OECD publishing

OECD DIGITAL ECONOMY PAPERS
No. 254

# MANAGING DIGITAL SECURITY AND PRIVACY RISK

## 2016 MINISTERIAL MEETING ON THE DIGITAL ECONOMY

## BACKGROUND REPORT

2016 MINISTERIAL MEETING
THE DIGITAL ECONOMY:
INNOVATION, GROWTH
AND SOCIAL PROSPERITY

OECD
BETTER POLICIES FOR BETTER LIVES

## FOREWORD

This report was prepared as part of the documentation for Panel 3.2 of the OECD Ministerial Meeting on the Digital Economy, "Managing Digital Security and Privacy Risk for Economic and Social Prosperity". It discusses how the economic and social dimensions of digital security and privacy risk have changed in the context of a hyper connected digital environment and data-driven innovation. It articulates why a risk management approach is essential in this new environment to realise the economic and social benefits of the digital economy. It reviews the special challenges for business, with particular attention to SMEs.

Preparation of the document was undertaken by Elettra Ronchi and Laurent Bernat (OECD), with the contribution of Carman Baggaley, (former strategic policy advisor, of the Office of the Privacy Commissioner of Canada) and the support of an informal expert group with representation from Australia, Canada, France, Germany, Italy, Japan, Korea, Portugal, Turkey, the United Kingdom, the United States, the Business Industry Advisory Committee, the Civil Society Information Society Advisory Council, and the Internet Technical Advisory Committee.

This report was approved and declassified by the Committee on Digital Economy Policy on 13 May 2016 and prepared for publication by the OECD Secretariat.

Note to Delegations:
This document is also available on OLIS under reference code:
DSTI/ICCP/REG(2016)1/FINAL

## TABLE OF CONTENTS

## EXECUTIVE SUMMARY

Increasing connectivity and data-intensive economic activities – in particular, those that rely on large streams of data ("big data"), and the emerging Internet of Things – have the potential to foster innovation in products, processes, services and markets and help address social and global challenges. These developments have been accompanied by a change in the scale and scope of digital security and privacy risk with potential significant impacts on social and economic activities. These developments underscore the need for an evolution in policies and practices to build and maintain trust.

### *Digital security incidents undermine innovation, create privacy risk and erode trust*

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

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 policy areas with only broadband availability ranking higher. Consumers are also increasingly paying attention to privacy in the digital environment. A 2014 CIGI-Ipsos survey of Internet users in 24 countries on Internet security and trust suggested that 64% of respondents are more concerned about privacy than they were a year earlier.

### *Risk Management can help ensure digital security measures protect and support economic and social activities*

Robust strategies to manage digital security risk are essential to establish the trust needed for economic and social activities to fully benefit from digital innovation.

The OECD's 2015 *Recommendation on Digital Security Risk Management for Economic and Social Prosperity* (*Security Risk Recommendation*) sets out a risk management policy framework to address digital security issues with three messages:

- It is impossible to entirely eliminate digital security risk when carrying out activities that rely on the digital environment. However, the risk can be managed, that is, can be reduced to an acceptable level in light of the interests and benefits at stake, and the context.

- Leaders and decision makers should focus on the digital security risk to economic and social activities rather than only on the risk to the digital infrastructure.

- Organisations should integrate digital security risk management into their economic and social decision making processes and overall risk management framework rather than treating it solely as a technical problem.

***Privacy Risk Management can enhance Privacy Protection***

The OECD 2013 *Guidelines Governing the Protection of Privacy and Transborder Data Flows* (the 2013 OECD Privacy Guidelines) also recommend taking a risk-based approach to implement the privacy principles and enhance privacy protection. Furthermore, privacy risk management can contribute to global interoperability of privacy protection frameworks. However, while the concept of risk management is well-established in the digital security space, more work is needed to determine how it can be applied to privacy protection and there is debate about how to implement a comprehensive risk management approach to strengthen the application of the well-established OECD Privacy Guidelines' principles.

***Further work is needed to understand how organisations can be incentivised to integrate privacy risk management in their decision making and risk management frameworks***

Many organisations still tend to approach privacy solely as a legal compliance issue rather than also as an economic and social risk, and a strategic issue that could provide them with a competitive advantage in the marketplace. In deciding how to treat privacy risk, organisations need to take into account the social and economic objectives they are pursuing. Like all forms of risk, privacy risk should not be assessed in isolation but rather in relation to the potential benefits. A number of potential benefits could be realised if privacy risk were addressed as part of the broader economic risk management framework of organisations and integrated in economic and social decision-making.

Further, privacy compliance obligations could be complemented by other measures aiming to turn privacy protection into a market differentiator, i.e., a factor on which business competes, thereby increasing individuals' choice in the market and improving overall privacy. Ideally, the market should reward effective privacy risk management. Currently, there is only scattered evidence about the market effects of companies' privacy failures. More research is needed to understand which market-based incentives could encourage organisations to address privacy protection as a business risk and an opportunity that could enhance their reputation, revenues, and trust in the marketplace.

***National strategies to manage digital security risk and protect privacy can encourage collaboration and knowledge sharing***

The Security Risk Recommendation and the Privacy Guidelines both call for the development of flexible and technology-neutral whole-of-society national strategies supported at the highest level of government to address digital security and privacy risk. The openness and interconnectedness of the digital ecosystem produces many economic and social benefits; it also makes devices, systems and networks more vulnerable to attacks, and can create privacy risk. Creating a risk-free environment without threatening these benefits is impossible. Therefore, all stakeholders need to work together to create an environment that promotes effective digital security and privacy risk management.

National strategies developed in concert with all stakeholders can create the conditions for greater stakeholder collaboration in relation to risk management at both policy and operational levels, for example, by promoting the sharing of knowledge, know-how, and experience on successful practices.

Such strategies can foster international cooperation and help guide cross-border efforts to address digital security risk, strengthen privacy protection and lessen uncertainty for transborder personal data flows.

***Special attention is essential to address the needs of SMEs***

Small and medium enterprises (SMEs), and early-stage start-ups in particular, are critical to economic growth; they drive competition and innovation, and contribute to job creation. They also face distinct challenges in managing digital security and privacy risk. A digital security incident that can result in a loss

of consumer trust, damage to reputation, or a drop in revenue, may be more damaging for SMEs than for larger companies because they are more likely to find it difficult to weather a temporary loss of customers or revenue. As well, they may not have the resources or expertise to effectively assess and manage risk. On the positive side, SMEs that are aware of the risk and can demonstrate that they have robust digital security and privacy practices may have a competitive advantage when seeking partnership opportunities with larger organisations. In order to help SMEs realise these opportunities, it is essential to increase SMEs awareness and promote adoption of good practice. Useful approaches could include the development of SME-specific risk management guidance tools and incentives, for example, by leveraging digital risk insurance.

# INTRODUCTION

The digital world is not static and continues to experience very rapid development. The widespread changes brought about by today's digital environment have significantly broadened the scale of digital security and privacy challenges, signalling the need for an evolution in how these risks are managed. Effective management of digital security and privacy risk is essential if countries are to realise the full economic and social benefits of the digital economy. Establishing higher levels of trust with users and customers may enable digital services to become more widely accepted and used by individuals and organisations. Governments play a key role in supporting conditions to build trust and complement private sector initiatives.

Trust is essential in situations where uncertainty and interdependence exist (Mayer, 1995), and the digital environment certainly encapsulates those factors. Today's digital economy relies on an intricate, hyper-connected information and communication technology (ICT) ecosystem based on the processing of large streams of data ("big data") enabled by sophisticated data analytics and the widespread use of mobile connectivity .These developments, combined with the emerging use of the Internet to connect computers and sensor-enabled everyday devices (the "Internet of Things"), add layers of complexity, volatility, and dependence on infrastructures and processes not fully within single jurisdictional and organisational control.

The result is that risk is a cross-boundary, cross-sector, and multi-stakeholder issue. What happens in a small business can affect a large business and all other actors within a value chain; what one actor (individual or group) does may affect many others. The converse is also true: organisations, whether functioning in the public or private sector, are doubtlessly benefitting from greater interconnectivity to drive innovation, and improve their efficiency and performance. The value chain ecosystem can also be used to raise the level of digital risk management across a range of organisations, for example by requiring a certain level of security risk management along a supply chain.

In this environment, data have become a core asset. The OECD refers to the increased use of large and disparate volumes of data and of analytics to significantly improve or foster the development of new products, processes, organisational methods and markets as "data-driven innovation" (DDI). DDI can create significant added value to a variety of operations, ranging from optimising and reengineering the value chain and manufacturing production to more efficient use of resources, better customer relationships, and the development of new markets. Equally important, DDI can also help address a range of social and environmental challenges, including improving health outcomes and social well-being of people, increasing food production, responding to natural disasters; and reducing the impact of climate change. The intensive exchange and use of large streams of data can, however, also facilitate privacy-intrusive uses of information and create digital security risks.

There is a need to acknowledge the increased uncertainty that can result from these new developments and the need for evolution in current digital security risk and privacy-protective strategies to deal with the emerging new vulnerabilities and threats, while taking into account the economic and social potential of the digital economy.

Various technological solutions to improve digital security exist and more are being developed. Yet to optimise the economic and social benefits anticipated from an open digital environment, leaders and decisions makers should no longer treat digital security risk solely as a technical issue but adopt an economic and social risk management approach.

This represents one of the key messages of the OECD's 2015 *Recommendation on Digital Security Risk Management for Economic and Social Prosperity* (Security Risk Recommendation). The Security

Risk Recommendation calls on leaders and decision makers to integrate digital security risk management in their economic and social decision making processes and broader risk management framework. Digital security risk management helps ensure that security measures do not undermine the economic and social activity they aim to protect, are appropriate to and commensurate with the risks faced, and take into account the interests of others.

Similarly, the 2013 revision of the OECD Privacy Guidelines emphasises the importance of applying the concept of risk to best implement the OECD privacy principles in a data driven economy. One of the key changes in the 2013 revisions to the OECD Privacy Guidelines is the inclusion of a new section that introduces the concept of risk-based Privacy Management Programme (PMP) and articulates its essential elements. The PMP is the primary operational vehicle through which an organisation is expected to give practical effect to the basic principles contained in the OECD Privacy Guidelines.

Protection of data and personal information from potential threats should also be part of an organisation's overall risk management strategy, as it can offer a competitive advantage to an organisation and deliver the means for more effective innovation and greater performance. Individuals are increasingly choosing to do business with organisations that are sensitive to privacy concerns.

Taking note of these issues and the changing digital economy landscape, policy makers, academics and privacy professionals have recently started to think about how best to apply the concept of risk management to make the protection of privacy more rigorous and more effective. While the importance of the concept is established, we are only now beginning to explore the practical aspects of its implementation in the area of privacy protection. For example, the 2013 OECD Privacy Guidelines do not elaborate on how such an approach would work in practice.

With respect to digital security issues, although risk management is not a new concept, there are also significant implementation challenges. The Security Risk Recommendation, for example, recognises that applying risk management practices raises challenges for stakeholders with limited capacity and resources to act, such as SMEs and individuals.

This paper aims to address these issues by first elaborating on how the economic and social dimensions of digital security and privacy risk have changed in the context of a hyper connected digital environment and data-driven innovation. Next, the paper introduces the Security Risk Recommendation, the concept of risk management and its application to digital security. The paper then articulates why the risk management approach is important to the implementation of the 2013 OECD Privacy Guidelines. It clarifies how to understand the distinction between risks to the organisation and risks to individuals and society and considers the challenges and opportunities in implementing privacy risk management. It then reviews the special challenges for business, with particular attention to SMEs.

