OECD publishing

MEASURING DIGITAL SECURITY RISK MANAGEMENT PRACTICES IN BUSINESSES

OECD DIGITAL ECONOMY PAPERS
June 2019 **No. 283**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report summarises the three phases of the OECD project undertaken between February 2017 and November 2018 to develop a framework and indicators to measure businesses' digital security risk management practices, in line with the principles of the 2015 Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity.

The project was led by Elettra Ronchi and Vincenzo Spiezia, and undertaken by Elif Koksal-Oudot, Laurent Bernat, and Christian Reimsbach-Kounatzé, from the OECD Secretariat. The report was drafted by Benjamin Dean, consultant to the OECD.

Phase one consisted of a review of past surveys and a workshop organised jointly with the Swiss Re Centre for Global Dialogue in Zurich, Switzerland, in May 2017. In phase two, the questionnaire development and testing were undertaken in co-operation with the Brazilian Center for Studies on the Development of the Information Society (CETIC.br), under the supervision of Alexandre Barbosa and Fabio Senne. The third phase involved the piloting of a revised survey instrument in conjunction with the Federation of European Risk Management Associations (FERMA).

At each phase of the project, input was sought from a joint working group comprising delegates from the OECD Working Party on Security and Privacy in the Digital Economy (SPDE) and the OECD Working Party on Measurement and Analysis of the Digital Economy (MADE). The Secretariat wishes to thank them as well as Christine Hoepers (CERT.br), Philippe Cotelle, Tiphaine Beaupérain and Julien Bedhouche from FERMA, and Nick Kitching from Swiss Re.

This document was declassified by the Committee on Digital Economy Policy on 16 November 2018.

This publication is a contribution to the OECD Going Digital project, which aims to provide policymakers with the tools they need to help their economies and societies prosper in an increasingly digital and data-driven world.

For more information, visit www.oecd.org/going-digital. #GoingDigital

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/SPDE/MADE(2018)2/FINAL

Table of Contents

Tables

Figures

Executive Summary

Digital security incidents can affect the public image, finances, operations and physical assets of businesses and their various value chain partners and other external parties. They can undermine business competitiveness, ability to innovate and position in the marketplace. Effective digital security risk management is essential for businesses to be able to minimise the frequency and negative impact of these incidents and thereby take advantage of and thrive with digital transformation.

For this reason, policymakers in OECD countries have taken greater interest in understanding and measuring the digital security risk management practices of businesses.

In 2016, the OECD embarked on a project to fill this gap. The first step was to review past surveys that had sought to provide data related to digital security risk. It was found that these typically included few questions on the digital security risk management practices of businesses. When they did, the questions were often limited to technical measures and not in line with the 2015 Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity ("Security Recommendation"), which emphasises the economic and social dimensions of digital security risk.

With the deficiencies in the evidence based identified, the OECD sought to improve measurement in this area by developing a framework to assess the digital security risk management practices of businesses. This measurement framework comprises six modules and eighteen associated indicators. It draws heavily from the Security Recommendation. The six modules are: demographics; digital security risk governance; digital security risk assessment; digital security risk reduction practices; digital security risk transfer practices; and digital security risk awareness and training. Following the OECD model survey framework, the individual modules could be adopted by national statistical offices or other organisations, should they wish to.

A survey instrument was designed with the goal of understanding the digital security risk management practices of a specific population: risk managers. This survey instrument was subjected to cognitive testing then reviewed and piloted between July and September 2018. The outcomes of the pilot suggest that the framework, on which the survey instrument is based, is robust though improvements could be made to the design of the survey instrument itself. These changes primarily relate to the length of the survey in terms of the time required to respond; removal of some questions that may be redundant given the limited utility of responses received; and slight adjustments or changes to the way in which some questions and their response options are designed.

This project has yielded a set of tools that represent major progress: a measurement framework, a set of core indicators and a pilot survey instrument. These tools provide a solid foundation for further work. Future work could usefully be undertaken to develop: a reduced list of indicators and truncated survey instrument to lower response burden and augment response rate to future surveys; a simpler survey instrument, which would involve developing a simplified risk management vocabulary for less data-intensive/non-expert respondents, particularly SMEs; a maturity model for enterprise digital security risk management; depth measures of certain aspects of digital security risk management such as digital intensity, information sharing or the contents of digital security policies; and robust indicators and methodologies for measuring incidents and their associated impacts.

Introduction

The need for better statistics and analysis to support and inform policy making on digital security risk management has grown alongside the emergence of new ways in which businesses communicate, process and store digital information as well as increasing globalisation of the digital economy and interdependence. Yet policymakers' ability to measure, analyse and understand the digital security risk management practices of businesses has not kept sufficient pace with this technological change. Without these abilities, it is difficult for businesses, policy makers, insurers and other stakeholders to effectively manage the risks that digital threats, vulnerabilities and incidents create. This impedes their ability to successfully navigate the risks and opportunities created due to ongoing digital transformation.

Developing and implementing policies related to digital security is difficult because the actual digital security needs of businesses are not entirely understood. Moreover, the factors that hinder potentially successful policies and initiatives are not known. This lack of knowledge suggests that policy makers possess an incomplete understanding of the risk exposure of a large swath of the digital ecosystem and thus their policies may be sub-optimal in terms of focus and resource allocation.

