chaired by the country's president. The group was formed, in part, to better co-ordinate China's Internet security policies. At present, no fewer than six different agencies and ministries provide input into China's cybersecurity policies, including the Ministry of Public Security, the State Encryption Bureau, the State Secrets Bureau, the Ministry of State Security, the Ministry of Industry and Information Technology and the People's Liberation Army. The group aims to improve co-operation among different agencies and ministries, while raising the profile of cybersecurity among leaders (Segal, 2014).

One notable trend for national cybersecurity strategies is the increasing role played by international and regional organisations in their development, implementation and evaluation. In Europe, the Cybersecurity Strategy of the European Union (2013) is accompanied by draft legislation that would oblige member states to adopt a national cybersecurity strategy. Eighteen of the European Union's 28 member states currently have a national cybersecurity strategy (ENISA, 2013).

The Organization for American States has assisted Colombia, Panama, and Trinidad and Tobago in drafting and adopting their national cybersecurity strategies. The OAS has also initiated a process with the governments of Dominica, Jamaica and Suriname to develop their national strategies, and also aims to assist Paraguay and Peru (OAS, 2014).

The African Union Convention on Cyber Security and Personal Data Protection (2014) calls on AU members to develop national cybersecurity strategies, focusing in particular on legislative reform and development, capacity building, public-private partnerships and international co-operation. Moreover, it stresses that such strategies should define organisational structures, set objectives and timeframes for successful implementation and lay the foundation for effective management of cybersecurity incidents and international co-operation.

In late 2014, ENISA published a framework for evaluating national cybersecurity strategies. It noted that many countries have different views on the intended outcomes or impacts of their strategies, or on how to achieve them (ENISA, 2014). The ENISA report suggested a number of possible key performance indicators for national cybersecurity strategies across five policy objectives: (i) developing cyberdefence capabilities, (ii) achieving cyber resilience, (iii) reducing cybercrime, (iv) developing industrial and technological resources for cybersecurity, and (v) securing critical information infrastructure.

To date, the process to revise the 2002 OECD Security Guidelines has underlined the need for national strategies to pursue the following complementary objectives: (i) create the conditions for all stakeholders to manage digital security risk to economic and social activities and foster trust and confidence in the digital environment; (ii) safeguard national and international security, and (iii) preserve human rights. Discussions supporting the revision of the 2002 OECD Recommendation also highlighted the need for further effort on ways to best support Small and Medium Enterprises and individuals, to manage digital security risks to their activities.

Data security breach notification

Notification requirements for data security breaches that affect personal data trace their origins to the United States, where virtually every state has followed in the footsteps of a 2003 breach notification law in California. The revised OECD Privacy Guidelines call for controllers to provide notifications in cases where there has been a significant security breach affecting personal data (OECD, 2013a, paragraph 15c). Countries outside the United States have begun to include data breach notification in their laws and policies.

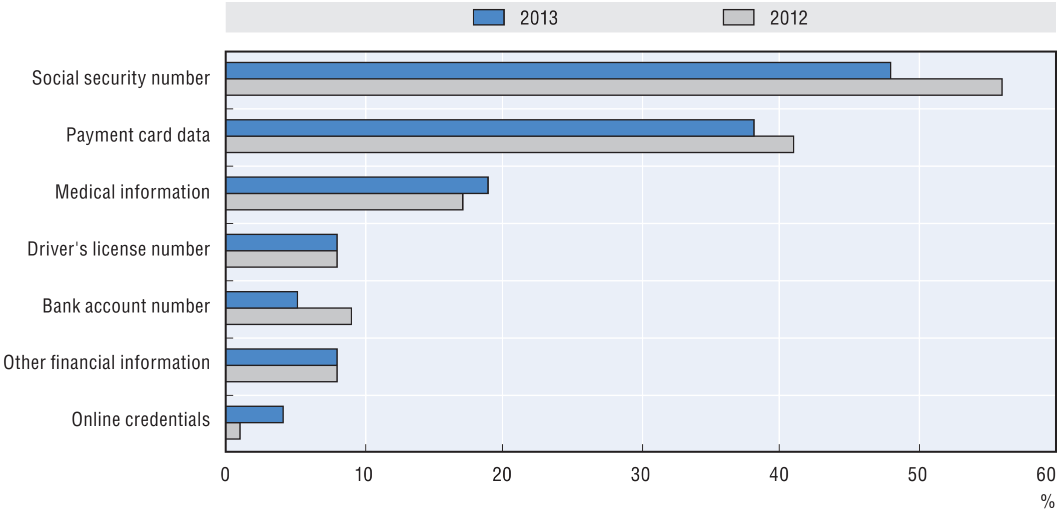
In terms of generally applicable or “ominibus” laws, Korea’s Personal Information Protection Act has a general notification requirement to relevant authorities in the event of a data breach. Meanwhile, proposed legislative reforms would make breach notification mandatory in Canada.

Sector-specific rules apply in EU/EEA countries, where breach notification requirements affecting the telecommunications sector arise out of the “e-privacy” Directive, 2002/58/EC. The required notice is directed to the relevant data protection authority and to individuals in particular circumstances, some of which vary depending on the country. Notification to an individual is required in Ireland in cases where the breach is likely to adversely affect the personal data or privacy of that individual. In Italy, preliminary notice to the Data Protection Authority must be provided within 24 hours, with additional information sent within three days via a form available on the website. In Hungary, notice is sent to the communications regulator, who may inform the public in appropriate cases. Given the potential damage from breaches in the communications sector, Korea has included additional requirements to its general notification provisions for communication service providers to notify affected individuals and relevant authorities within 24 hours of a breach. Other sector-specific requirements are in place in Canada, where they apply to the public sector, with notifications to the OPC and Treasury Boards.