## THE ECONOMIC AND SOCIAL DIMENSIONS OF DIGITAL SECURITY AND PRIVACY RISK: EVIDENCE OF A CHANGE IN SCALE

In a 2014 OECD survey on the digital economy, governments identified security as the second highest policy priority area and privacy as the third out of 31 possible priority areas, with only broadband availability ranking higher (OECD, 2015a). In 2015, privacy was added to cybersecurity on the US Government's "High Risk List" (US GAO, 2015).

The increase in data breaches and the greater importance of Data-Driven Innovation (DDI) have elevated the visibility of digital security and privacy challenges. At the same time, the increasing prominence of these issues is also 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.

For many businesses and governments across OECD and its partner economies, analytical techniques and technologies for processing and analysing large volumes of data, commonly known as "big data", are becoming an important resource and have already created significant added value in a variety of operations across all stages of the value chain, from more efficient use of labour, to improved products and services, and better customer relationships. The confluence of several trends, including the increasing migration of socio-economic activities to the Internet, and the decline in the cost of data collection, storage and processing, has contributed to what is now commonly referred to as DDI. In particular, cloud computing has played a significant role by increasing the capacity to store and analyse data (OECD, 2015b).

Equally important, DDI can also help address social and global challenges, including climate change and natural disasters, ageing populations, food production, energy security, and mass urbanisation. The effectiveness and efficiency of the health care system can also be improved by using big data. Big data can help identify people who are at risk and it can be used to personalise treatment and medication based on a person's unique genetic makeup and data on their lifestyle and environment. Aggregate health and wellness data can improve the post-market surveillance of drugs and medical devices by revealing unforeseen adverse drug reactions and complications from devices. Data gleaned from the location of mobile phones, purchases made using mobile devices, social media and other sources can help identify natural and humanitarian crises and provide clues for the best way to respond to a given situation.

In cities, sensors and data on traffic volumes and flows can be used to improve traffic management and the development of traffic plans. Smart water solutions can save utilities money and reduce water consumption. The adoption of smart-grid technologies is generating large volumes of data on energy and resource consumption patterns that can be exploited to improve energy and resource efficiency.

### Data-intensive economic and social activities rely greatly on an open and interconnected digital environment

Data-intensive economic and social activities rely greatly on an open and interconnected digital environment, on the ability to move data easily, flexibly and cheaply among a potentially unlimited number of partners across different organisations, and even across jurisdictions.

The overall interdependencies across the actors within this ecosystem can be very high as they share elements or sub-elements of a data life cycle, which includes all the processes involved in managing the flow of data, from data collection to its processing. While DDI is becoming the main driver for using ICTs to drive productivity, innovation and growth, its characteristics increase the complexity of digital security risk management and privacy protection. The rapid evolution of big data technologies and the ready acceptance of the concept by public and private sectors have left little time for the policy discourse to develop and mature.

The idea that, for security reasons, a system should be kept closed by default and open only by exception belongs to the past, when information technologies were not designed for interoperability and when their contribution to economic and social progress depended less on the free flow of data. It has in fact become complicated and expensive to "close" information systems, both in terms of the security measures needed to reduce interconnectedness and – most importantly – because limiting interconnectedness also reduces the potential for economic and social gains. Closing these systems is no longer possible without undermining the related economic and social activities and would therefore provide only an illusion of security.

**Data-driven innovation raises new privacy challenges**

In this data-rich environment, new privacy challenges are also emerging. The growing number of entities, such as online retailers, Internet service providers (ISPs), financial service providers (i.e. banks, credit card companies, etc.), and governments are increasingly collecting vast amounts of personal data[1]. In addition complementary information can be derived, by “mining” available data for patterns and correlations, many of which do not need to be personal data. Advances in data analytics now make it possible to infer sensitive information from data which may appear trivial at first, such as past individual purchase behaviour or electricity consumption. The misuse of these insights can implicate the core values and principles which privacy protection seeks to promote, such as individual autonomy, equality and free speech, and this may have a broader impact on society as a whole.

In some cases, personal data are provided or revealed by choice, for example, through social media and email; in other situations, through compulsory disclosure, for example, as a pre-condition to receiving services, or without awareness or consent, for example, by tracking an individual’s browsing. Other personal data are collected by sensors in smartphones, tablets, laptops, wearable technologies and even sensor-enabled clothing, cars, homes and offices. And increasingly, new data are derived or inferred based on correlations gleaned from existing data (Abrams, 2014).

By collecting and analysing large amounts of consumer data, firms are able to predict aggregate trends such as variations in consumer demand as well as individual preferences, thus minimising inventory risks and maximising returns on marketing investment. Furthermore, by observing individual behaviour, firms can learn how to improve their products and services, or re-design them in order to take advantage of the observed behaviour. These uses may also benefit the consumer: targeted advertising may give consumers useful information, since the ads are tailored to consumers’ interests (Acquisti, 2010). However, this ability to profile and send targeted messages and marketing offers to individuals may also have adverse consequences: some consumers may object to having their online activities observed; they may end up paying higher prices as a result of price discrimination; or they could be manipulated towards products or services they may not even need.

One of the most significant changes in the online and mobile environment over the last decade has been the emergence of social media and a dramatic increase in user-generated content. The widespread adoption of new ICTs, including mobile devices, together with the rise of social media that these technologies have enabled, has fundamentally changed the role of individuals.

Individuals create, post and share information about themselves and their friends, relatives, teachers, and even people they do not know using a variety of platforms, including social networks, photo-sharing sites, rating systems and other social media services. Individuals may inadvertently compromise their own privacy when they disseminate information about themselves since they have little control over what others may do with this content or how it will be interpreted by others. This raises challenging questions about how policymakers should respond to individuals' new role as creators and disseminators of content, including personal data. [2]

Governments are also using big data and sophisticated analytics for law enforcement and national security purposes. For example, financial transactions can be analysed to detect money laundering and terrorist financing. These types of uses have generated debate around privacy and civil liberties issues, sometimes resulting in policy or behavioural change. For example, the United States and the European Union have renegotiated the arrangement under which personal data are processed in the United States with the development of the EU-US Privacy Shield.[3] Some governments are proposing data "localisation" laws requiring data be stored and processed within their jurisdiction. An increasing number of companies are publishing "transparency reports" voluntarily providing information about data requests from governments.

There is evidence to suggest that individuals' trust is being threatened. A 2014 CIGI-Ipsos survey of Internet users in 24 countries on Internet security and trust suggests that 64% of respondents are more concerned about privacy than they were one year ago. According to a 2014 Pew Research Centre poll, 91% of Americans surveyed agree that consumers have lost control of their personal information and data. In a special 2014 Eurobarometer report on cybersecurity, EU Internet shoppers reported their top two concerns to be the misuse of personal data and the security of online payments. The level of concern in both areas is up from 2013, with fear of personal data misuse increasing from 37% to 43% and security concerns up from 35% to 42% (OECD, 2015a: 211).

***Digital security incidents continue to rise in frequency and scale***

In recent years large and small organisations appear to be subject to more frequent and severe digital security incidents. From an economic and social perspective, security incidents can affect organisations' reputation, finances, and even physical activities, damaging their competitiveness, undermining their efforts to innovate and their position in the marketplace. These incidents can disrupt the availability, integrity or confidentiality of information and information systems on which economic and social activities rely, and they can be intentional (i.e. malicious) or unintentional (e.g. resulting from a natural disaster, human error or malfunction).

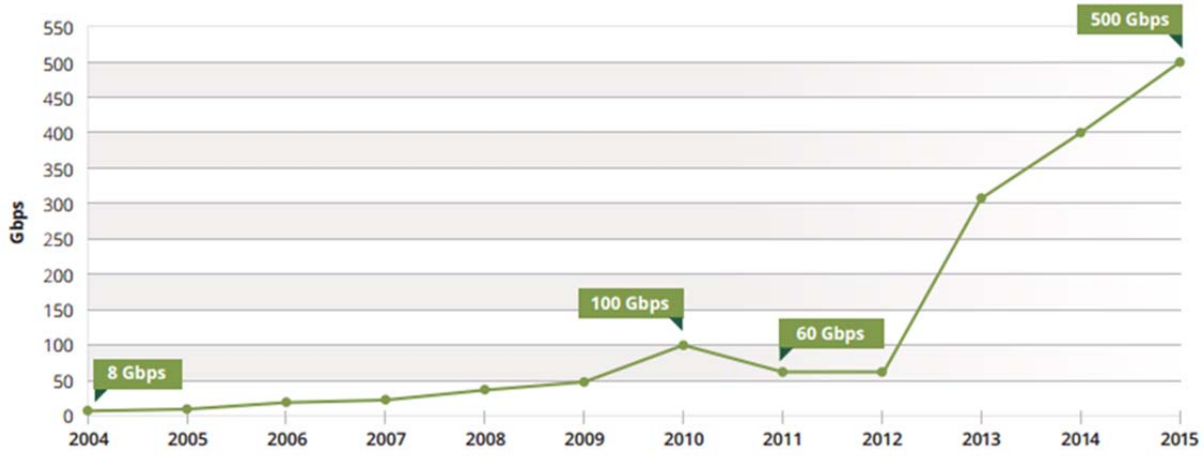
Digital security incidents have taken a variety of forms. Criminal organisations are increasingly active in the digital environment. Industrial digital espionage is on the rise. "Hacktivists" routinely attack selected targets to increase the visibility of their political cause. Some governments are also carrying out online intelligence and offensive operations. In some cases, the motive may be political or the attacks may be designed to damage an organisation or an economy. This was for example the case with the attack that targeted Sony Pictures Entertainment at the end of 2014, exposing unreleased movies, employee data, emails between employees and sensitive business information like sales and marketing plans (BBC, 2015).

An attacker can also target an organisation by flooding its online service or bandwidth with spam requests, knocking it offline for hours or days (Goodin, 2015). Although small businesses are often victims of these so-called denial-of-service attacks, large companies and core digital infrastructure components can also be targeted, as demonstrated by the 2013 massive attack carried out against anti-spam organisation Spamhaus. The strength of such attacks has increased over time, using an ever increasing amount of

bandwidth. In 2015, several attacks used over 300 Gigabits per second (Gbps) and one peaked at 500 Gbps, which represents a tenfold increase compared to 2009 (see Figure 1) (Arbor Networks, 2016).

Attackers may also undermine business continuity by penetrating a system and disrupting its operations, such as when French television channel TV5 Monde's global broadcasting was interrupted for several hours in April 2015. One of the most destructive acts of computer sabotage on a company to date affected the oil company Saudi Aramco after the introduction of a virus in its information system which erased data on three-quarters of corporate computers, i.e. 30 000 hard drives (Perlroth, 2012). It took over two weeks for the oil company to recover. During this time, oil production continued, but other operations had to revert to pre-computer age paper-based processes (Pagliery, 2015 and Rashid, 2015). In 2014, a malicious actor gained access to the corporate network of a steel mill in Germany, moved into the plant network, and disrupted critical components which resulted in massive physical damage (Conway et al, 2014).

**Figure 1. Evolution of bandwidth used for largest denial of service attack since 2004**




Note: This graph shows the evolution of strength of the largest denial of service attack reported each year measured in gigabits per second (Gbps).

*Source*: Arbor Networks, 2016: 24.