These concerns were expressed in the 2016 OECD Ministerial Declaration on the Digital Economy (the "Cancún Declaration") in which ministers declared that they will support implementation of coherent digital security risk management and privacy protection practices, with particular attention to the freedom of expression and the needs of small and medium enterprises and individuals and that they will, "strengthen the collection of internationally comparable statistics on… use of digital technologies by firms and individuals across the economy and society; and contribute to developing new indicators for the digital economy, such as on trust". The OECD examined these issues as part of its work on improving the evidence base on digital security and privacy policy making following the 2016 Cancun Ministerial on the Digital Economy.

The 2015 Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity (the "OECD Security Recommendation") also called for collaboration in the development of, "internationally comparable digital security risk indicators based on common measurement methodologies, standards and best practices, as appropriate, to improve effectiveness, efficiency and transparency in the management of digital security risk."

This report synthesises the process and findings of an OECD project to fill this gap by establishing a framework to better measure digital security risk management practices in businesses, particularly SMEs (the "OECD project"). This project complements previous OECD work on digital security measurement since 2012 (OECD, 2012 and 2015b). Its central contribution is a measurement framework and associated set of indicators that can be used to assess the digital security risk management practices of businesses. This framework was translated into a survey instrument, which was then subsequently piloted. The output of this survey instrument provides data that present a glimpse of the digital security risk management practices of a unique population of businesses.

The report is structured as follows:

- The remaining sections of the **introduction** provide a background of the process undertaken in the course of the two-year long OECD project.
- **Part One** provides a brief overview of the state of affairs in the measurement of digital security risk and its management prior to the OECD project. Primarily a summary of Phase One of the project, it identifies and explains long-standing issues specific to and associated with the measurement of digital security risk and its management.
- **Part Two** provides an in-depth explanation of the measurement framework for the assessment of digital security risk management practices in businesses. Each module and its associated indicators is then explained.
- **Part Three** provides an analysis of the outcomes of a pilot survey instrument based on the measurement framework, which was conducted with FERMA during July to September 2018. The goal of this section is to identify ways in which the pilot survey instrument might be improved given the responses received.
- The **conclusion** of the report provides recommendations for future efforts that build on this project.
- A set of **annexes** include: a list of past surveys reviewed in the course of phase one of this project; the full pilot survey instrument; and a summary of the key findings from the Cetic.br cognitive testing of the draft survey instrument.

The timeline of the OECD project

The OECD project was undertaken over almost two years. It involved an extensive process of development, review and finalisation of a measurement framework, set of core indicators and a pilot survey instrument. This sub-section explains the process and the steps undertaken as a part of each phase.

Phase One: Review of past surveys and proposed draft framework

Phase One involved a review of national and international surveys on digital security risk management; an examination of the challenges related to terminology and measurement; and a comparison of past surveys and data. This provided the basis for the establishment of measurement priorities, which in turn informed the development of a proposed draft measurement framework for internationally comparable indicators on digital security risk management practices in businesses.

This phase identified that past surveys examining digital security typically included few questions on digital security risk management practices of businesses. When they did, the questions were often limited to technical measures. The results of the majority of past surveys were not representative of the overall business population (owing to small sample size and low response rates), had issues with selection and response bias (owing partly to a lack of randomisation in participant selection) and did not employ common definitions, typologies and taxonomies. The report for Phase One concluded with a proposed draft measurement framework, which included proposed draft indicators and laid a path for overcoming the measurement and methodological issues of past surveys.

Following input from SPDE and MADE Delegates and other experts in May 2017, and input from the joint working group guiding this project, the framework and indicators were further revised and refined. Several important changes were made. It was decided that module “Risk awareness, risk management skills and governance” should be divided-up into three separate modules. The module “Incident impact evaluation” was not included

owing to complex methodological issues that these concepts pose. Finally, the joint working group remained divided over whether the module on 'Awareness' and the module on 'Governance' required dedicated modules. A proposed alternative would have involved removing these two modules and instead measuring these aspects of digital security risk management using composite measures derived from indicators in other modules.

Phase Two: A priority list of core indicators

Phase Two of the OECD project involved development and delivery of a priority list of core indicators for measuring digital security risk management in businesses. The draft indicators were heavily based on the Principles contained in the OECD Security Recommendation and Companion Document. They were structured into six modules following the OECD Model Survey framework.

At the conclusion of phase two, input was again sought from from SPDE and MADE Delegates and the joint working group. This input led to a reduction in the number of indicators and slight conceptual adjustments. A demographic module was added to the framework and some modules were reordered.

A draft pilot survey instrument was then developed by a joint task force between the OECD and the Brazilian Network Information Center (NIC.br) through the Regional Center for Studies on the Development of the Information Society (Cetic.br) and the Brazilian National Computer Emergency Response Team (CERT.br). The draft survey instrument underwent cognitive testing, which was used to evaluate translation and adaptation issues of cross-national questionnaires; to identify possible sensitivities to specific issues; and to ensure that the questions were appropriate for each target population. Cognitive interviews were carried out between 26 March to 11 April 2018 in three municipalities in Brazil.

Key conclusions from the cognitive testing included: most questions and concepts presented in the draft survey instrument were associated with a more technical or incident management perspective than expected; companies appeared to have very low maturity in terms of implementing digital security risk management policies; problems of comprehension increased among small and medium enterprises (SMEs), especially for those that did not have an IT team; and responses varied depending on the level of digital intensity found across enterprises that performed different economic activities. Annex C includes a more detailed summary of the main findings from the cognitive testing.