There are numerous non-binding guidelines or codes of practice outlining circumstances where notification would be appropriate. In some cases, these have general application (Ireland, New Zealand) and in others they are sector specific, for example, covering health (United Kingdom). In some cases, the authority has provided guidelines for compliance. For example, the Italian Data Protection Authority issued guidelines in 2013 (DPA, 2013) addressing issues such as coverage of specific entities.

One important benefit of notification obligations is the opportunities they provide for measurement of data breaches. For example, the US state of California's data breach report, issued in October 2014, reported 167 data breaches for 2013, an increase of 28% from 2012 (OAG California, 2014).

Figure 5.6. **Types of data breached in California, 2012-13**



Note: The total is bigger than 100% because some breaches involved more than one data type.

Source: OAG California (2014).

StatLink http://dx.doi.org/10.1787/888933225252

These breaches involved the personal information of more than 18.5 million California residents, an increase of more than 600% over 2012. This rise was due largely to two massive retailer breaches, one of which – the Target breach – involved the payment card data of 41 million individuals, including 7.5 million Californian residents. A majority of reported breaches (53%) resulted from malware and hacking, affecting 93% of all compromised records.

A number of national privacy enforcement authorities have begun to publish information on the volume of data security breach notices they receive, often in annual reports (e.g. Ireland, New Zealand, United Kingdom). Anecdotal evidence suggests that enforcement activity as a result of security breaches appears to be on the rise. As an example, the French regulator has issued a public warning to Orange France in response to failures that resulted in a data security breach compromising the personal data of more than 1 million customers.[7]

Cyber insurance policies

The extension of existing insurance policies, such as those covering first-party commercial property or business interruption, to protect businesses and individual users from Internet-based risks – and more generally from risks relating to information technology infrastructure and activities – may provide sufficient coverage for some cybersecurity incidents. In practice, however, insurance companies have been traditionally averse to covering risks associated with widespread corporate use of IT infrastructure (including the Internet) or the risks associated with non-tangible assets such as data. For example, most property, business interruption, theft and terrorism policies are based on loss of – or damage to – physical assets (data is not generally considered "property") (Marsh, 2013: 5). Both liability coverage and errors and omissions coverage generally respond to negligence by the insured and do not usually cover the expenses associated with a data breach, such as customer notification costs and regulatory fines (Marsh, 2013: 10). Even kidnap and ransom insurance will generally not cover "cyber extortion" without a specific amendment (Box 5.3).

Box 5.3. **Cyber insurance policies for enhancing risk management**

Cyber insurance policies have long reflected the approach taken by organisations towards the role of ICTs in their overall functioning (i.e. relative isolation from other business processes). Accordingly, insurance policies have considered IT risk exposure in terms of technological risk (e.g. "Operational Technology" exposure). However, ICTs have progressively become essential to the functioning and development of all aspects of the value chain and competitiveness of organisations. Simultaneously, incidents are multiplying across all sectors and are generating significant losses.

Organisations are therefore progressively integrating risks related to the use of ICTs into the broader enterprise risk management framework, and are approaching it from a business needs perspective. This relatively new context provides a basis for organisations to explore the option of risk transfer, as well as the possibility of a growing "cybersecurity" risk insurance market.

The insurance market is, however, evolving to respond to increased demand for new cybersecurity risk insurance products. Specialised cybersecurity risk insurance, sometimes referred to as "cyber risk" insurance or simply "cyber" insurance, has been designed to mitigate losses from cybersecurity incidents such as data breaches, business interruption and computer network damage. Following an incident, significant costs may arise from forensic investigations, lawsuits, data breach notification expenses, regulatory investigations, regulatory fines, attorneys and consultants, public relations professionals and remedial measures (Ferrillo, 2014).

It is estimated that over 50 insurers in 2014 offered stand-alone cybersecurity risk insurance policies (Armerding, 2014). Most of these insurers are based in the United States, where the policies are commonly used to transfer risk in jurisdictions which have mandatory data breach notification laws that require organisations to inform customers when their data has been lost or stolen. According to the Ponemon Institute (2014), 26% of companies in the United States held cybersecurity risk insurance policies in 2014, up from 10% in 2013.

However, the cybersecurity risk insurance market is still nascent compared to other insurance markets. In the United States, where the market is most mature, insurers write just over USD 2.5 billion of premium income per year, equivalent to less than 0.5% of the country's commercial insurance market (Gray, 2014). The cybersecurity risk market is even smaller in Europe, where the industry writes an estimated USD 150 million worth of premiums a year (Gray, 2014). However, the number of cybersecurity risk insurance products is growing. In 2013, insurers introduced 38 new cybersecurity risk insurance products (Advisen, 2014).

National and regional regulation likely has an influence on the size and attractiveness of the cyber insurance market. For example, data breach notification laws adopted in the United States may have served as a driver for insurance, as the costs of notifying affected users can be very high. Regulatory trends in the European Union with respect to the protection of critical infrastructures could have a similar effect on the European cybersecurity insurance market.