Attackers can also breach confidentiality by penetrating in an organisation's information system to export confidential data (business plans, cutting edge research, confidential employees information, etc.), whether to sell it to competitors, expose it publicly or, blackmail the victim. Examples include the attack against Sony Pictures Entertainment mentioned above, and the Canadian firm Nortel where intruders spied on the company for ten years until it sold its assets in the wake of a 2009 bankruptcy filing (CBC News, 2012).

### *Digital security incidents involving personal data ("data breaches")*

Digital security incidents affecting the confidentiality of personal data commonly referred to as "data breaches" [4], have similarly increased in terms of scale and profile. In 2005 ChoicePoint , a consumer data aggregation company, was the target of one of the first high profile data breaches involving over 150000 personal records.[5] The company ended up paying more than USD 26 million in fees and fines. In 2007, retail giant TJX announced that it was the victim of an unauthorised computer system intrusion that affected over 45.7 million customers and cost the company more than USD 250 million.

Since then, data breaches have become almost commonplace. According to a study commissioned by the UK government, 81% of large British organisations suffered a security breach in 2014 (UK Department for Business Innovation and Skills, 2014).[6] Data breaches are not limited to the private sector as evidenced by the theft in 2015 of over 21 million records stored by the US Office of Personnel Management including 5.6 million fingerprints, and by the Japanese Pension Service breach that affected 1.25 million people (The Japan Times, 2015). In Canada, the Office of the Privacy Commissioner reported that the number of data breaches more than doubled during the 2013/14 fiscal year. Accidental disclosure was indicated as the reason behind more than two-thirds of these breaches.

Many breaches in the private sector involve credit card account information and customer credentials theft, as highlighted in the Target and Home Depot cases - two major US retailers. The Target breach reportedly involved approximately 40 million customer records containing financial data such as information on credit cards, and other information including names and email addresses of 70 million customers[7]. The breach at Home Depot involved 56 million credit card accounts and 53 million customer email addresses. In 2014, another major breach involved three Korean credit card companies and affected 20 million individuals – 40% of the Korean population. In 2015, Anthem Inc., a large US-based health insurance company, announced that hackers broke into its servers and stole social security numbers, addresses, and employment data across its business lines, which would, by some estimates, affect 80 million individuals (OECD, 2015a: 211-212).

Although external attackers have been responsible for most of the high profile breaches, malicious insiders and careless employees are also significant sources of incidents.

***Cost of digital security incidents***

As noted above, digital security incidents can have various types of consequences for organisations: undermined reputation when the brand is exposed, loss of competitiveness when for example trade secrets are stolen, financial loss resulting from the attack itself (e.g. in sophisticated scam schemes[8]), from lost business, disruption of operations (e.g. sabotage), recovery costs or legal proceedings and fines. It is difficult to have a clear idea of the average cost of incidents: organisations are often reluctant to share potentially damaging information, intellectual assets are difficult to value and, in many instances, organisations do not even report some incidents, particularly when there is no legal obligation to do so, for example in cases of theft of trade secrets and sabotage. It is also difficult to assess the cost of digital security incidents outside the organisation, for example, to individuals and society.

As a result, there are no official statistics, data sources or widely recognised methodologies to measure the true cost of incidents. Thus, much of the evidence is anecdotal. Some studies provide interesting aggregated estimates, which should nevertheless be treated cautiously. Examples include the joint study by the US Center for Strategic and International Studies (CSIS, 2014) and Intel McAfee, which estimated that the likely annual cost to the global economy from cybercrime is between USD 375 and 575 billion. According to this source, the costs of cybercrime would range from 0.02% of GDP in Japan to 1.6% in Germany, 0.64% in the United States and 0.63% in China. Other examples include the Atlantic Council-Zurich Insurance “Risk Nexus” study (2015) and the Ponemon-HP study on the cost of cybercrime (2015).

Based on anecdotal evidence, it appears that litigation is increasingly common in the case of data breaches, with card issuers seeking to recover the costs of reissuing payment cards from the hacked companies and affected individuals launching class-action lawsuits. Breached organisations can end up paying fines, legal fees, and redress costs. As mentioned above, ChoicePoint paid more than USD 26 million in fees and fines including as a result of the action by the Federal Trade Commission (US FTC, 2006). In 2008, a data breach at one of the largest credit card processing companies in the United States, Heartland

Payment Systems, affected more than 600 financial institutions for a total cost of more than USD 12 million in fines and fees (McGlasson, 2009) . Target Stores corporate filings for 2013-14 recorded USD 252 million expenses related to the data breach, which after being offset by USD 90 million in insurance proceeds leaves charges of USD 162 million (Lunden, 2015). In 2015, AT&T agreed to pay USD 25 million to settle a US Federal Communications Commission (FCC) investigation relating to data breaches involving almost 280 000 US customers (US FCC, 2015).

Although some of the direct financial costs may be covered by insurance (as discussed in the last section) the damages to the firm's reputation, relationships in the industry, and the impact on individuals may be long-lived and are difficult to measure.

Another type of consequence is changes in organisations' top management after a significant digital security incident. For example, Target's CEO stepped down shortly after the incident was disclosed, as did Sony Pictures Entertainment's co-chair, and the Director of the US Office of Personnel Management, while some three dozen executives lost their jobs as a result of the attacks against Korean banks mentioned above.

It is important to emphasise that data breaches can have a significant impact on individuals' privacy. Individuals can experience tangible harms including financial loss, physical threat or injury, identity theft and other economic and social impacts. They can also experience intangible harms such as damage to reputation, excessive intrusion into private life or a loss of trust. More generally, security incidents can erode trust not just in the affected institutions but also can spill over to other sectors as customers lose confidence in the system.

***Measurement challenge***

While technical experts and policy makers generally agree that digital security risk and privacy concerns are changing in scale and require urgent action by all stakeholders, the evidence to support this conclusion remains often anecdotal and qualitative. Almost every week, if not daily, new reports are published with metrics covering a specific aspect of digital security and/or privacy risk. However, many of these reports do not provide sufficient details regarding their data sources or methodology, are limited in scope and in geographic diversity, and may be developed or funded by actors with vested interests. With some notable exceptions, these statistics are not regularly updated, come from different sources and provide a snapshot on trends from constantly different perspectives. While such statistics are useful, they are often not sufficiently robust to be used with a high degree of confidence for public policy making.

While this situation is typical of an area which, without being completely new, is still at an early stage of maturity, there are also some complex challenges related to measuring digital security and privacy risk. For example, organisations may be reluctant to disclose quantitative information about vulnerabilities, incidents and impact to avoid further exposing their reputation or attract malicious actors. Compared to other areas of digital economy policy, such as telecommunications policy, digital security and privacy statistics are still in their infancy. However, the need for better evidence has increased proportionally to the elevation of digital security and privacy risk to the top of governments' policy agendas. An OECD (2012) report on "Improving the Evidence Base for Information Security and Privacy Policies highlighted "the potential for the development of better indicators [for security and privacy]". It showed "in particular that there is an underexploited wealth of empirical data that, if mined and made comparable, will enrich the current evidence base for policy making". It further noted that "such indicators would help identify areas where policy interventions are most clearly warranted, and can provide guidance on designing policy interventions and determining their effectiveness". Following this report, the OECD initiated work in 2013 to provide public policy makers with a more robust evidence base (OECD, 2015c).

**Key findings**

- Data-driven innovation can foster new, or significantly improve products, processes, organisational methods and markets and help address social and global challenges.

- In this data-rich and hyperconnected environment, digital privacy and security challenges are also increasing and affecting trust and the potential of the digital economy to support economic and social prosperity.

- These data-intensive economic and social activities rely on an open and interconnected digital environment that increases the complexity of digital security and privacy risk management.

- Digital security and privacy incidents are difficult to measure quantitatively but evidence suggests that they are growing in both number and sophistication.

- Further work is needed to better understand the practical and public policy implications of the changing role of the individual and to consider possible options to help individuals manage digital privacy and security risk.

## THE EVOLVING UNDERSTANDING OF RISK AND RISK MANAGEMENT

Risk management has progressively emerged as a means to better address digital security and privacy challenges. This section provides a brief overview of risk and risk management and introduces the key elements of the 2015 Security Risk Recommendation. The following section will introduce the role of risk management to further implement the principles of the 2013 OECD Privacy Guidelines.

### Brief overview of risk and risk management

In common language, risk refers generally to the possibility that an event, usually undesirable, will occur. Everyday language uses the term risk in a loose way. For example, it can be used to mean threat, vulnerability, incident, likelihood, chance and danger. Risk management, however, requires a clear distinction between causes and their consequences and addresses the former (threats, vulnerabilities and incidents) in order to manage the latter (risk) (OECD, 2015d: 32).

#### *What is risk?*

While risk is a common and widely used term, it is a much more complex and nuanced concept than it appears at first glance. Risk theory has evolved over time, and continues to do so (Aven et al, 2011). Although there are many definitions of risk, ISO Standard 31000, *Risk Management: Principles and Guidelines* and ISO Guide 73 (2009a, 2009b) provide an internationally agreed understanding of this concept.

According to ISO, risk is "the effect of uncertainty on objectives". This definition contains three important elements: "objectives", "uncertainty", and "effect". Organisations and individuals engage in activities to achieve specific objectives or benefits. When engaging in these activities, they face a certain degree of uncertainty: some events or changes may happen that affect their chances of success in ways that cannot be entirely predicted and controlled. Risk is the possible adverse effect of such uncertainty on objectives. Uncertainty is a broad concept that covers the lack of certainty regarding potential events or situations that may or may not occur, whether they can be imagined, for example on the basis of previous experience, or are complete outliers, rare anomalies, or so-called "black swans". The effect of uncertainty can be negative – i.e. undermining the achievement of the objectives, or positive, – i.e. supporting the realisation of the objectives. However, as it is the case in this paper, the term risk is generally used to capture only the negative effect of uncertainty, and the positive effect is generally called an opportunity.

Risk is often measured in terms of likelihood of events and impact on objectives, reflecting the three aspects of the above definition. Risk should not be confused with its risk factors, i.e. the causes of risk. In some areas, such as digital security risk management, risk is often described as the effect of "threats" exploiting "vulnerabilities" to generate "incidents". Threats, which can be intentional or unintentional, are typically external factors that cannot be directly controlled by the organisation (e.g. weather conditions or the intentions of a criminal); vulnerabilities are typically internal (e.g. weaknesses in the organisation such as obsolete security practices, or lack of staff awareness about threats); and incidents resulting from their combination.

#### *What is risk management?*

Because uncertainty cannot be entirely eliminated, risk is common to all human enterprises and cannot be entirely avoided without also forgoing the benefits of the activity at stake. Some degree of risk

has to be accepted to harness the benefits of an activity. However, risk can usually be managed and reduced to an acceptable level in light of the objectives and benefits to be achieved.

Individuals manage risk all the time when they make decisions, whether it is something as simple as crossing the street, or as important as buying a house or changing jobs. From a business perspective, seizing opportunities is inherently related to risk taking, for example when investing in new products or services or expanding into new markets. In professional environments, including health, engineering, finance, industrial processes, etc., risk management has become a widely accepted practice. It improves decision-making by taking into account the effect of uncertainty on the organisation's objectives and, thereby, increases the likelihood of success.

Sophisticated tools, methodologies, standards and terminology have been developed to identify, measure and manage risk in various areas. According to the above mentioned ISO standard, a risk management framework is "a set of components that provide the foundations and organisational arrangement for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation." Box 1 describes the fundamental components of a risk management cycle.