Phase Three: Pilot survey and analysis of outcomes

The OECD Secretariat reviewed the survey instrument based on outcomes from the cognitive testing. The revised survey instrument was then piloted in association with the European Federation of Risk Management Associations (FERMA), which brings together 22 risk management associations across 21 European countries. A major advantage of partnering with FERMA for the pilot was their ability to provide targeted access to a population of 4,800 risk managers across Europe.

Risk managers are a desirable population to survey because the OECD Security Recommendation calls for integration of digital security risk management into the overall risk management decisions of an organisation. By surveying risk managers directly it was possible to determine in what ways and to what extent the Principles of the OECD Security Recommendation are already operationalised within enterprises.

The pilot was conducted between July and August 2018. 80 complete responses were received from enterprises in 15 countries[1]. The respondents were primarily risk managers

in mostly large enterprises, which helped overcome some of the issues identified in the cognitive testing stage though at the expense of a more representative sample of the overall business population.

1. Challenges in the measurement of digital security risk and its management

There is a great deal of debate as to the nature and prevalence of digital security threats; the pervasiveness and types of vulnerabilities; the frequency, severity and impacts of digital security incidents; and the effectiveness of different security practices. These debates occur due to a number of conceptual, methodological and epistemological issues confronted when measuring phenomena associated with digital security. Compounding these issues, surveys as a measurement tool present their own unique challenges particularly when deployed for the purposes of measuring elements associated with digital security risk.

This section examines each of these categories of measurement issues. It is a summary of the key insights from Phase One of the OECD project, which reviewed a number of past surveys on digital security risk.[2] This section explains ongoing debates related to the measurement of digital security, digital security risk and its management. It explains and provides examples of common methodological pitfalls that past measurement and surveying efforts have fallen-into. In doing so, it summarises the issues that the OECD project sought to address and overcome so as to achieve its goal of improving the measurement of digital security risk management practices in businesses.

Conceptual issues in measuring digital security

At a conceptual level, the term 'security' is not often well defined in the field of digital security. Discussions on security sometimes fall into a dichotomous, binary conceptions whereby something is deemed 'secure' or 'insecure' [DSTI/CDEP/GD(2018)14]]. This discussion lacks much of the nuance that is required to develop an understanding that would, in turn, lead to effective management of the risks that would lead to greater security. A more nuanced understanding would consider issues like the relative security of *something* (the entity or its activity), *somewhere* (the context) against some *adversary* (including intentional and unintentional as well as human and non-human –e.g. natural– threats sources), among other issues. Clearing up this conceptual ambiguity is the first step towards more accurate and useful measurement of digital security and, by extension, the effective management of associated digital risks.

The field of digital security risk management is also in a constant state of flux. Much is still unknown because of the dynamic phenomena under examination, and because of limits to one's ability to observe and understand the phenomena under examination, among other reasons. Even when data are collected and analysed, thereby giving a greater understanding of the current state of affairs, this understanding can quickly become outdated again owing to the dynamic nature of the phenomena.

Where evidence is available, disagreements frequently arise as to the 'correct' way in which to frame findings and the criteria by which to infer or evaluate results. For instance, a common assertion is that digital security incidents are increasing in frequency and severity. However, one perspective (Jardine, 2015) contends that a more accurate picture of the security of the digital environment requires that related statistics — including mobile vulnerabilities, malicious web domains, zero-day exploits and web-based attacks, among others — be expressed as a proportion of the growing size of the Internet ('normalised').

When expressed this way, the picture that emerges is one where the number of incidents may be increasing at a slower rate than the number of people and devices using the internet.

Another a common assertion is that data breaches are increasing in scale, frequency and severity. However, Edwards et al (2014) analysed a database of reported data breaches and their outcomes. They found that, "neither size nor frequency of data breaches has increased over the past decade." The authors contend that the high-profile incidents that have attracted attention in recent years can be explained by the heavy-tailed statistical distributions underlying the dataset. These findings were later supported by Romanosky (2016) who found that, "the cost of a typical cyber incident [in our sample] is less than $200 000 (about the same as the firm's annual IT security budget), and that this represents only 0.4% of their estimated annual revenues." Findings such as these demonstrate the nuance and complexity in assessing the true severity of data breaches, though these are just one sub-set of all digital security incidents.

Complicating one's ability to draw inferences and make decisions based on empirical findings is the limitation of using the past as a guide to future outcomes. This limitation is a particular issue in the digital domain given that the severity and impact of digital incidents in aggregate often follow heavy-tailed distributions (Taleb and Cirillo, 2015). While one may consider Jardine's contention that on average (i.e. most days) cyberspace is getting 'safer', or Edwards et al's and Romanosky's findings on the stable frequency and severity of past data breaches, with heavy-tailed distributions, the worst days in the future can be far worse than any seen before (Geer, 2016).

All these debates point to the inherent difficulties in effectively measuring then interpreting the results of analyses in the field of digital security risk management. There are few simple and definitive answers and, where there are, there is no guarantee that the answers will remain 'true' in the future. To correctly measure and evaluate evidence in this field one must maintain an open-mind and continually re-examine the assumptions that underlie one's inferences or conclusions.

Methodological challenges for digital security surveys

Compounding these issues are a series of methodological issues linked specifically to surveys that seek to collect data on elements associated with digital security risk and its management. Surveys (or polls) are one of the most frequent sources for empirical data used for policy making. They are based on questions asked to people (i.e. the sample population). Their goal is to learn about certain attributes of the population based on a sample of this population through statistical inference (OECD, 2012).

Every year new reports – based on surveys - are published with indicators covering specific aspects of digital security. However, final reports for these surveys commonly 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. While such statistics can be useful for certain narrow purposes, they are often not sufficiently robust to be used with a high degree of confidence for development of public policy.