Governments are beginning to explore ways to promote the growth of cybersecurity risk insurance markets as a means to improve overall cybersecurity risk management in organisations. For example, a robust cybersecurity insurance market may help reduce the number of successful cyber attacks by (i) promoting the adoption of risk reduction measures in return for better coverage, and (ii) encouraging the implementation of best practices by basing premiums on the insuree's level of protection (DHS, 2014). A key question – and an area for further research – relates to the potential obstacles and inhibitors preventing the cybersecurity insurance market from expanding at a faster pace.

On the supply side, lack of actuarial data has impeded the development of policies. The high prices of available policies reflect uncertainty among underwriters, who find it challenging to price risks when they lack experience with past claims. In addition, insurance coverage for cyber risks requires a significant investment by insurers in the necessary technical expertise to assess such risks. Insurers need to develop an evidence base and to refine methodologies to assess the cybersecurity risks of different industries and organisations. This is important because different industries face different kinds of cybersecurity risks.

On the demand side, an important limitation is the slow pace at which businesses have progressed in adopting a wider operational risk management approach. While many organisations are progressively adjusting their digital security risk management governance to better integrate it within the broader enterprise risk management framework, many leaders and decision makers still view "cybersecurity" as a technical issue, reducing the potential scope for insurance.

It has also been recognised that many organisations forego available insurance policies due to their perceived high cost, confusion about what they cover and how much insurance to purchase, as well as uncertainty regarding the assessment of cyber risk (DHS, 2014). It will be important to track how governments respond to ongoing developments in the cyber insurance industry, and to further ascertain which measures prove effective in strengthening and supporting the market.

Validation of Domain Name System Responses (DNSSEC Validation)

The Domain Name System (DNS) is one of the key components of the Internet, and also a critical point of vulnerability. Hostile attacks that manage to replace a genuine DNS response with a crafted response can misdirect a user's traffic to unintended locations.

This may result in a breach of confidentiality (data snooping) and/or permit the launch of various forms of deceptive attacks against the user. Internet users are placed in the position of being forced to trust the responses they receive from their queries, yet have no certain means to assure themselves that they are not being misled by a malicious third party.

The response to this vulnerability in the DNS is to add digital signatures to the DNS resource records. While this does not prevent third parties from attempting to inject false information into the DNS, it does enable a DNS resolver to validate the DNS response it receives by validating the digital signature signed across the response, thereby confirming that the received DNS information is genuine. The security technology, called Domain Name System Security Extensions (DNSSEC), defines a method for adding digital signatures to a DNS zone, and a validation procedure to authenticate both responses provided by the DNS and assertions of non-existence in the DNS for entries in signed zones.

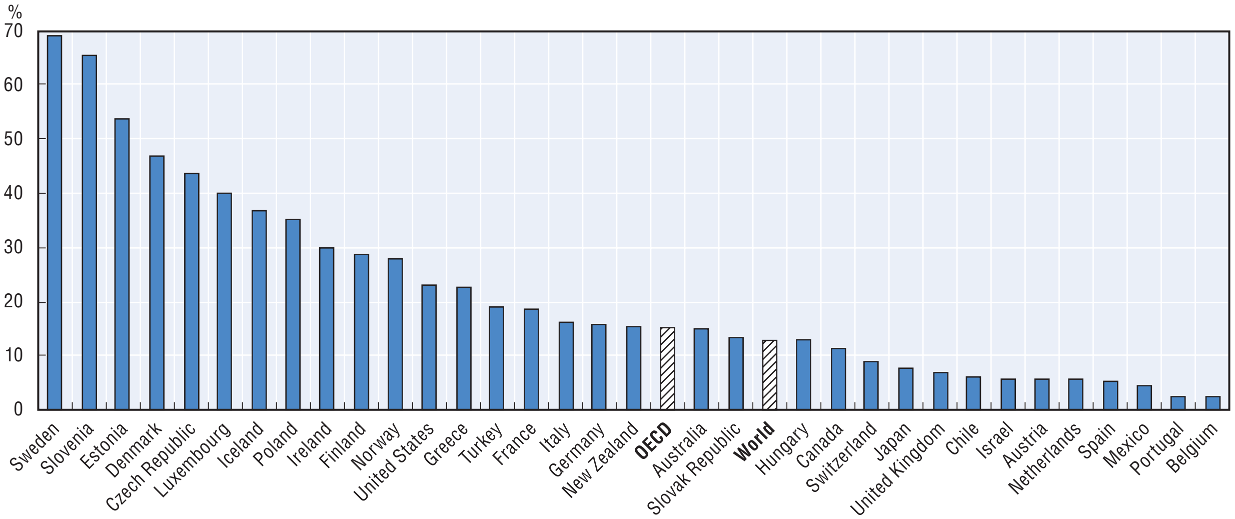
Widespread adoption of DNSSEC has the potential to significantly improve the robustness and reliability of the Internet, by providing an effective means to detect attempts to subvert the functioning of the Internet's naming system and to avoid the use of falsified DNS responses. The overall effectiveness of DNSSEC depends on two factors: the extent to which domain name zone administrators use DNSSEC to sign the contents of their DNS zone, and the extent to which clients use DNS resolvers that perform DNSSEC validation when they receive a digitally signed response. The greater the number of clients who use DNS resolvers that perform DNSSEC validation, the greater the level of motivation for DNS zone administrators to use DNSSEC to sign their zone as a measure to improve confidence in the integrity of the online services provided under the auspices of a particular DNS name.