**Box 1. Risk management cycle components**

**1. Establishing the objectives and the context.** One cannot determine the acceptable risk level in the abstract. It is always contextual. Therefore, the first step is to understand the mission of the organisation, its economic and social objectives, the benefits it is aiming to realise, and its values. It also requires examining the broader context including society's values, laws, regulations and culture, identifying stakeholders and their concerns and other internal and external factors that define what a successful achievement of the objectives means.

**2. Assessing the risk.** This analytical step consists of three distinct tasks:

a) Identifying risk factors: intentional and unintentional threats (such as a criminal attracted by a company's asset), vulnerabilities (weaknesses such as keys left under the doormat or lack of employee training) and possible events (e.g. incidents such as an intrusion by a thief).

b) Analysing the risk factors. This involves taking into account the likelihood or probability that an event will occur. It can be described qualitatively – e.g. low, medium or high – or using a numeric value.

c) Evaluating the risk (impact). This phase involves assessing the severity or magnitude of the estimated consequences of uncertainty on the organisation's objectives defined in stage 1. The impact can be tangible (e.g. money loss, physical harm) or intangible (e.g. reputation).

**3. Treating the risk.** This decision making step aims to determine the most appropriate way to address the risk in order to achieve the anticipated objectives and benefits. This involves one or more of the following:

a) Accepting the risk.

b) Reducing the risk to an acceptable level. Risk can be reduced through security measures generally involving people (e.g. training), processes (e.g. legal, organisational, etc.) and technologies (e.g. keys, locks, fences, etc.). Since risk cannot be completely eliminated, the persistence of some residual risk means that undesirable events can occur despite the presence of security measures. Therefore organisations also need to be ready to deal with undesirable events through measures that reduce the impact of incidents when they happen (preparedness measures) to ensure resilience and continuity. Finally, organisations can also use innovation to reduce risk, i.e. designing the activity differently, including its business model and organisational aspects, to reduce its risk exposure.

c) Sharing the risk or transferring it to another party (e.g. through insurance).

d) Avoiding the risk by not carrying out the activity and thus forgoing the potential benefits.

The choice of risk treatment depends on several factors including the organisation's tolerance of risk, also called "risk appetite".

**4.Ongoing monitoring and review cycle**. Since the environment is constantly changing, a cycle has to be created to ensure that the risk is continuously managed. This includes returning to step 1 and examining, for example, changes in the context (e.g. objectives, market, expected benefits) and the risk level (threats, vulnerabilities, likelihood, possible impact), effectiveness of the risk treatment measures, and accuracy of the risk assessment.

### OECD Recommendation on digital security risk management for economic and social prosperity

As pointed out in the previous section, organisations and individuals carrying out activities in the digital environment are constantly exposed to potential digital security incidents. How should they address this situation? A typical response is to consider the problem as solely technical and to ask digital security experts to solve it by creating a safe and secure digital environment.

In contrast, the OECD recognises that the digital environment, like any other environment, cannot be entirely secure. Using the digital environment to achieve economic and social objectives always requires accepting a certain level of digital security risk. While digital security measures should be implemented to reduce digital security risk, they can never eliminate it entirely. And since they have a cost, balanced decisions have to be made on which security measures to put in place in light of the risk, the economic and social objectives and the benefits at stake.

The digital security measures themselves can undermine the economic and social activities that they aim to protect, which rely on the openness and dynamic nature of the digital environment. Thus, the Security Risk Recommendation calls on leaders and decision makers to treat digital security as an economic and social risk rather than solely as a technical issue (OECD, 2015e). Digital security risk management is the application of the generally applicable risk management cycle described above to economic and social activities that use or rely on the digital environment. It addresses the type of uncertainty that can have a negative effect on economic and social activities by affecting the availability, integrity and confidentiality of the activities, or of the digital environment (OECD, 2015d: 29-31).

Digital security risk management is the process whereby decision makers can ensure that security measures are appropriate to and commensurate with the economic and social activities at stake, i.e. that they protect and support them without undermining them. In fact, digital security risk management should be viewed as a process that can both protect and create value.

Economic and social activities are exposed to numerous risks. Risk management is most effective when it is applied to risks and activities in a holistic manner. Its systematic, dynamic and cyclical nature makes organisations more agile, responsive and capable to handle change and take advantage from it. Thus the Recommendation also calls on leaders and decision makers to integrate digital security risk management into their organisation's overall risk management framework and economic and social decision-making processes, rather than address it in isolation. Such a holistic approach is particularly important given the generalised reliance on the digital environment both vertically, for each specific activity of an organisation, and horizontally along the value chain, since all activities share the digital infrastructure.

Risk management is not new to ICTs. As illustrated by the development of technical standards such as ISO/IEC 27000[9] in the 1990s, digital security experts have, for many years, been integrating risk management into the way they approach the security of information systems. The Security Risk Recommendation aims to bridge the gap between the leaders and decision makers responsible for achieving economic and social objectives and the technical experts in charge of developing and operating the digital environment on which these activities rely. In fact, co-operation between them is crucial to managing digital security risk for economic and social prosperity.

The Recommendation includes 8 principles to guide the development of digital security risk management frameworks, consistent with existing risk management standards and methodologies (Figure 2).

**Figure 2. Digital security risk management principles**


The risk management cycle introduced in Figure 2 is relatively universal. In crossing the street, for example, it has been shown that people assess risk in real-time, deploying the components of the cycle. In this example, however, risk management is so well integrated in every-day life that it is difficult for an individual to realise that he/she is actually going through each step. This is not yet the case for digital security risk. It has been recognised that individuals as well as SMEs often do not have the knowledge and resources to fully implement a risk management approach.

In addition, individuals and SMEs have little influence or control over the design of software or hardware available on the marketplace; and may not be able to judge if the lack of a particular digital security measure or option generates added risk. (OECD, 2015d: 38-40) Further work is therefore needed to better understand how to address the specific needs of individuals and SMEs. These issues are further addressed in later sections of this report.

**National strategies to foster digital security risk management**

Governments should play an important leadership role in encouraging the adoption of digital security risk management by developing national strategies in collaboration with other stakeholders as called for in the Security Risk Recommendation. The OECD recommends that these strategies are supported at the highest level of government to ensure that competing policy objectives are appropriately balanced. Strategies should "articulate a clear and whole-of-government approach that is flexible, technology-neutral and coherent with other strategies fostering economic and social prosperity" (OECD, 2015d: 11). National strategies are essential to better address at least four interrelated aspects of digital security challenges: economic and social prosperity, technology, law enforcement and national/international security (cf. Figure 3). Because they pursue different goals, policies addressing each facet do not necessarily involve the same players or require the same culture and mindset. A national strategy is a useful tool to clearly distinguish each facet and address it with the appropriate paradigm, while ensuring consistency and addressing intersections.

**Figure 3. Key facets of the digital security challenge**


Note: there may be other facets such as human rights, etc.

National strategies can help create the conditions to make it easier for all stakeholders to collaborate in the management of digital security risk, for example by sharing knowledge, skills and successful experience and practices in relation to digital security risk management at both policy and operational levels. They can strengthen international and regional co-operation and the ability of all stakeholders to respond to domestic and cross-border threats.

In addition to the core elements that the development of a national strategy should take into account, the Security Risk Recommendation includes guidance for governments in many public policy areas. For example, governments can lead by example by adopting comprehensive frameworks to manage digital security risk to their own activities; ensuring the establishment of one or more Computer Security Incident Response Teams (CSIRTs); and using their market position to foster digital security risk management across the economy and society, for example through public procurement policies and supporting the development of a workforce with appropriate risk management qualifications. Governments can strengthen international co-operation and mutual assistance, engage with other stakeholders and create the conditions for all stakeholders to collaborate in the management of digital security risk. Finally, national digital security strategies can also facilitate the development of more robust digital security risk indicators to better inform public policy makers, help assess the effectiveness of public policies and provide useful information to other stakeholders (e.g. private sector, academia, etc.) (OECD, 2015d: 12-15).

**Key findings**

- Governments and decision-makers in organisations should address digital security as an economic and social risk rather than treating it solely as a technical issue.
- Risk management aims to reduce the risk to a level that is acceptable in light of the potential economic and social benefits, taking context (i.e., values, mission, etc.) into account.
- Governments can play an important leadership role to foster digital security risk management by developing national digital security strategies in collaboration with other stakeholders.

## KEY CHALLENGES: APPLYING RISK MANAGEMENT TO PRIVACY PROTECTION

The challenges to privacy in today's hyper connected and data-intensive digital environment have prompted policy makers and other organisations to look for new ways to more effectively implement privacy protection principles. Several interrelated responses can be identified. First, improving transparency empowers individuals who can then better ascertain the uses of data and the basis on which decisions are taken. Promoting transparency and the right to access and correction have been part of the OECD Privacy Guidelines since their initial adoption in 1980 and are incorporated into national laws around the world. A second response is the use of technologies to protect privacy, which has been long identified and is an area of increasing interest to policy-makers (e.g. "privacy enhancing technologies" and "privacy by design"). The 2013 OECD Privacy Guidelines also introduce a focus on the promotion of responsible usage of personal data by organisations by emphasising governance and accountability (Part Three). An accountable organisation should have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a risk-based privacy management program (PMP). The 2013 OECD Privacy Guidelines highlight that the determination of appropriate safeguards should be based on a process of identifying, analysing and evaluating the risks to individuals' privacy.

Although the usefulness of a risk-based approach to privacy protection as called for in the 2013 OECD Privacy Guidelines is well recognised, how to implement it is a topic of debate. This section aims to contribute to this discussion.

### Thinking about privacy protection from a risk perspective is not new

The Security Safeguards Principle in the 2013 OECD Privacy Guidelines, dating from 1980, already refer to the need to protect personal data from the "risk" resulting from unauthorised access, destruction, use, modification or disclosure of data. The European Union's Data Protection Directive 95/46/EC contain numerous references to risk.

The concept of privacy risk and of privacy risk management is now receiving increased attention from regulators, academics and policy makers. Yet, despite growing appreciation of its importance and work carried out by various groups on this topic (OECD, forthcoming),[10] these concepts remain difficult to understand.

The Security Risk Recommendation provides a valuable starting point to explore whether and how some of the concepts and methodologies developed to manage digital security risk might be usefully applied to privacy. However, while the domain of privacy partially overlaps security as it includes protection of personal information, it is important in this discussion to consider the full spectrum of privacy issues, and distinguish privacy issues resulting from digital security incidents from other privacy concerns.

Privacy issues resulting from security incidents are covered by the OECD Privacy Guidelines Security Safeguards Principle. They encompass for example the "data breaches" mentioned in previous sections, i.e. incidents where the confidentiality and the integrity of personal data have been breached. According to the Security Risk Recommendation "digital security risk management provides a robust foundation to implement the "Security Safeguards Principle".

However, other situations can undermine privacy without involving digital security risk. For example, data collected automatically from smart meters by an energy company to optimise electricity production may reveal people's behaviour inside their homes. Whether there is a violation of privacy will depend on how personal information is collected, used, disclosed and accessed according to other Privacy Guidelines principles. This can be illustrated by questions such as: are the individuals informed about this data

collection? Do they have access to their personal data? Is the data used only for the purpose initially specified? Thus, while there is an overlap between privacy protection and digital security, current security risk models may not be appropriate for understanding the full spectrum of privacy risk (World Economic Forum, 2014).

To keep this section as clear as possible, "privacy risk" will refer to privacy issues *unrelated* to digital security incidents, which are covered in the previous section of this report.

**Introducing accountability: key challenges and opportunities**

The concept of accountability was first developed in the original OECD Privacy Guidelines issued in 1980 and it can be found in national laws such as Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA)[11] .