Two common weaknesses of surveys include: the operation of a survey can be costly and time consuming; and poorly designed surveys tend to confirm existing preconceptions and fail to bring up new insights (OECD, 2011). On top of these, past digital security risk management surveys tend to suffer from specific weaknesses in the areas of: sampling; ensuring sufficient technical knowledge of respondents; accurate incident detection and

reporting; accurate impact measurement/estimation; and lack of common definitions, terminologies and taxonomies. These limitations undermine the usefulness, comparability and reliability of the survey results.

Sampling and selection

In order for inference from survey results to be correct, the survey sample needs to clearly state the target population and then provide a representative sample of that population. In the event that the target population is the general business population, but the survey sample is not representative of that population, different weights can be applied so as to compensate for sampling shortcomings.

Selection of respondents for a survey sample should be randomised so as to reduce the potential for response or selection bias. In addition, non-response bias may be present, which affects results given that individuals or businesses who did not respond to the survey might be substantially different in terms of underlying beliefs from those who completed the survey. The sample frame might be biased for many other reasons. This could have to do with influence from external forces, such as media coverage, or because respondents are rewarded with a monetary sum.

The availability of large sample frames from which to draw a representative sample of a population, thereby addressing sampling issues, can be difficult and costly. While national statistical offices typically have access to large databases to randomly draw their sample, many private consultancies or security vendors (who undertake the majority of the currently publicly available digital security risk surveys) do not have access to such large samples. This limits the representativeness of these survey results to sub-sets of the overall business population and tends to increase the error rate, which in turn reduces the ability to draw accurate and appropriate inferences from the survey results.

Requisite technical knowledge

It is important to ensure that an appropriate person responds to the survey instrument within the target enterprise. Who is deemed ‘appropriate’ is largely determined by the subject matter covered in the survey instrument as well as the size and structure of the enterprise in question.

Determining an appropriate respondent for a digital security risk survey could start by focusing on people with a certain role and/or level of seniority in the enterprise. To measure digital security as an economic and social challenge, the respondent should have an understanding of the business activities and economic and social risks that the business faces. This person should also understand the technical aspects of digital security and would ideally possess knowledge of: human resources and training; corporate governance; risk management; network and computer configuration; among others. This person should be in a sufficiently senior role to be able to have visibility across the enterprise. Depending on the business size, this person may have one of the following titles: Chief Risk Officer; Chief Risk Manager; Internal Auditor; Accountant; Risk (and Audit) Management Committee Chair/Member; Chief Executive Officer; Chief Operating Officer; or Chief Finance Officer. The respondent would ideally not be someone who is only in charge of the information communication technologies (ICTs) as this person will not likely possess sufficient knowledge of business activities and other important enterprise risk management elements.

This definition of 'appropriate' is subject to some limitations in practice. Some enterprises may not have a person in one of these roles. This is likely to be the case in many micro and small enterprises as well as in some medium-sized enterprises with low digital intensity. Large firms without a risk management culture and framework in place may also not have a person with the appropriate profile to address digital security as a business risk. In such instances, the more appropriate respondent would likely be the owner of the enterprise or someone else in a senior, leadership position.

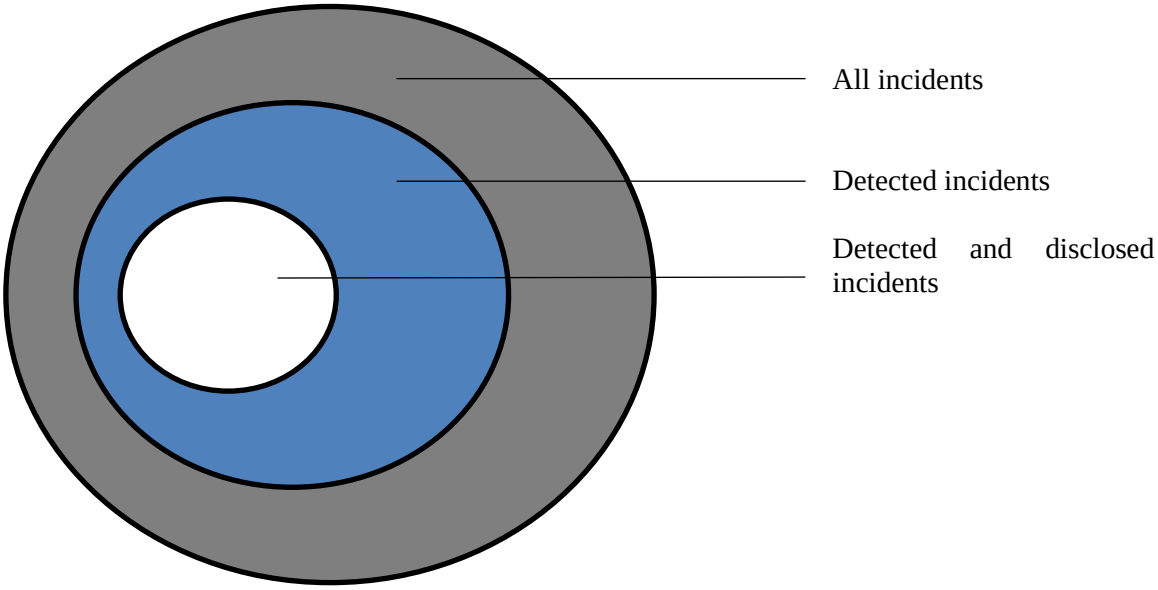
Digital security risk management can involve concepts that certain respondents may not understand. Such concepts can be technical (e.g. denial of service, malware) or risk-related (e.g. risk assessment, risk transfer). Furthermore, the terminology associated with such concepts may not be homogeneous across sectors, countries and cultures. If the respondent is not properly versed in the technical concepts, or if the survey is worded in a way that a generalist might not understand, the reliability of the responses to the survey would suffer. A balance therefore needs to be struck between a respondent with sufficient seniority to have visibility over multiple domains in the enterprise and sufficient knowledge of basic technical concepts to be able to accurately respond to the survey instrument. One way to potentially mitigate against this risk is to phrase the survey instrument in a way that a generalist should be able to understand, which implies avoidance of overly technical jargon or specialised domain knowledge.