It is possible to estimate the proportion of end users who pass their DNS queries to a DNS resolver that performs DNSSEC validation. The experimental technique[8] used to automatically gather the data (Figure 5.7) involves the presentation of a set of simple DNS tasks to a very large cross-section of users, where the task includes the resolution of a DNS name signed using DNSSEC. The users who contributed experimental results were gathered using an online advertising network with broad penetration across the entire Internet user population. Figure 5.7 shows the estimated percentage of users in each OECD country who use DNSSEC-validating DNS resolvers. Adoption of DNSSEC validation in DNS resolvers varies significantly across countries.

Several factors are hindering more widespread adoption of DNSSEC validation. Among these is the perception that efforts to improve the integrity of basic query/response transactions within DNS operation are of a lower level of relative priority than, for example, devising methods to mitigate use of the DNS as a platform for launching various forms of denial-of-service attacks. Another factor might be the relatively conservative approach of many service providers with respect to possible changes to the existing operational DNS infrastructure required for DNSSEC adoption. Considering that almost every transaction on the Internet intrinsically requires a call for DNS name resolution, and that the stability and consistency of DNS resolver operations is a critical element of online service provision, some conservatism with respect to adoption of changes to the operation of DNS services is not unreasonable.

Further studies of validation activity would be needed to corroborate the results reported in Figure 5.7. Nevertheless, the figure shows a high level of variance in the use of DNSSEC-validating resolvers across the member countries of the OECD. The exceptional

Figure 5.7. **Use of DNSSEC validation, 2015**



Note: These statistics reflect the proportion of end users who pass their DNS queries to a DNS resolver that performs DNSSEC validation from 1 January 2015 through to 22 April 2015. It does not reflect the use of DNSSEC by domain name zone administrators to sign the contents of their DNS zone.

Source: Asia Pacific Network Information Center, April 2015. *http://stats.labs.apnic.net/dnssec*.

StatLink *http://dx.doi.org/10.1787/888933225269*

results of Sweden, where almost three quarters of the national user population use DNSSEC-validating resolvers, were the result of the co-ordination of efforts undertaken by name registrants, name registrars, DNS resolver operators and governmental agencies in the country. The .se operator provided financial incentives through reduced registration fees when domain name registrars registered signed domain names in .se. Additional outreach efforts by the .se national registry to the major DNS resolver operators in Sweden prompted a number of access service operators to experiment with switching on DNSSEC validation for their customers. Following the decision of one of the largest access providers to switch on DNSSEC validation – and the lack of negative impact from the change – other major access providers in Sweden followed suit. As a result, some three quarters of Swedish Internet users now have their name queries handled by DNS resolvers which use DNSSEC to validate DNS responses when querying for names that are DNSSEC-signed. The Swedish experience suggests that co-ordinated efforts by key stakeholders can have a positive impact on the adoption rate of this promising technology.

Transparency reporting

Governments have long recognised the importance of accessing data about citizens to achieve public interest objectives, particularly in the context of law enforcement and national security. As more and more human activity generates data that traverses global commercial networks, government actors are increasingly looking to communications providers and Internet intermediaries to help meet their data needs. Laws and oversight mechanisms shape government access to this type of data, but government power may also induce business co-operation beyond what is mandated by data access provisions.

Today there are concerns about the level of transparency regarding the scale and scope of access to commercial data for law enforcement and national security purposes. Laws and agency practices in these areas typically impose secrecy requirements on the commercial targets of access requests. The result is an increasing flow of data from businesses to government that is largely opaque to the customers and citizens whose data are at issue.

Fostering trust in the digital economy though improved transparency is a long-standing OECD objective. The "openness" principle of the OECD Privacy Guidelines dates back to the original 1980 adoption and counsels in favour of a general policy of openness about the processing of personal data. The 2011 OECD Recommendation on Principles for Internet Policy Making (IPPs) also calls for policies that ensure transparency, fair process and accountability. It recognises that policy making for the Internet should promote openness and be grounded in respect for human rights and the rule of law.

Transparency is an important means of ensuring trust in an organisation, particularly where it handles personal data. Concerns about government access requests – particularly to data entrusted to providers of cloud computing services – predate the revelations by Edward Snowden in 2013 and are not limited to intelligence gathering. But it is clear that those revelations have brought into sharper focus the need for transparency. Today, Internet and communications businesses with large data holdings about individuals are under market pressure to be much more open about the manner in which they respond to government access requests.

Responding to those market pressures in a manner consistent with government rules and practices can be difficult for businesses. As mentioned above, law enforcement and national security legislation often includes restrictions preventing businesses from disclosing information relating to government access demands, barring even the disclosure of aggregate statistics. In many countries, commercial operators are also prohibited from providing the public with any insight into the manner in which they respond to those demands. These restrictions can make it difficult for companies to respond to public demand for greater transparency.