In the context of privacy protection, accountability has at least two key elements: *i)* putting into place mechanisms and procedures to give effect to the organisation's policies and obligations; and *ii)* accepting responsibility, i.e., being answerable to regulators and other stakeholders such as individuals for compliance.

As noted in the introduction to this section, the new Part Three of the 2013 OECD Privacy Guidelines ("Implementing Accountability") introduces the concept of a privacy management programme (PMP) as a way to address privacy risk by achieving these goals and articulates its essential elements.

**A privacy risk management approach can help organisations tailor policies and practices**

In moving from theory to practice, organisations have to tailor their PMPs to their specific circumstances including social and economic objectives. A "one-size-fits-all approach would only lead data controllers towards structures that are unfitting and ultimately fail" (Article 29 Data Protection Working Party, 2010). Organisations need to take into account factors such as the type of data, the size of the data processing operation, the intended purposes of the processing and uses of the data, the number of envisaged data transfers, as well as the privacy risks to individuals.

A privacy risk management approach can help organisations take account of the above factors and of the risks and opportunities to both the organisation and the individuals whose data is being processed.

**Addressing the misalignment of interests and objectives**

Like any form of risk management, privacy risk management should be based on good information and reflect stakeholders' concerns and interests; it should be scalable and take human and cultural factors into account and it should be responsive to change.

Privacy risk and digital security risk differ, however, in that, for privacy risk, the party carrying out the risk assessment and in a position to reduce the risk (the "data controller", or, to simplify, "the organisation") will not suffer the same consequences from a privacy breach as the "data subject", or "the individual". As interests are not well aligned, organisations may have an incentive to underestimate privacy risk or to provide incomplete information about it (OECD, 2015d: 38).

Effective privacy regulation, including enforcement, is one way to correct this misalignment. If they are significant and predictable, fines and other forms of sanctions (e.g. mandatory notifications) can create financial, legal and reputational risk for organisations processing personal data (i.e., a compliance risk), and help ensure that privacy risk is given the same weight and importance as other categories of risk. A balanced approach would include additional "soft law" mechanisms such as codes of conduct or self-

regulation, certification and Binding Corporate Rules (BCRs) which can also help realign the interests of the data controllers and the individuals.

Misalignment between the objectives and interests of organisations and those of the public is not unique to privacy protection. It can occur with other well-known categories of risk that organisations and business routinely manage, such as in health and safety, food hygiene and drinking water, where individuals can be adversely affected. As with privacy protection, legislation and other legal mechanisms to protect health and safety are often indispensable to realign the interests of the two parties. Regulation remains a key influence on business risk management practices although other considerations can play a significant role (Hutter and Jones, 2007). Consumers, for example, can exercise a direct and important influence.

**Risk assessment can help organisations comply more effectively**

Regular risk assessment can help organisations adjust their PMPs to reflect evolving risk and other changes in context and help ensure compliance with the obligations set out in basic principles such as collection limitation, and data quality. Risk assessment features prominently, for example, in the accountability guidance developed by Canadian Privacy Commissioners which considers it as part of a risk management process that feeds an organisation's decision-making: "*Organisations should develop a process for identifying and mitigating privacy and security risks, including the use of privacy impact assessments and security threat risk assessments*" (Office of the Privacy Commissioner of Canada, 2012).

Assessing risk is an essential component of Privacy Impact Assessment (PIAs)[12] and Privacy by Design, both of which are important accountability and compliance mechanisms. Assessing and treating risk can also help organisations move beyond mere compliance with legal requirements and assist in integrating the protection of personal data into their enterprise-wide risk management.

**The distinctive nature of privacy risk makes benefits/risk assessment challenging**

The distinctive nature of privacy risk makes benefits/risk assessment challenging for a range of reasons. To be effective, the scope of any privacy risk assessment must be sufficiently broad to take into account the wide range of harms and benefits, yet sufficiently simple to be applied routinely and consistently. It is a challenging task, involving identification of relevant risk, which may be subjective, and then determining its possible severity and likelihood. Risk assessment can sometimes lead to a simplification of problems, often through quantification, which typically disguises the full complexity of risks (Cohen, 1996). Bias in quantification and in the use of information may be concealed by an appearance of objectivity. Determining "acceptable" costs or levels of risk has long been a subject of contention: indirect costs and benefits are rarely considered and the figures often look different from different perspectives (Ackerman and Heinzerling, 2004). Even if the causes and costs of risk are clear, *acceptable* risk must still be defined, and that is often a political decision.

This complexity has not prevented organisations like the French Commission Nationale de l'Informatique et des Libertés (CNIL) or the Centre for Information Policy Leadership (CIPL) from establishing broad categories of risk as part of their risk management guidance. In fact, many other areas of risk management do not rely on precise definitions and narrow categorisations of the effect of uncertainty. For example, a key risk that organisations manage relates to reputation, which is also an intangible asset.

These issues require further work. Efforts regarding risk assessments could benefit from existing risk assessment methodologies and standards in other areas, and from the expertise of risk management professionals. Privacy Impact Assessments for example, tend to focus solely on privacy and security risk without taking the potential benefits of the activity or project into account. More work is needed to explore

how data “benefit analysis” can be used in conjunction with more traditional PIAs “to form a balanced, comprehensive view of big data risks and rewards.” (Polonetsky et al, 2014).

**From compliance to competitive advantage**

As noted above, many organisations will tend to address privacy protection as a "compliance risk" rather than a competitive advantage or product benefit. Organisations may only[13] focus on complying with the law without considering changing the business model, the way technologies are used or using privacy as a competitive advantage on the marketplace. In other words, privacy compliance may be viewed solely as a legal challenge, exactly like digital security risk may be considered solely as a technical security challenge. The OECD has addressed this narrow view in digital security by calling on leaders and decision makers to handle digital security challenges as an economic and social risk and to integrate digital security risk management as part of the decision-making process of their organisation. A similar perspective could be considered for privacy risk management.

Another possible consequence might be that organisations only protect themselves against the compliance risk by formally respecting the law while not implementing effective privacy protection measures in their products and services. For example, a company may use a very long and complex privacy policy notice to comply with the law and offer individuals a "take-it or leave-it" binary choice to access their services. Where individuals can choose another provider on the marketplace with greater assurance regarding privacy protection, this would not necessarily be a problem. But this is often not the case since many companies often adopt similar binary choice practices and have limited incentives to compete on the basis of privacy protection. Moreover individuals may not have market power to demand better protection.

This should not be interpreted as a call to diminish or eliminate compliance obligations. As explained above, there may be a fundamental misalignment of interests and objectives which requires regulatory compliance to incentivise organisations to protect privacy. However, these obligations could be complemented by other measures to increase individuals’ choice or incentivise organisations to more broadly incorporate protection of privacy, turning privacy protection into a market differentiator, i.e., a factor on which business competes, thereby improving overall privacy.[14]

As an example, Apple, now the world’s most valuable publicly traded company, has begun to explicitly market its privacy practices, emphasising security and privacy as fundamental design elements in Apple products and services.

Further work would be needed, however, to progress in this direction. Presently there are no easy ways to value intangible privacy protection in a manner that all actors can understand, nor is there an objective and agreed scale or indicator of privacy protection on the basis of which stakeholders could make rational decisions.

**Contributing to global interoperability**

Paragraph 21 of the 2013 OECD Privacy Guidelines urges member countries to “encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines.” The Supplementary Explanatory Memorandum goes on to note that: “Improving the global interoperability of privacy frameworks raises challenges but has benefits beyond facilitating transborder data flows. Global interoperability can help simplify compliance by organisations and ensure that privacy requirements are maintained.”

There are significant differences among national privacy and data protection laws. Some laws are based on the premise that privacy is a fundamental human right; other laws are more consumer-protection

oriented; some jurisdictions have broad comprehensive laws while others rely on sector specific laws. There are even fundamental differences around basic concepts such as what constitutes personal data.

As noted in the 2013 OECD Privacy Guidelines, the accountability principle recognises these differences in privacy law and regulation, but neither requires one country or region to necessarily adopt or adapt to the system of another, nor forces all systems to bend to a common regime. Rather, it takes the view that obligations - in law, regulation, best practices - must be met wherever or by whomever the data is processed. Accountability vests the user of data with responsibility for ensuring that the obligations are honoured by implementing a risk management process to assess, manage and mitigate the privacy risks created by data use, employee training, and the means to manage data events such as breach, inappropriate access, or failure to meet the obligations of the privacy policy.

Privacy risk management has, thus, the potential to facilitate interoperability. While the context – the laws, the regulations, the cultural values, etc. – in which organisations operate may vary across the globe, many of the uncertainties and organisational objectives are the same. Global organisations are able to use risk management processes and methodologies to comply with diverse regulatory requirements and different social and cultural values. A common understanding and application of risk management principles has, for example, facilitated mutual confidence and promoted more consistent decisions among regulators in other areas such as food production, medical devices and pharmaceuticals.

To be successful, stakeholders will need to approach privacy risk management from the economic and social perspective, by integrating privacy risk management into their organisation-wide risk management methodologies and business decision making. Realising this potential will require developing and using a common vocabulary, for example consensus around fundamental concepts such as privacy risk, and on metrics to assess privacy risk and evaluate the outcomes of a risk management approach.

While the need for interoperability is clear, considerable work remains if it is to work in practice. A first step could be to start bridging the gaps between communities. The OECD has invested significant effort in recent times to develop a framework for cooperation among privacy enforcement authorities. There is also a global community of risk management and privacy professionals that could be leveraged to promote good risk management practice.[15]

**National privacy strategies**

The 2013 OECD Privacy Guidelines recommend that governments “develop national privacy strategies that reflect a co-ordinated approach across governmental bodies”. While many countries have adopted national digital security strategies, very few countries have adopted equivalent privacy policy strategies.

Legislation continues to be the primary response to addressing personal data protection. Rather than being directed at all stakeholders, these laws typically impose obligations on organisations subject to the law and require them to grant individuals specific rights. Complementary measures such as education and awareness-raising are often left to privacy enforcement authorities or civil society bodies.

While protection by the law is essential, privacy in an increasingly data-driven economy would benefit from a multifaceted strategy, reflecting a whole-of-society vision, and supported at the highest levels of government, as called for in the Privacy Guidelines (Part Five). Along the model of “digital security strategies”, such multifaceted privacy strategies would help create the conditions for privacy protection to become a differentiator in the marketplace while providing the flexibility needed to capitalise on emerging technologies. They could also encourage research and innovation with respect to "privacy by design" approaches and help focus efforts by privacy enforcement authorities and other actors. Coordinated

privacy strategies at the national level would help foster cooperation among all stakeholders and lessen uncertainty in data flows.

Finally, the inter-relation between digital security and privacy risk has long been recognised as illustrated in the areas of digital identity management and cryptography policy. Whole-of-government solutions require an understanding of complementarities and tensions. Synergies between digital security and privacy policy approaches, as well as co-operation among the different stakeholders could be strengthened and better leveraged if coordinated at the national level.

**Key findings**

- Although digital security and privacy risk are inter-related, they are typically addressed in silos and at different policy levels; privacy risk is generally not addressed based on the management of uncertainty, but rather on avoiding harm to the individual.

- In deciding how to treat privacy risk, organisations need to take into account the social and economic objectives they are pursuing. Like all forms of risk, privacy risk should not be assessed in isolation; it should be assessed in relation to the potential benefits.

- A number of potential benefits could be realised if privacy risk was addressed as part of the broader economic risk management framework of organisations and integrated in economic and social decision-making.