Incident detection and reporting

There are a number of methodological issues that make incident reporting and incident impact reporting problematic in the context of surveys, some of which had been identified in previous OECD work (OECD, 2015b). Respondents are likely to understate the true number of digital security incidents that they incur during a given time period. For instance, in any one year, a business might experience a certain number of digital security incidents. Of this total universe of incidents, the business might not detect all of the incidents. These non-detected incidents will not be taken into account when respondents answer questions related to past incidents. To compound this issue, if respondents do not feel that their answers will be kept confidential, they may not disclose the true extent or all of the incidents that were detected (e.g. due to reputational concerns).

It is not definitively known what proportion of incidents go undetected. Some studies have quoted estimates that suggest anywhere between 60% to 89% of security incidents go unreported (Edwards et al, 2014). If these estimates are accepted, this would imply that a substantial proportion of the total universe of incidents forms part of an "unknown unknown". However, at an epistemological level, it may simply be impossible to definitively determine the proportion of incidents that are undetected owing to the nature of the phenomenon and the possible methods of inquiry.

Figure 1. Limitations in the detection and disclosure of digital security incidents

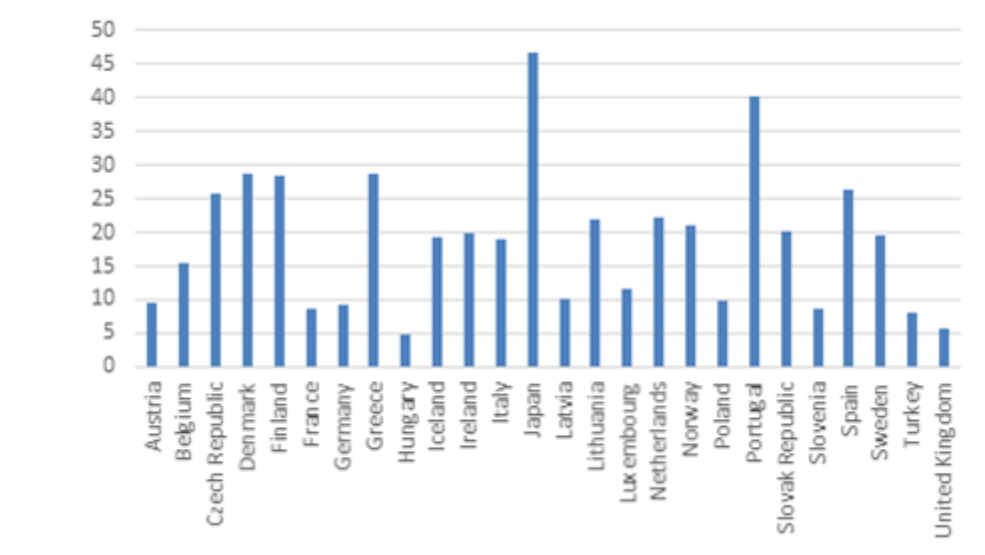


Note: Provided for illustrative purposes only. The actual proportion that each concentric circle occupies is not yet known.
Source: OECD.

The consequences of these methodological issues bear out in the examples provided below, which are based on the results of prior surveys. Consider first the results of the OECD ICT Access and Use by Businesses Survey for 2010. Figure 2 provides comparable cross-country statistics on the digital security breach incidents detected by businesses. There is wide variance across countries, in aggregate, which raises questions as to whether the proportion of enterprises experiencing incidents is really higher in some countries over others or whether it is just that the incident detection capabilities are higher in enterprises in some countries over others.

Figure 2. Digital security incidents (breaches) detected by enterprises in OECD countries, 2010

Percentage



Source: OECD.

Going into more detail, it could be that only some incidents are detected and reported and that the more important determinant is the size of the enterprise and the class of incident in question. Table 1 shows the results from a survey released in the United States in 2005. The results are measured as a proportion of all enterprises affected by size and incident class. Note the wide variance not only across different incident classes but also the size of the respondent enterprise. Some of the incidents are more likely to be detected, due to their differing impacts, than others. Moreover, the proportion of respondents that are likely to have the capabilities to detect certain classes of incidents is also likely to differ across enterprises of different sizes. This raises questions as to the reliability and usefulness of the survey results.