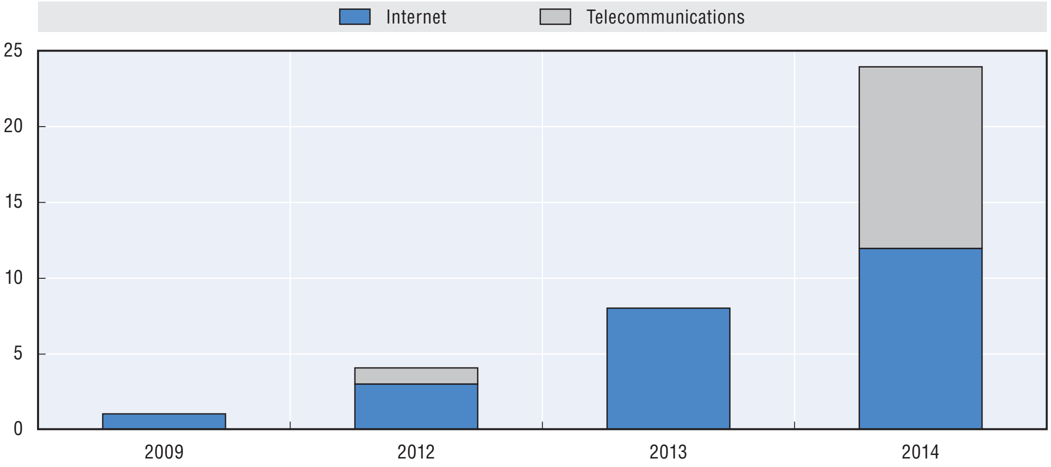
In 2011, The Privacy Projects (TPP) began to study the issues surrounding systematic government access to commercial data through a series of expert reports and roundtable discussions. One of the key findings from that work is the existence of a serious transparency gap surrounding both the laws and governmental agency practices (Box 5.4).

Box 5.4. **Preliminary findings from TPP work**

- Systematic access demands do appear to be growing, although the recent disclosures make it clear that governments are not only demanding stored data in bulk, but also are tapping into cables to collect or filter large swaths of data as it moves across the Internet.
- There is a profound lack of transparency about countries' laws and practices. Relevant laws are at best vague, and government interpretations of them are often hidden, especially in the national security realm.
- In particular, published laws and policies do not expressly address the unique challenges of bulk collection.
- Plummeting data storage costs and enhanced analytical capabilities spur governments' appetites to collect more data.
- As Internet-based services have become globalised, surveillance has become trans-border, posing increased legal and reputational risks to businesses operating globally.

One response to this situation has been an effort by companies to shed light on the issue through the publication of transparency reports. Since the release of the first such report by Google in 2009, more than 30 companies have issued public reports.[9] According to the Transparency Reporting Index, as of November 2014 there are 37 companies reporting on transparency. Out of these, 65% are Internet companies, while 35% are telecommunications firms. Out of 37 companies, around two thirds began reporting in 2014. The majority of companies report on a six-month basis (54%), and 32% prefer to do so on a yearly basis (Figure 5.8).

Figure 5.8. **Company transparency reporting, 2009-14**



Source: Based on data from the Transparency Reporting Index, November 2014. *https://www.accessnow.org/pages/transparency-reporting-index.*

StatLink http://dx.doi.org/10.1787/888933225279

These reports represent an important step forward in increasing the transparency associated with government access to commercial data. However, there is little consistency or comparability in the reports produced so far. For example:

- Some report on the number of individual demands received, while others report on the cumulative number of targeted accounts, communications services or subscribers.
- Sometimes multiple legal powers are used to obtain the same record, creating classification challenges.
- The same demand may be described or disclosed in a different way by different companies. There are therefore significant risks of over-counting/under-counting (Vodaphone, 2014).

While governments have begun to acknowledge the need to improve transparency and are taking steps in that direction,[10] more work is needed to improve public understanding about how governments access and use commercial data. Transparency reports are an important step forward in this regard, but work is needed to improve the quality and comparability of these reports and to identify unnecessary barriers to making these improvements.

The role of the courts

Courts have begun asserting greater influence over the rules governing privacy and data protection. The shift is most pronounced in the European Union, where the Court of Justice issued three significant rulings in 2014.[11] One ruling struck down the EU Data

Retention Directive, which obliged communications companies to retain communications metadata for law enforcement access. The Court considered that the Directive interfered with the fundamental right to private life and the protection of personal data.

A second key ruling involved the search engine Google, which interpreted the EU data protection directive as establishing a limited right for individuals to have search engines delete material from search results (commonly referred to as the "right to be forgotten").[12] The ruling places Google in the position of evaluating whether a link should be removed. As of January 2015, Google had removed approximately 40% of the 700 000 URLs it evaluated, amounting to nearly one quarter of a million links (Google, 2014).

The final ruling involved the "household exception", which exempts certain types of domestic processing from data protection rules. A homeowner's decision to install a CCTV camera succeeded in helping him identify individuals who attacked the property. However, the court ruled that because the cameras partially monitored a public space, the household exemption did not apply and that therefore the homeowner should have complied with the relevant data protection rules.

According to one commentator, the cumulative effect of these three rulings is to suggest increasing discomfort on the part of the court regarding society's dependence on data (Ustaran, 2014). The impact of these rules goes well beyond the particular parties to the cases, setting standards across Europe. The Google case, in particular, raises issues related to the role of intermediaries, extraterritorial jurisdiction, and the challenges of balancing data protection with other fundamental rights. Likewise, a challenge to the Safe Harbor arrangement under the EU Charter of Fundamental Rights, referred to the CJEU in June 2014 by the Irish High Court, could allow for an overturning of the adequacy finding for Safe Harbor by the European Commission. If the decision were to lead to the overturn of Safe Harbor, it would have direct implications for the governance of data flows.