- More work is needed to determine how risk management principles can be implemented with respect to privacy protection and several complex questions remain to be explored such as how to allocate responsibility, how to define the acceptable level of risk and who should make this determination.

- Multifaceted national privacy strategies, reflecting a whole-of-society vision, and supported at the highest levels of government would enhance privacy protection in an increasingly data-driven environment.

## KEY CHALLENGES: ADDRESSING THE VULNERABILITY OF SMALL AND MEDIUM ENTERPRISES

SMEs, in particular early-stage start-ups, spur economic growth, drive competition and innovation, and contribute to job creation. The digital economy provides opportunities for SMEs to improve productivity and transform their business models. At the same time it raises special challenges as there is evidence that a large number of SMEs do not have the capacity or do not seem aware of how digital risk can impact their business.

SMEs often operate under the assumption that they are too small to become the target of a digital security attack- failing to appreciate evidence suggesting that malicious actors may target their business because of their links with larger companies or organisations. In addition, many SMEs are focused on their core activities, and still largely perceive digital security and privacy risk as solely a technical and legal issue and appear to underestimate the need to protect personal data and manage digital security risk as part of their overall risk management and decision making process.

A key issue for policy makers is thus how to best encourage SMEs to leverage the opportunities of the digital environment for their business and at the same time promote good practice in risk management to minimise potential adverse effects. This section examines some of the challenges that small businesses face in integrating digital security and privacy risk in their decision-making and provides information about the opportunities in adopting risk management practices.

### Advancing SME's digital agenda depends on trust

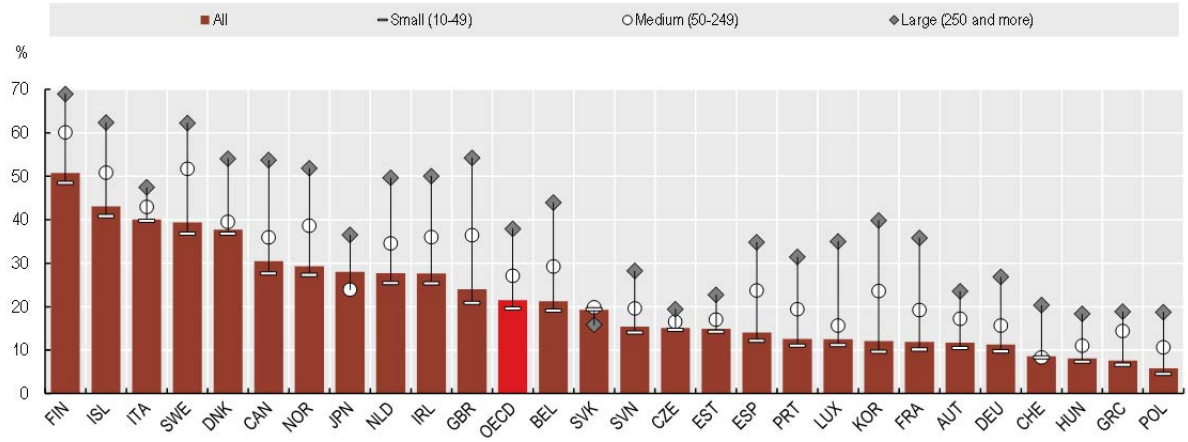
While large firms are often at the forefront in recognising and investing in IT advancements, SMEs can be slower to catch up and appreciate the business benefits that the digital environment can deliver. The internet and ICTs are likely to contribute to the growth and profitability of SMEs, but the extent of that contribution depends on the way in which small businesses and their employees adapt their organisational behaviour and make good use of the digital environment.

Current surveys on the diffusion of ICT tools and activities in enterprises indicate that many SMEs are not making the most of the business opportunities of the online environment. While almost 95% of SMEs in the OECD had a broadband connection in 2014, only 20% used it to conduct e-sales.

In Europe, a mere 14% of SMEs use the Internet as a sales channel. The reasons cited by SMEs for not trading online include technical issues, such as reorganising business processes and systems, skills issues, including a lack of specialist knowledge or capability, and trust issues. Recent surveys confirm that SMEs do not yet have full confidence in the digital solutions available and, in some cases, this is more likely to be reported as a key obstacle among those members whose knowledge of and involvement with the digital sector are high.

In a survey of European SME perspectives on cloud computing, the security of corporate data and potential loss of control featured highly among the concerns for SME owners (ENISA, 2009). In the United Kingdom, 21% of all smaller enterprises (10 to 49 employees) are using cloud computing services, compared to 54% of all larger enterprises. A similar adoption gap can be observed in other countries (Figure 4).

**Figure 4. The diffusion of cloud computing in enterprises, by country and size, 2014**




Source: OECD, 2015a. Based on OECD, ICT Database; Eurostat, Information Society Statistics and national sources, July 2014.

## Why SMEs are important

For an SME, losses due to security incidents might result in an unexpected drop in revenue that closes their business. The consequences of a security incident, such as loss of consumer trust, damage to reputation, negative impacts on revenue, etc., may be harder to weather for SMEs than for large organisations. According to a 2011 study cited by the US House Small Business Subcommittee on Health and Technology, roughly 60% of small businesses close within six months of a digital security attack (Kaiser, 2011).

The implications for national economies are significant as SMEs make a vital contribution to the economies of many OECD member countries and other developed economies. Studies suggest that more than 95% of enterprises globally are SMEs, accounting for approximately 60% of private sector employment (Edinburgh Group, n.d.: 7-8).

In the United States and Canada, SMEs account for the majority of GDP in most industries. Similarly, in Europe, SMEs represent 99% of businesses in the EU and are a key driver of economic growth, innovation and employment.

SMEs experiencing a digital security or privacy incident either accidentally or through commercial espionage may be more affected than a larger company that is in a better position to pursue a legal recourse to protect their investment. Some SMEs rely heavily on the strength and scope of their intellectual property (IP) to generate investment to take their technologies to commercialisation. IP is critically important to many small, innovative, and R&D-intensive businesses and the theft or exposure of IP can significantly damage their competitive edge and economic base. Early stage start-ups, such as those in the biotechnology or nanotechnology field, may be especially vulnerable to IP theft.

SMEs are often part of a larger value chain, partnered with large and small organisations. As a result, the digital security risk they face and their potential failure to manage it also represent a risk to the larger circle of organisations and firms with which they are partnered within their business ecosystems and their vulnerabilities may negatively impact other actors within the larger ecosystem. For example, the credentials of a small heating and air conditioning subcontractor working for Target Stores were used to successfully attack the large retail chain in 2013 (Krebs, 2014).

**Many SMEs are not aware of the digital security and privacy risks they face**

In 2015, 90% of large business and 74% of small businesses in the UK reported that they had suffered a security incident (UK HM Government, 2015). Digital security is increasingly expensive for SMEs: the average financial cost of a digital security incident for an SME in the UK is between USD 78 000 and 115 000. In addition, a greater proportion of SMEs spend more than 25% of their overall budget on digital security, a greater proportion than large business (15% vs. 10%) (UK Department for Business, Innovation and Skills, 2014) This suggests that both the cost of managing digital security risk and the risk itself are relatively a greater burden for SMEs than for larger companies.

Table 1 highlights the most common security incidents confronting SMEs in the UK. The percentages in the table refer to SME organisations surveyed in 2015.

The second and third most common attacks listed in the figure below exploit human vulnerabilities rather than technological ones which are easier to remediate.

**Figure 5. Most common security incidents faced by SMEs (% of total number of UK SMEs surveyed- N=355)**

| Incident | SME rate |
|---|---|
| **Infection from viruses or malware** | 63% |
| **Attack by an unauthorised outsider** | 35% |
| **Staff-related breach** | 27% |
| **Denial of service attack** | 16% |
| **Network penetrated by external source** | 14% |
| **Theft of intellectual property or confidential information** | 6% |

Source: Adapted from UK HM Government, 2015.

These results lend support to the notion that many SMEs may not be aware of and/or have limited or no knowledge about the types of digital security risks they face, their potential economic consequences and the specific approaches to mitigate them. Yet, any SME that accepts credit or debit cards or is involved in processing payment card data whether directly or through third-party vendors or contractors can face a digital security breach exposing private payment card information. Professional health service firms are also likely to have potential data breach concerns. Attorneys and law firms hold information that may be valuable to criminals who are intent on gaining access to private and company information. Insurance brokers, accountants, and payroll providers must often share personal financial data that could be devastating to consumers if exposed. All innovative start-ups are at risk of theft of their innovation through intrusions in their information systems.

In short, any small company that relies on sensitive information and continuous operation of its digital activities must understand the economic and social consequences of digital security incidents and give close consideration to how it protects its activities, information and information system.

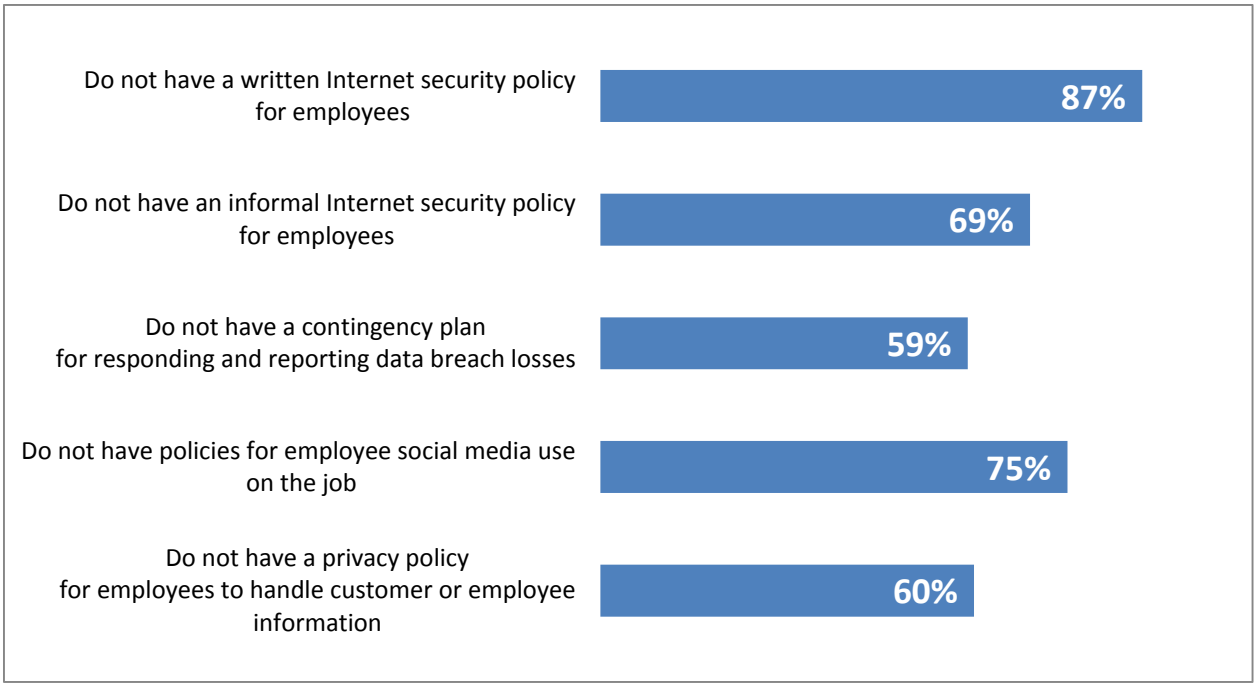
However, many SMEs and start-ups have limited staff and resource constraints, and will tend to focus on their core business and financial sustainability rather than digital security risk management. SMEs struggle with issues such as a lack of agility, budget and digital security skills (Ernst & Young, 2014).