Table 1. Prevalence of computer security incidents, United States, by business size (headcount), 2005

Percentage

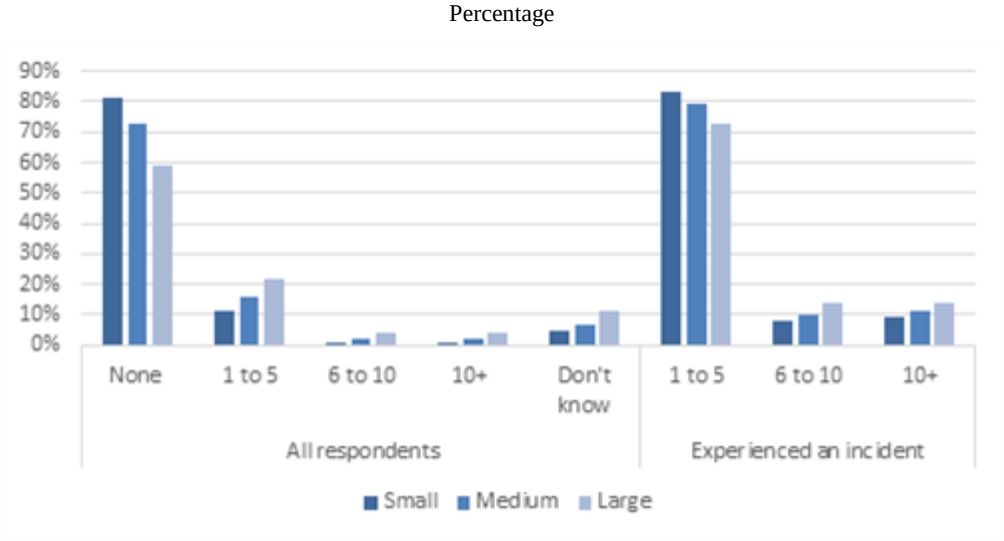
	All incidents	Cyber attack	Cyber theft	Other
All businesses	67	58	11	24
2-24	50	44	8	15
25-99	59	51	7	17
100-999	70	60	9	24
1000+	82	72	20	36

Source: 2005 National Cyber Security Survey.

Once reduced to the level of the frequency of incidents per enterprise, it becomes apparent that the number of incidents detected and reported is actually quite small for most enterprises and is largely a function of the size of the enterprise in question. Below are

results from a survey released in Australia in 2009. Note immediately that the majority of enterprises do not report any incidents of any class at all over the prior year. Of those that did detect and report incidents, again the majority report 1-5 incidents in total. It is not clear what class of incidents are detected and reported, which makes it difficult to understand where the related threats and vulnerabilities lie, which in turn would assist in effectively managing the relevant risks. Further work is required to better understand where the most reliable incident data could be sourced and whether surveys could provide any useful additional data[3].

Figure 3. Number of computer security incidents experienced, by business size, Australia, 2009



Source: 2009 ABACUS survey.

Impact measurement, estimation and reporting

The true financial impact of a digital security incident is difficult to accurately estimate and measure. As a first step, it is important to differentiate between direct costs, indirect economic losses and opportunity costs.

When a digital security incident like a data breach occurs, there are **direct costs** incurred by the organisation that has been breached. These costs might include network repair, hiring of security consultants and purchase of credit monitoring services for those affected. Direct costs are redistributive, that is, they represent cash paid by or stolen from one entity to another.

This is different to **indirect economic losses**, which represent foregone economic activity or destroyed economic value. The indirect losses from digital security incidents are those that cannot be linked by a reasonable degree of accuracy directly to a particular incident (Gordon and Loeb, 2006). Such categories typically comprise: loss of customer trust/reputational damage, reduced uptake of digital technologies due to lack of trust, and opportunity costs and foregone productivity associated with the need to invest in non-digital infrastructure (Anderson et al, 2012).

There is also an **opportunity cost** tied to the direct costs due to digital security incidents, investment in preventative security measures. For private enterprises, rather than spending

funds on security consultants and preventative measures, those same funds could have been invested in activities that contribute to the top-line revenue generating activities or measures to increase the productivity of the firm. These concepts are not always differentiated in digital security surveys, leading to inaccurate cost/loss estimates from incidents.

Costs and losses typically comprise many categories, each with their own relative measurement challenges. The examples below, which are drawn from past surveys, demonstrate the wide variance that occurs between different cost/loss methodologies and, by extension, the importance in clearly defining what is being measured in a way that can be reliably reported by the respondent.

The direct costs following an incident, such as hiring consultants or repairing IT infrastructure, might be relatively easily estimated due to the availability of invoices for discrete services. However, one must be careful in defining key terms (e.g. incident type, cost/loss categories, time scale) so as to generate useful, reliable and comparable results.

The results from the survey below pertain to the direct losses (though losses are not clearly defined) from incidents incurred by enterprises in the United States in the year prior to 2005. They indicate that the majority of respondents incurred a total loss of USD 1,000 – 9,000 over the prior year. The distribution of these losses across the population include a minority of enterprises for which no loss was incurred. The reported losses and their distribution vary substantially across different incident categories though the differences between the different categories is not always clearly delineated.

Table 2. Monetary loss incurred from computer security incidents, by type of incident, United States, 2005 (USD)