While the evolving role of the judiciary is most pronounced in the European Union, there are other court decisions with significant policy implications. In a case that is still pending, a New York court is considering a challenge by Microsoft to an effort by a US prosecutor to gain access to emails held on a Microsoft server in Ireland, without using existing treaty-based arrangements. The government of Ireland has intervened in the case on the side of Microsoft, arguing that it is illegal under Irish data protection law for Microsoft to provide the data to the US authorities without approval by the Irish courts. The case raises important issues regarding the trust individuals can place in the privacy protections of their own laws and courts. A number of US business associations have also filed briefs in the proceedings, arguing that law enforcement access requests place at risk much of the benefits promised by cloud computing.[13]

Although the role of courts, and particularly appellate courts, has been less evident in the context of security issues, some commentators see signs of new developments regarding liability in tort for cybersecurity breaches (Rosenzwieg, 2013). Where a security breach involves payment card data, card issuers have begun to look to the affected retailer to recover the costs of reissuing cards.[14] Government efforts to promote good practices, such as the Framework for Improving Critical Infrastructure Cybersecurity, released by the US National Institute of Standards and Technology in 2014, may provide a de facto standard for determining negligence in the event of a cyber incident (NIST, 2014).

Notes

1. For more information, see *www.privacylaws.com/Privacy-Officers-Network/*.
2. For more information, see *www.afcdp.net/*.
3. For more information, see *www.apep.es/*.
4. These guidelines are currently under review. For more information, see *http://oe.cd/security-guidelines-review*.
5. "No one nation can have full insight into the world's networks; we have an obligation to share our insights about our own networks and collaborate with others when events might threaten us all. As we continue to build and enhance our own response capabilities, we will work with other countries to expand the international networks that support greater global situational awareness and incident response – including between government and industry." (White House, 2011: 19)
6. "[C]oordinated national, regional and international action is required for prevention, preparation, response and recovery from computer security incidents" (ITU, 2010: 1)
7. The CNIL was notified of the breach, which happened due to a technical error by one of the phone company's providers, in April 2014. (All publicly available EU electronic communications services are obliged to report data breaches to the regulator.) In May, the CNIL carried out an inspection on Orange and its subcontractors, and found gaps in data security. According to the CNIL, the company claimed to have taken all necessary measures to fulfil its data security obligations, but had not conducted a sufficient security audit before using a certain technical solution for sending email campaigns.
8. For more details about the methodology, see Huston (2012, 2013).
9. Access maintains a compilation here: *www.accessnow.org/pages/transparency-reporting-index*.
10. The US Department of Justice authorised greater disclosures in January 2014, in response to a lawsuit brought by a number of Internet companies. President Obama called for still greater transparency in a February 2014 speech.
11. The first is called C-293/12 and C-594/12 Digital Rights Ireland. For more information see *http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=313440*.
12. The ruling is available at: *http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=152065&occ=first&dir=&cid=45442*.
13. Documentation and commentary about the case, including the legal briefs and opinions, are maintained at *www.digitialconstitution.com* (accessed 6 January 2015).
14. For more information see "In re: Target Corp. Customer data Security Breach Litigation", Memorandum and Order (US Dist. Ct. Minn.) (2 December 2014), *http://cdn.arstechnica.net/wp-content/uploads/2014/12/document3.pdf*.

References

Advisen (2014), *20% New Cyber Insurance Products Uptick in 2013*, Advisen, New York, *www.cyberrisknetwork.com/2014/01/31/new-cyber-insurance-products-20-percent-uptick-in-2013/* (accessed 25 April 2015).

Armerding, T. (2014), "Cyber insurance: Worth it, but beware of the exclusions", *CSO Online*, 20 August 2014, *www.csoonline.com/article/2835274/cyber-attacks-espionage/cyber-insurance-worth-it-but-beware-of-the-exclusions.html* (accessed 25 April 2015).

Bamberger, K. and D. Mulligan (2010), "Privacy on the Books and on the Ground", *Stanford Law Review*, Vol. 63/2, pp. 247-315.

Barrett, C. (2014), "Skills gap leaves UK vulnerable to cyber attack, says business", *Financial Times*, 6 August 2014, *www.ft.com/intl/cms/s/0/76b1eef4-1d3c-11e4-8b03-00144feabdc0.html#axzz3XOcYy48T* (accessed 15 April 2015).

BIS (2014), *Information Security Breaches Survey 2014: Technical Report*, UK Department for Business, Innovation and Skills, London, *www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf*.

CIGI (2014), *CIGI-Ipsos Global Survey on Internet Security and Trust*, Centre for International Governance Innovation, Waterloo, ON, *www.cigionline.org/internet-survey* (accessed 15 April 2015).

Cabinet Office of Japan (2014), "Policy Outline of the Institutional Revision for Utilization of Personal Data" Cabinet Office of Japan, Tokyo, *http://japan.kantei.go.jp/policy/it/20140715_2.pdf*.

Choe Sang-Hun (2014), "Theft of data fuels worries in South Korea", *New York Times*, 20 January 2014, *www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html?_r=1* (accessed 15 April 2015).

Clearwater, A. and J.T. Hughes (2013), "In the Beginning … An Early History of the Privacy Profession", *Ohio State Law Journal*, Vol. 74/6, pp. 897-921, *http://moritzlaw.osu.edu/students/groups/oslj/files/2013/12/8-Clearwater-Hughes.pdf*.

Coughlan, S. (2014), "Cyber-attacks increase leads to jobs boom", *BBC News*, *www.bbc.com/news/business-26647795* (accessed 15 April 2015).

DHS (2014), *Cybersecurity Insurance*, US Department of Homeland Security, Washington DC, *www.dhs.gov/publication/cybersecurity-insurance* (accessed 15 April 2015).

DPA (2013), *Implementing Measures with Regard to the Notification of Personal Data Breaches*, 4 April 2013, Italian Data Protection Authority, Rome, *www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2414592* (accessed 15 April 2015).