Also, they often do not consider digital security issues during the initial stages of setting up the business (ENISA, 2009). Hence, they may not have dedicated systems administrators or the specialised expertise needed to identify vulnerabilities and respond to digital security threats.

A 2013 survey of business leaders by the Economist Intelligence Unit (2013) suggests that most companies and particularly SMEs are failing to create a culture of risk awareness. Only one in four SMEs (27%) reports an extensive awareness of digital security risk across the organisation.

Data from a 2012 study, co-sponsored by the US National Cyber Security Alliance (NCSA) and Symantec confirm these findings. The study reports that only 13% of US small businesses have a formal written Internet security policy, 59% do not have contingency plans, and just 35% provide any training to employees about Internet safety and security (Figure 6). Similarly, a 2013 Study of the Impact of Cyber Crime on Businesses in Canada suggests that only 22% Canadian businesses employ a risk assessment process to identify where their business is most vulnerable (International Cyber Security Protection Alliance, 2013). Recent UK data points to similar concerns.

**Figure 6. What small businesses can do better to protect themselves**




Source: Adapted from National Cyber Security Alliance and Symantec, 2012.

### Privacy risk management is much discussed but poorly developed in practice

A study of business practice in Canada notes that privacy risk management is much talked about but poorly developed in practice (Greenaway et al., 2012). While the study's results are to be interpreted with caution, this may indicate a lack of understanding of how to implement privacy regulatory requirements, it may also reflect a lack of organisational strategies on how to deal with privacy risk and a gap in the assignment of responsibilities. The authors conclude that "integrating privacy risk into an organisation's risk management strategy requires an understanding of the type or categorisation of risk and where it should reside within the risk management structure". This is not straightforward as risk managers often do not view privacy as within their remit and IT managers see risk management in the context of technical digital

security (Greenaway et al., 2012). Those responsible for privacy see the management of risk as captured by activities such as PIA, or not as their responsibility. Privacy is seen either as a digital security issue, or as a compliance issue. Privacy risk management is therefore often viewed as "someone else's responsibility".

In the absence of robust metrics on personal data processing by businesses, it is difficult to compare the potential exposure of SMEs to privacy-related risk with that of larger firms. Nevertheless, in some sectors such as health, law or finance, SMEs will tend to process significant volumes of personal data. Therefore, for many small enterprises, the consequences of failing to prevent and mitigate privacy risk can be very significant.

As noted elsewhere in this paper, privacy risk can directly affect business reputation, revenues, and trust in the marketplace, with respect to customers, shareholders, employees, and other stakeholders. Customers are often hesitant to do business with an organisation that does not adequately protect its data, and the damage to a firm's reputation could dissuade enough customers to the point that the company is no longer viable. The financial impacts of a privacy breach involving personal data can also be significant. A small business without the resources to pay for legal assistance, forensic investigations, the required notifications, remediation measures, and the fines, penalties, or judgments that could arise in the event of a privacy breach, might find itself out of business. SMEs everywhere recognise that privacy protection is good for business but often lack the resources and expertise needed to effectively manage privacy-related risks.

Unintentional employee misuses of personal data are estimated to account for 85% of privacy breaches (Greenaway et al., 2012). These most commonly include uses of data that are inconsistent with the original purpose of the data collection or unauthorised inspection of personal data. This indicates that employee actions may represent privacy vulnerabilities through a lack of awareness of privacy issues (discussed in previous sections) including potentially unintentional, but problematic, uses of data.

The responsibility of managing personal data throughout a firm requires an organised, well-thought-out approach to privacy risk management. Yet, a recent OECD study suggests SMEs often do not recognise the distinction between privacy and security risk. Privacy risk may be unrelated to security, for example when personal data is processed by the organisation in a manner that infringes on individuals' rights.

Firms can create privacy risk for individuals by failing to adequately understand how they use and protect personal data. Because of resource constraints, lack of expertise or because they may be too preoccupied building and running their business, SMEs may find it challenging to develop clear policies explaining how they use personal data. Or they may simply resort to cutting and pasting a privacy policy from another firm.

**Opportunities and challenges of mandatory data breach notification requirements**

A greater focus on good risk management and privacy protection practice is to be expected as measures passed by OECD governments to increase transparency and requirements for data breach notification requirements extend to SMEs.

The simple fact of having to publicly notify consumers about data breaches can bring small firms to implement stronger privacy and security standards that protect personal information. A data breach can have a huge impact on consumers' perception. How the violation occurs, how the company handles the announcement and how it makes amends may be critical factors in consumers' decisions to do business with that company in the future. Notifications of digital incidents also lead to greater awareness and attention across different levels of management.

Notification requirements for digital 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. Breach notification laws typically have provisions regarding what constitutes a breach (e.g., unauthorised acquisition of data); who must comply with the law (e.g., businesses, data/ information

brokers, government entities, etc.); definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information or when the breach is unlikely to cause harm to the individual concerned ).

Countries outside the United States have also begun to include data breach notification in their laws and policies. Recent reforms such as in Australia, Canada, European Union and Korea make breach notification mandatory in the event of a data breach that could give rise to a *"real risk of serious harm"* to the affected individuals. The extension of breach notification requirements to SMEs is expected to dramatically increase the number of notices. Educating and making small businesses aware will require significant efforts and resources.

This has given rise to a growing number of non-binding guidelines or codes of practice outlining circumstances where notification is required, establishing thresholds and processes. In some cases, these have general application (Australia,[16] 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[17] addressing issues such as coverage of specific entities.

A number of national privacy enforcement authorities have also begun to publish information on the volume of data breach notices they receive, often in annual reports (e.g. Ireland, New Zealand, and the United Kingdom). Anecdotal evidence suggests that enforcement activity in both small and large business as a result of security breaches is on the rise.

**Digital risk insurance**

Mandatory data breach notification regulations may play an important role in the growth of a digital risk insurance market. As the financial outlay of dealing with a breach gets more expensive, with the added efforts of dealing with mandatory notification, the option of using digital risk insurance will become more attractive for many small and large businesses.

Public policy can leverage insurance in raising awareness and incentivising adoption of good digital risk management practice. While it is the case that from a business perspective, digital risk insurance is viewed principally as one means to transfer risk outside the firm, its greatest potential is in helping firms, organisations and individuals better understand and evaluate digital risk and harness the opportunities from better risk management practices. The UK government, for example, has started to work with the insurance industry to develop a comprehensive digital security insurance model as the next step to encouraging small firms to adopt the Cyber Essentials Scheme[18] - a set of good practice measures in digital risk management. As is the case for notification requirements, digital risk insurance could generate valuable empirical data that would provide an important evidence base to support digital risk management policy.

However, in practice, insurance companies have been somewhat cautious with respect to covering the risk associated with widespread business use of ICTs or the risk associated with non-tangible assets such as personal data. Today, standard insurance policies are not designed to cover digital security and privacy risks. This can be attributed to the uncertainties around definitions of digital risk based on different causes and consequences, the absence of relevant data on past incidents and losses, the limited actuarial information available on the frequency and magnitude of actual and potential digital security and privacy incidents, and the ever-evolving nature of digital risks that are major challenges for the insurance sector. As a result digital risk insurance is still an emerging market.

Providers of this type of insurance today are located mainly in United States, and the United Kingdom. The market for digital risk insurance in the United States was about USD 2 billion in 2014.

Recent reports indicate that the market continues to broaden, especially in health care and the SME insureds segments (Betterley, 2015). The European market remains far smaller, at only around USD 150 million in gross written premiums, although with annual growth of 50-100%.

Although governments are beginning to explore the opportunities of digital risk insurance, more work is needed to identify the factors that have prevented the industry from developing more quickly (OECD, 2015a: 228-229).

**Good practice in risk management is good for business**

Good practice in digital security risk management and privacy protection can enhance the agility and resilience of SMEs, increase their competitiveness and provide better opportunities for partnership with other organisations.

SMEs that have stronger practices are in a better position to meet customers' privacy and digital security expectations. Moreover, SMEs that can demonstrate robust digital security and privacy risk management practices may have a competitive advantage when seeking partnership opportunities with large organisations and be in a better position to attract larger clients, who are more likely to generate higher revenues.

Increasing SMEs awareness of digital risk and elevating their capacity to manage it is critical. Given that SMEs may lack expertise and face resource constraints, larger organisations, industry associations, the technical community and governments can play an important role in this area and share their knowledge, skills and expertise about best practices in managing digital risk.

Given the interconnectedness of the digital environment this type of assistance has the potential to reduce overall risk in the value chain. Initiatives such as the development of "cyber-hygiene" tools developed by the British and French governments[19], as well as practical privacy assessment and compliance guides developed by data protection authorities in these two countries (UK ICO, 2016 and CNIL, 2010) are going in the right direction. Examples of other such governmental initiatives include a study by the Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, 2011) on IT-security in SMEs. Non-for profit organisations are also active in this space as illustrated by the "Information Security Framework"[20] developed by the International Association of Accountants Innovation & Technology Consultants for its members, the majority of which are SMEs. Further work could be carried out to adapt digital security and privacy risk management standards for SMEs and tools to facilitate their implementation by small entities lacking technical knowledge and resources.

**Key findings**

- Assisting SMEs in the use of the digital environment for their business is particularly critical as SMEs are vital to the economic functioning and the growth of many countries.

- SMEs face distinct challenges, including a lack of awareness and of ability in managing digital security and privacy risk that warrant particular attention.

- SMEs generally have resource constraints that limit their ability to implement comprehensive risk management practices to respond and manage digital security and privacy risk.

- Although governments are beginning to explore how to promote the growth of digital risk insurance markets, more work is needed to identify the factors that have prevented the industry from developing more quickly.

## NOTES

1 "Personal data means any information relating to an identified or identifiable individual (data subject)" (OECD, 1980).

2 Paragraph 19(h) of the 2013 Privacy Guidelines invites Member countries to consider the role of actors other than data controllers, "in a manner appropriate to their individual role". This provision, which is included under "National Implementation", was intended to make policymakers aware that there are other actors who, while not covered by the concept of data controller, nevertheless influence the level of protection of personal data and can create privacy risk for themselves and others. The Privacy Guidelines go on to suggest that non-legislative measures, including education and awareness raising, are two ways to address the privacy risk associated with the activities of individuals and that when an individual does cause damage to the privacy interests of others, tort or civil law may offer a possible remedy.

3 On 29 February 2016, the European Commission published a draft adequacy decision on the Privacy Shield that shall replace the Safe Harbour scheme invalidated following a decision by the Court of Justice of the European Union. At time of writing, consultation on the draft adequacy decision and regulatory review of the Privacy Shield was underway.

4 This paper uses the terms "data breach" to refer to an incident involving "a loss, unauthorised access to or disclosure of personal data as a result of a failure of the organisation to effectively safeguard the data" (OECD, 2011). It uses the term "digital security incident" to refer to incidents that may or may not involve personal data.

5 The Choicepoint breach became public because of a 2003 California law requiring notification to individual when their personal information was wrongfully disclosed. This contributed to the adoption of similar laws in many other jurisdictions. The 2013 OECD Privacy Guidelines call for controllers to provide notifications in cases where there has been a significant security breach affecting personal data (OECD, 2013, paragraph 15(c)).