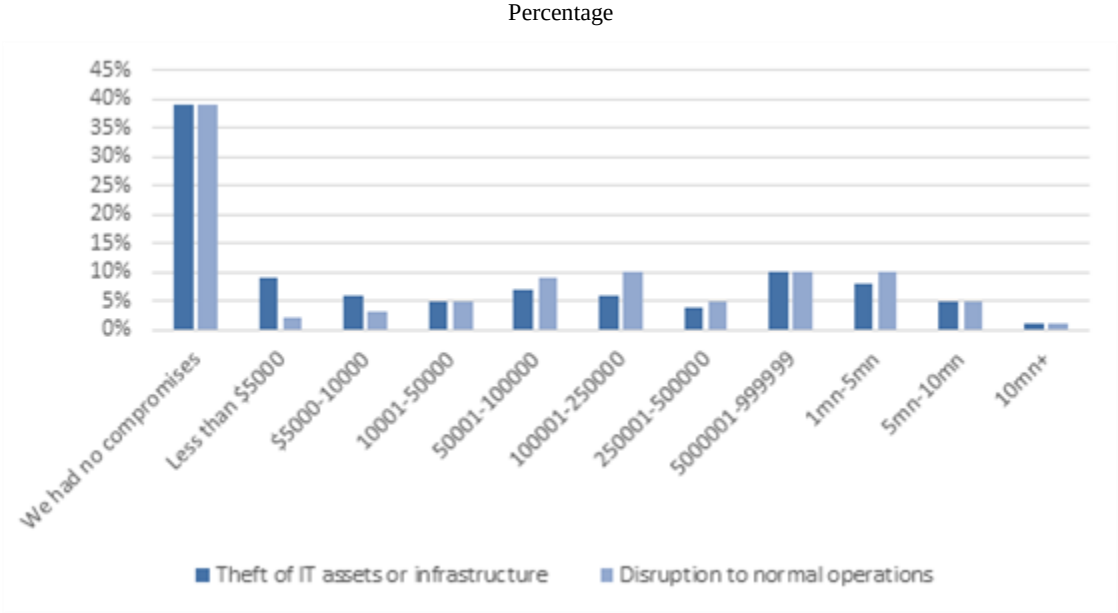
	No loss	USD 1,000-9,000	USD 10,000-99,000	USD 100,000+
All incidents	10	51	27	13
Cyber attack	9	57	25	9
Computer virus	7	60	24	9
Denial of service	19	52	24	6
Vandalism or sabotage	11	59	21	9
Cyber theft	6	26	38	30
Embezzlement	4	19	44	33
Fraud	7	32	36	24
Theft of intellectual property	9	17	36	38
Theft of personal or financial data	11	31	29	29
Other computer security incidents	20	49	25	7

Source: 2005 National Cyber Security Survey.

The indirect losses from an incident such as lost revenue or the value of stolen intellectual property, however, might in some cases, though not always, be difficult to distinguish. For instance, separating the proportion of a fall in revenue due to an incident from that which was due to broader economic conditions over a certain period of time may not be entirely clear (and if the impact is clear, it may not necessarily be clear to the survey respondent). By contrast, determining the indirect costs due to business interruption is relatively easier to determine though, again, these costs may not be clear to the survey respondent.

The figure below summarises results from a survey undertaken in 2016. The results are meant to include all costs from certain incidents that affected the respondent's enterprise over the prior year. Perhaps the most meaningful conclusion one can draw from these results is that the majority of respondents did not incur any costs given they incurred no incidents. Assuming that those who reported costs did indeed incur incidents, the distribution of reported costs cover all bands in a relatively uniform way though it is not clear which enterprises incurred what costs. This is relatively important given that costs are likely to vary substantially across enterprise size, industry and digital intensity.

Figure 4. "Approximately how much did damage or theft of IT assets and infrastructure / disruption to normal operations cost your organisation over the past 12 months?", 2016.



Source: 2016 Ponemon State of Cybersecurity in Small and Medium-Sized Businesses.

Ideally, estimation of indirect losses would require the establishment of a counter-factual (i.e. what revenues might have been had the incident not taken place). This might be possible if the revenues were from a stable company operating in a mature industry over many years. However, this is rarely the case in reality. Moreover, many digital security incidents involve or affect intangible assets, which can be difficult to value. Further work is needed to more clearly categorise and measure the economic impacts of digital security incidents before sufficiently reliable and useful data can be collected from a survey instrument[4]. Use of simulations (e.g. Monte Carlo) might permit bounded, probabilistic estimates to be calculated, but have been underutilised so far in the field, and so future work might make use of these and other related analytical techniques.

Definitions

When attempting to compare the results across surveys, aside from the methodological difficulties detailed above, a major obstacle is the lack of consensus on definitions, typologies and taxonomy for digital security incidents, threats and vulnerabilities, among many other aspects. Three particular examples stand out from the digital security risk and management surveys of businesses examined in Phase One: digital security, enterprise size and incident.

Digital security: there was great variance across surveys with regard to the terminology used to refer to digital security. The terms 'information', 'internet', 'computer' or 'cyber' were variously used in conjunction with the term 'security'. In some cases, no definition was provided for the term in use, which makes it difficult to understand what the survey results relate to, to draw inferences and conclusions from the results, and to compare results across surveys and over time.

Enterprise size: different definitions may be used for small, medium and large businesses in surveys where results are stratified by enterprise size. This is a common issue worldwide for surveys and statistics relating to businesses and is not limited to digital security risk management surveys. The definition of an SME (or SMB in the US) might be determined based on annual revenue or current headcount. The threshold at which a business is deemed to be an SME differs across countries and within countries, by industry sector. Moreover, some samples include businesses with zero employees (sole traders) while others do not. Some surveys exclude businesses with less than ten employees. Surveys refer variously to enterprises, businesses, firms, establishments, etc. and do not define what is meant by the term used. All these elements impede cross-survey comparison of results.