EC (2015), *Special Eurobarometer 423: Cyber Security Report*, European Commission, Brussels, *http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf*.

EDPS (2014), Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition and Consumer Protection in the Digital Economy, European Data Protection Supervisor, Brussels, *https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf*.

ENISA (2014), *An Evaluation Framework for Cyber Security Strategies*, European Union Agency for Network and Information Security, Haraklion, Crete, *www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1* (accessed 15 April 2015).

ENISA (2013), *National Cyber Security Strategies in the World*, European Union Agency for Network and Information Security, Haraklion, Crete, *www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world* (accessed 15 April 2015).

FCC (2014), *FCC Joins Global Privacy Enforcement Network*, Press release, Federal Communications Commission, Washington DC, *www.fcc.gov/document/fcc-joins-global-privacy-enforcement-network* (accessed 15 April 2015).

Ferrillo, P. (2014), *Cyber Security, Cyber Governance, and Cyber Insurance*, Harvard Law School Forum on Corporate Governance and Financial Regulation, Cambridge, MA, *http://corpgov.law.harvard.edu/2014/11/13/cyber-security-cyber-governance-and-cyber-insurance/* (accessed 25 April 2015).

Google (2014), "European privacy requests for search removals", *Tranparency Report*, *www.google.com/transparencyreport/removals/europeprivacy/?hl=en* (accessed 15 April 2015).

Government of Australia (2014), *Cyber Security Review*, Government of Australia, Canberra, *www.pm.gov.au/media/2014-11-27/cyber-security-review-0* (accessed 15 April 2015).

Gray, A. (2014), "Cyber insurance market tempts new participants", *Financial Times*, 6 October 2014, *www.ft.com/intl/cms/s/0/69db580c-4d37-11e4-8f75-00144feab7de.html* (accessed 15 April 2015).

HM Government (2014), *Cyber Security Skills: Business Perspectives and Government's Next Steps*, HM Government, London, *www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf*.

Home Depot (2014), *The Home Depot Reports Findings in Payment Data Breach Investigation*, Press release, *https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf*.

Humber, Y. and G. Reidy (2014), "Japan takes its first step to fight hackers", *Bloomberg Business*, 24 July 2014, *www.bloomberg.com/bw/articles/2014-07-24/proposed-law-would-fix-japans-lax-cybersecurity* (accessed 15 April 2015).

Huston, G. (2013), "DNS, DNSSEC and Google's public DNS service", *CircleID* blog, 17 July 2013, *www.circleid.com/posts/20130717_dns_dnssec_and_googles_public_dns_service/* (accessed 15 April 2015).

Huston, G. (2012), "Counting DNSSEC", *RIPE Network Coordination Centre*, *https://labs.ripe.net/Members/gih/counting-dnssec* (accessed 15 April 2015).

IAPP (2014), "Benchmarking privacy management and investments of the Fortune 1000", *International Association of Privacy Professionals* (IAPP) website, *https://privacyassociation.org/resources/article/benchmarking-privacy-management-and-investments-of-the-fortune-1000-2/* (accessed 15 April 2015).

IAPP (2013), "IAPP Privacy Professionals Role, Function and Salary Survey", *International Association of Privacy Professionals* (IAPP) website, *https://privacyassociation.org/resources/article/2013-iapp-privacy-professionals-role-function-and-salary-survey* (accessed 15 April 2015).

(ISC)^2 (2011), *Annual Report 2010*, International Information Systems Security Certification Consortium, Palm Harbor, FL, *www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Annual_Reports/2010%20Annual%20Report.pdf*.

ITU (2010), Resolution 130: Strengthening the Role of ITU in Building Confidence and Security in the Use of Information and Communication Technologies, Plenipotentiary Conference of the International Telecommunication Union, Guadalajara, *www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_130.pdf*.

Junker, J-C. (2014), *A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change*, Strasbourg, *http://ec.europa.eu/priorities/docs/pg_en.pdf#page=6*.

Madden, M. (2014), "Few feel that the government or advertisers can be trusted", *Pew Research Center*, 12 November 2014, *www.pewinternet.org/2014/11/12/few-feel-that-the-government-or-advertisers-can-be-trusted/* (accessed 15 April 2015).

Marsh (2013), *Cyber Risks Explained: What They Are, What They Could Cost and How to Protect Against Them*, March & McLennan Companies, New York, *http://uk.marsh.com/Portals/18/Documents/Cyber_risk_client_briefing_FINAL_exp%20Apr13.pdf*.

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, Gaithersburg, MD, *www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*.

NYMITY (2014), *Global Privacy Research Report 2014*, NYMITY, Toronto, ON, *www.nymity.com/innovations/privacy-research-2014-infographic/~/media/NymityAura/Resources/Research/Global-Privacy-Research-Report-2014.pdf*.

OAG California (2014), *California Data Breach Report 2014*, Office of the Attorney General, California Department of Justice, Sacramento, CA, *http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2014data_breach_rpt.pdf*.

OAS (2014), "OAS begins supporting Suriname in the development of a national cyber security plan", Press release. Organization of American States, Washington DC, *www.oas.org/en/media_center/press_release.asp?sCodigo=E-555/14* (accessed 15 April 2015).

OECD (2015a), *Data Driven Innovation for Growth and Well-Being*, OECD Publishing, Paris.