6 The severity and impact of data breaches have also increased. According to a study released in 2015 by data security research organisation the Ponemon Institute, the total average cost of a data breach is now USD 3.8 million, up from USD 3.5 million a year earlier. The study also reported that the cost of a data breach is now USD 154 per record lost or stolen, up from USD 145 the previous year and the cost resulting from lost business because of decline in customers' trust after a breach can be even greater. The UK study referred to above estimated that big breaches cost large organisations between GBP 600 000 and 1.15 million.

7 See Target's Data breach FAQ at https://corporate.target.com/about/shopping-experience/payment-card-issue-faq (accessed 28 April 2016).

8 Such as USD 45 million loss by a bank in a global cybercrime scheme. For an example see: www.reuters.com/article/us-usa-crime-cybercrime-idUSBRE9AH0YZ20131118.

9 See www.27000.org for more information.

10 An increasing number of regulators, standards bodies and other organisations are now looking at ways to apply a more systematic risk management approach to data protection. For a brief overview of the initiatives see OECD, 2016 p. 10. See also Centre for Information Policy Leadership, 2014.

[11] For further information on the *Personal Information Protection and Electronic Documents Act* (PIPEDA) see www.priv.gc.ca/leg_c/leg_c_p_e.asp; on accountability and privacy management programmes see the guidance published by the Office of the Privacy Commissioner of Canada et al., 2012.

[12] PIA is a methodology to identify, assess, mitigate or avoid privacy risks. It describes the functions of the organisation to enable individuals to assess for themselves what may be considered a potential impact on their privacy, but it also goes on to explain what the organisation will do to protect individuals' privacy, and to identify solutions.

[13] This is not always the case for all organisations in all markets as some markets generate incentives for organisations to integrate privacy protection in their economic and social decision making processes, beyond pure compliance.

[14] Some regulators have started to think about privacy seals and certification as a way to enable consumers to differentiate on the basis of privacy standards. And the General Data Protection Regulation encourages seals and certification as a way for organisations to demonstrate privacy compliance.

[15] See for example the survey by the Federation of European Risk Management Association (FERMA, 2015) according to which 85% of risk management functions report to top management level.

[16] Office of the Australian Information Commissioner, 2015.

[17] See www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3134436.

[18] See www.cyberstreetwise.com/cyberessentials/ for more information.

[19] See UK Department of Innovation and Skills, 2015 and ANSSI and CGPME 2015.

[20] See www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/Other-sources-of-cyber-security-advice-for-your-business/ for more information.

## REFERENCES


Abrams, M. (2014), "The Origins of Personal Data and its Implications for Governance", http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf.

Ackerman, F. and Heinzerling, L. (2004), *Priceless: On Knowing the Price of Everything and the Value of Nothing*, The New Press, New York.

Acquisti, A. (2010), *The Economics of Personal Data and the Economics of Privacy*, www.oecd.org/sti/ieconomy/46968784.pdf.

ANSSI and CGPME (2015), *Guide des bonnes pratiques de l'informatique*, www.ssi.gouv.fr/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf.

Arbor Networks (2016), *Worldwide Infrastructure Security Report Volume XI*. www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf (accessed 27 April 2016).

Article 29 Data Protection Working Party (2010), *Opinion 3/2010 on the principle of accountability*. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

Atlantic Council, Zurich Insurance Group (2015), *Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*, www.atlanticcouncil.org/images/publications/risk-nexus-september-2015-overcome-by-cyber-risks.pdf.

Aven, T., Renn, O., and Rosa E., (2011) "On the ontological status of the concept of risk" in *Safety Science* 49 (2011), pp.1074–1079.

BBC News (2015), *Sony Pictures computer system hacked in online attack*, www.bbc.com/news/technology-30189029 (accessed 27 April 2016).

Betterley R. (2015), *The Betterley Report- Cyber/Privacy Insurance Market survey*, www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf.

Bundesamt für Sicherheit in der Informationstechnik (2011), *Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen (Study of IT Security in Small and Medium sized Enterprises)*, https://www.bsi.bund.de/DE/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.html.

CBC News (2012), Chinese Hackers Suspected In Long-Term Nortel Breach, www.cbc.ca/news/business/nortel-hit-by-suspected-chinese-cyberattacks-for-a-decade-1.1218329 (accessed 27 April 2016).

Centre for Information Policy Leadership (2014), *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, www.informationpolicycentre.com/files/Uploads/Documents/Centre/The_Role_of_Risk_Management_in_Data_Protection_FINAL_Paper.PDF

Centre for Strategic and International Studies (2014), *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II*, www.mcafee.com/jp/resources/reports/rp-economic-impact-cybercrime2.pdf

CNIL (2010), *Guide. La sécurité des données personnelles*. www.cnil.fr/sites/default/files/typo/document/Guide_securite-VD.pdf.

Cohen, A. V. (1996), "Quantitative Risk Assessment and Decisions about Risk" in Hood, C. and Jones, D. K. C. *Accident and design – contemporary debates in risk management*. UCL Press, London.

Edinburgh Group (n.d), *Growing the global economy through SMEs*. www.edinburgh-group.org/media/2776/edinburgh_group_research_-_growing_the_global_economy_through_smes.pdf (accessed 27 April 2016).

ENISA (2009), *An SME Perspective on Cloud Computing*, www.enisa.europa.eu/publications/cloud-computing-sme-survey.

Ernst & Young (2014), *Get ahead of cybercrime EY's Global Information Security Survey 2014*. http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

FERMA (2015), *European Risk and Insurance Report*. www.ferma.eu/app/uploads/2014/10/20141009-FERMA-BenchmarkingSurvey2014-v8-FINAL-FINAL.pdf.

Goodin D. (2015), *Pay or we'll knock your site offline — DDoS-for-ransom attacks surge*, http://arstechnica.com/security/2015/11/pay-or-well-knock-your-site-offline-ddos-for-ransom-attacks-surge/

Hutter, B.M., and Jones, C. (2007), "From government to governance: external influences on business risk management" in the *International Journal of Regulation and Governance* 1(1) 27-45, ISSN 1748-5991

International Cyber Security Protection Alliance (2013), *Study of the Impact of Cybercrime on businesses in Canada - Fighting Cybercrime Together*, www.icspa.org/wp-content/uploads/2014/12/ICSPA-Canada-Cyber-Crime-Study-Report.pdf.

ISO (2009a) *ISO 31000:2009 Risk management—Principles and guidelines*, www.iso.org/iso/catalogue_detail?csnumber=43170.

ISO (2009b), *ISO Guide 73: 2009*, www.iso.org/iso/catalogue_detail?csnumber=44651.

Kaiser, M. (2011), Prepared testimony of the National Cyber Security Alliance on the State of Cybersecurity and Small Business before the Committee on House Small Business Subcommittee on Healthcare and Technology, United States House of Representatives, 1 December 2011, http://smallbusiness.house.gov/uploadedfiles/kaiser_testimony.pdf (accessed 27 April 2016).

Krebs, B. (2014), *Target Hackers Broke in Via HVAC Company*, http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ (accessed 27 April 2016).

Lee, R., Assante M. and Conway, T. (2014), *ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack*. https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf (accessed 27 April 2016).

Lunden, I. (2015), *Target Says Credit Card Data Breach Cost It $162M In 2013-14*, http://techcrunch.com/2015/02/25/target-says-credit-card-data-breach-cost-it-162m-in-2013-14/ (accessed 3 May 2016).

Mayer et al, (1995), "An Integrative Model of Organizational Trust", *The Academy of Management Review*, Vol. 20, No. 3, New York, pp. 709-734

McGlasson, L. (2009), *Heartland Payment Systems, Forcht Bank Discover Data Breaches*, www.bankinfosecurity.com/heartland-payment-systems-forcht-bank-discover-data-breaches-a-1168 (accessed 3 May 2016).

National Cyber Security Alliance, Symantec (2012), *NCSA / Symantec National Small Business Study*. https://staysafeonline.org/download/datasets/4389/2012_ncsa_symantec_small_business_study.pdf

OECD (forthcoming), *Opportunities and Challenges in Developing a Risk Management Approach to Privacy*.

OECD (2015a) *Digital Economy Outlook*, OECD Publishing, Paris, DOI: http://dx.doi.org/10.1787/9789264232440-en

OECD (2015b), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264229358-en

OECD (2015c), *Guidance for Improving the Comparability of Statistics Produced by Computer Security Incident Response Teams (CSIRTs)*, www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2013)9/FINAL&doclanguage=en

OECD (2015d), *OECD Recommendation for Digital Security Risk Management for Economic and Social Prosperity*, OECD Publishing, Paris, DOI: http://dx.doi.org/10.1787/9789264245471-en.

OECD (2015e), *CEOs and governments should treat digital security as an economic risk* www.oecd.org/newsroom/ceos-and-governments-should-treat-digital-security-as-an-economic-risk.htm (accessed 27 April 2016).

OECD (2013) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Publishing, Paris, DOI: http://dx.doi.org/10.1787/9789264196391-en.

OECD (2012), "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 Digital Economy Papers*, No. 214, OECD Publishing, Paris, DOI: http://dx.doi.org/10.1787/5k4dq3rkb19n-en

OECD (2011), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, OECD Digital Economy Papers, No. 176, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/5kgf09z90c31-en

Office of the Australian Information Commissioner (2014), *Data breach notification — A guide to handling personal information security breaches*, www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches (accessed 2 June 2016).

Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner of British Columbia (2012), *Getting Accountability Right with a Privacy Management Program*, www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp.

Pagliery, J. (2015), *The inside story of the biggest hack in history*, http://money.cnn.com/2015/08/05/technology/aramco-hack/ (accessed 27 April 2016).

Perlroth, N. (2012), *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back.* www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html (accessed 27 April 2016).

Polonetsky, J., Tene O., and Jerome J.(2014), *Benefit Risk Analysis for Big Data Project*, www.futureofprivacy.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf.

Ponemon Institute, (2015), Ponemon Cyber Crime Report: IT, Computer & Internet Security, http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/.

Rashid, F. (2015), *Inside the Aftermath of the Saudi Aramco Breach*, www.darkreading.com/attacks-breaches/inside-the-aftermath-of-the-saudi-aramco-breach/d/d-id/1321676 (accessed 27 April 2016)

The Economist Intelligence Unit (2013), *Information Risk: managing digital assets in a new digital landscape*, www.economistinsights.com/search/node/information%20risk (accessed 27 April 2016).

The Japan Times (2015), Japan Pension Service hack used classic attack method, www.japantimes.co.jp/news/2015/06/02/national/social-issues/japan-pension-service-hack-used-classic-attack-method//#.VsskvU32bIU (accessed on 27 April 2016).

UK Department for Business Innovation and Skills (2015), *Small Business: What you need to know about cyber security*, www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know.

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

UK HM Government (2015), *2014 Information Security Breaches Survey*. www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

UK Information Commissioner's Office (2016), *ICO launches new data protection self-assessment tool for SMEs*. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/01/ico-launches-new-data-protection-self-assessment-tool-for-smes/.

US FCC (2015), *AT&T To Pay $25M To Settle Investigation Into Three Data Breaches*, www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0

US FTC (2006), *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress*, www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million

US Government Accountability Office (GAO) (2015), *High Risk List*, www.gao.gov/highrisk/overview (accessed 27 April 2016).

World Economic Forum (2014), *Rethinking Personal Data: A New Lens for Strengthening Trust*, http://reports.weforum.org/rethinking-personal-data/ (accessed 28 April 2016)

Worsfold, D., and Worsfold, P. (2005), "Increasing HACCP awareness: a training intervention for caterers" 125(3) *Journal of the Royal Society for the Promotion of Health*, 129-35.