OECD (2015b), *Improving the International Comparability of Statistics Produced by Computer Security Incident Response Team*, OECD Publishing, Paris.

OECD (2014), *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, DOI: 10.1787/9789264221796-en.

OECD (2013a), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, *http://oe.cd/privacy*.

OECD (2013b), *The OECD Privacy Framework*, OECD Publishing, Paris, *http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*.

OECD (2012a), *Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online*, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/5k4dq3rkb19n-en*.

OECD (2012b), *Internet Economy Outlook 2012*, OECD Publishing, Paris, *www.oecd.org/sti/ieconomy/oecd-internet-economy-outlook-2012-9789264086463-en.htm*.

OECD (2012c), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", *OECD Digital Economy Papers*, No. 211, OECD Publishing, Paris, DOI: *http://dx.doi.org/10.1787/5k8zq92vdgtl-en*.

OECD (2011a), *Recommendation on Principles for Internet Policy Making*, OECD, Paris, *www.oecd.org/sti/ieconomy/49258588.pdf*.

OECD (2011b), *Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, DOI: 10.1787/5kgdpm9wg9xs-en.

OECD (2007), *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, *www.oecd.org/sti/ieconomy/privacylawenforcementco-operation.htm* (accessed 15 April 2015).

OPC (2014a), *Joint Open Letter to App Marketplaces*, Office of the Privacy Commissioner of Canada, Ottawa, *www.priv.gc.ca/media/nr-c/2014/let_141210_e.asp* (accessed 15 April 2015).

OPC (2014b), *Global Cross Border Enforcement Cooperation Arrangement*, Office of the Privacy Commissioner of Canada, Ottawa, *www.privacyconference2014.org/media/16667/Enforcement-Cooperation-Agreement-adopted.pdf*.

OPC and ICO (2014), *Resolution on Enforcement Cooperation*, 36th International Conference of Data Protection and Privacy Commissioners, Office of the Privacy Commissioner of Canada, Ottawa, and Information Commissioner's Office, Wilmslow, UK, *www.privacyconference2014.org/media/16430/Resolution-International-cooperation.pdf*.

PHAEDRA (2014), *Workstream 1 Report: Co-ordination and Co-operation Between Data Protection Authorities*, PHAEDRA, *www.phaedra-project.eu/wp-content/uploads/PHAEDRA-D1-30-Dec-2014.pdf*.

Ponemon Institute (2014), "2014 Cost of Data Breach Study", *www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/* (accessed 15 April 2015).

Rosenzweig, P. (2013), "When companies are hacked, customers bear the brunt. But not for long", *New Republic*, 15 October 2013, *www.newrepublic.com/article/115187/cybersecurity-liability-court-cases-are-changing-blame-game* (accessed 15 April 2015).

Science (2015), "The end of privacy", *Science*, Special Issue, 30 January 2015, *www.sciencemag.org/site/special/privacy/index.xhtml* (accessed 15 April 2015).

Segal, A. (2014), "China's new small leading group on cybersecurity and Internet management", *Forbes*, 27 February 2014, *www.forbes.com/sites/adamsegal/2014/02/27/chinas-new-small-leading-group-on-cybersecurity-and-internet-management/* (accessed 15 April 2015).

Somogyi, S. (2014), "Making end-to-end encryption easier to use", *Google Online Security Blog*, 3 June 2014, *http://googleonlinesecurity.blogspot.fr/2014/06/making-end-to-end-encryption-easier-to.html* (accessed 15 April 2015).

Taddicken, M. (2014), "The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived societal relevance on different forms of self-disclosure", *Journal of Computer-Mediated Communication*, Vol. 19, pp. 248-273. DOI: 10.111/jcc4.12052.

Tene, O. (2015), "Privacy is the New Antitrust: Launching the FTC Casebook", *International Association of Privacy Professionals* (IAPP) website, 15 January 2015, *https://privacyassociation.org/news/a/privacy-is-the-new-antitrust-launching-the-ftc-casebook/* (accessed 15 April 2015).

UN (2013), *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations, New York, *www.un.org/ga/search/view_doc.asp?symbol=A/68/98* (accessed 24 April 2014).

US DoJ (2014), "U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator", US Department of Justice, Washington DC, *www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware* (accessed 15 April 2015).

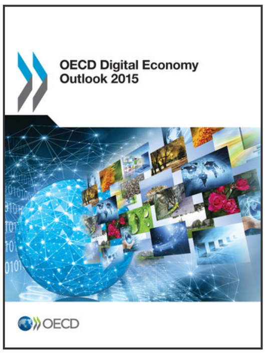
US GAO (2015), *High Risk List*, US Government Accountability Office, Washington DC, *www.gao.gov/highrisk/overview* (accessed 15 April 2015).

Ustaran, E. (2014), "The judiciary v. the surveillance society", *LinkedIn* blog, 15 December 2014, *www.linkedin.com/pulse/judiciary-v-surveillance-eduardo-ustaran?trk=object-title* (accessed 15 April 2015).

Vodaphone (2014), *Sustainability Report 2013/14*, Vodaphone, Newbury, UK, *www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf*.

White House (2015), "State of the Union Address", White House, Washington DC, *www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015* (accessed 15 April 2015).

White House (2011), *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, White House, Washington DC, *www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf*.



From:

OECD Digital Economy Outlook 2015

Access the complete publication at:

https://doi.org/10.1787/9789264232440-en

Please cite this chapter as:

OECD (2015), “Trust in the digital economy: Security and privacy”, in *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/9789264232440-7-en