Table 3. Definitions of enterprise size and sample population used in past surveys

Survey name	Definition
Australian Business Assessment of Computer User Security (ABACUS) survey, 2009	Small businesses were defined as those with zero to 19 employees; medium businesses, as those with 20 to 199 employees; and large businesses, as those with 200 or more employees.
FERMA European Risk and Insurance Report, 2014	Respondents could list annual revenue or headcount. Employment size classes: <1000, 1000-5000, 5001-10000, 10001-20000, 20000+
France CGPME Survey of Members for Cybersecurity, 2015	Employment size classes: 0, 1-9, 10-49, 50-250, 250+
Korean Survey on Information Security in Businesses, 2015	Employment size classes: 1-4, 5-9, 10-49, 50-249, 250+
UK PWC Information Security Breaches Survey, 2015	Employment size classes: <10 employees, 10-49, 50-249, 250-499, 500+
UK Digital Capabilities in SMEs Survey, 2014	Employment size classes: 0, 1-9, 10-49, 50-249, (250+ not included)
National Computer Security Survey, 2005	Excludes sole traders. Employment size classes: 25-99, 100-999, 1000+
Ponemon 2016 State of Cybersecurity in Small and Medium-Sized Businesses	Employment size classes: Firms with less than 100 to 1000 headcount

Incidents: Vastly different taxonomies were used to refer to classes of incidents with some mixing threats, vulnerabilities, incidents and impacts together under broad, all-encompassing terms. For instance, many surveys used the term 'breach' to refer to an 'incident', broadly speaking, when the term 'breach' would typically be used to refer to a subset of incidents affecting confidentiality and possibly integrity of data. The best surveys clearly explain to respondents what each term means in a glossary. However not all surveys provide a glossary, which compounds the problem of respondents not understanding technical concepts given that the terms themselves are not clearly defined. This in turn reduces the reliability of the results from such surveys. The lack of clear definition or a glossary also impedes readers' ability to interpret what the final results of the survey mean.

Table 4. Definitions of incident across past surveys

Survey name	Definition
Australian Business Assessment of Computer User Security (ABACUS) survey, 2009	"Computer security incident": any unauthorised use, damage, monitoring, attack or theft of your business information technology.
France CGPME Survey of Members for Cybersecurity, 2015	Cyber attack ("cyberattaque"): no definition provided
Korean Survey on Information Security in Businesses, 2015	No definition provided for "security incident" in the final report (questionnaire not available) In the final report, however, a definition for "malicious code" is provided: A software program designed for malicious activities such as system destruction and information leakage (virus, worm, adware, spyware, etc.) ?
UK PWC Information Security Breaches Survey, 2015	Terms "security" with "breaches", "incidents", "attacks" used interchangeably throughout the results. No precise definitions provided in the final report.
National Computer Security Survey, 2005	"Computer security incident": 'incident' refers to any unauthorised access, intrusion, breach, compromise or use of this company's computer system."
Ponemon 2016 State of Cybersecurity in Small and Medium-Sized Businesses	"Cyber attacks": no definition given.

Unit of measurement

An overall unit of measurement has to be explicitly named when surveying the practices of digital security risk management in businesses so as to derive useful, relevant data from the survey instrument. It might be theoretically possible for some indicators to relate to the individual respondent, to units or divisions within the business or to the overall business itself. Moreover, risk management practices as well as the absolute and relative levels of security are likely to differ depending on the unit of measurement in question (e.g. the practices of an enterprise as a whole as compared to those of an individual respondent).

Conclusion

These constraints, limitations and issues provide a backdrop for the decisions made in developing the measurement framework, indicators and pilot survey instrument during this OECD project. A detailed explanation of how they inform the pilot survey in particular can be found in section 3 of this report.

2. A measurement framework for digital security risk management in businesses

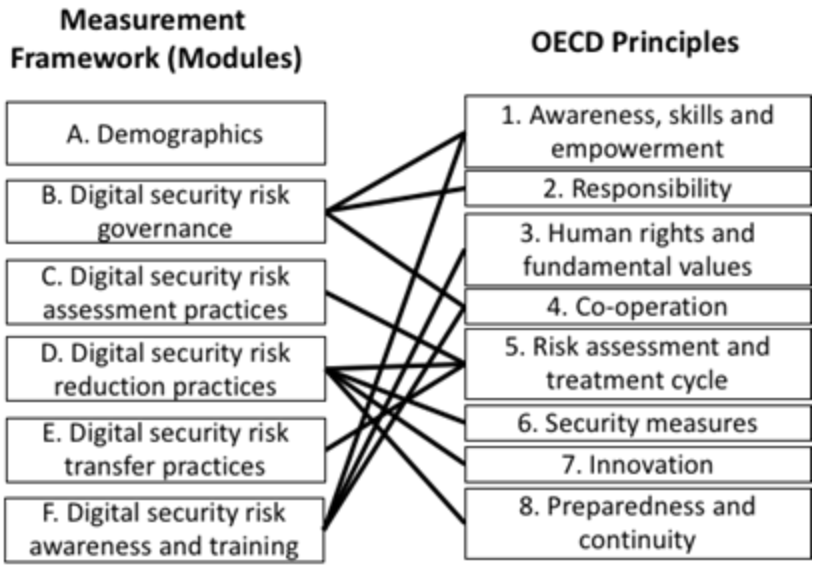
This section explains the measurement framework developed to assess the digital security risk management practices of businesses. It explains how this framework was translated into the survey instrument used for the pilot with FERMA. This framework forms the basis for collection of data that can: help businesses benchmark their relative digital security risk management practices against peers; and help inform government policies intended to raise the level of digital security risk management maturity of businesses in OECD countries.

The framework has been developed over the course of almost two years with the input of an joint working group comprising delegates from the SPDE and MADE Working Parties; delegates of these Working Parties; as well as input from other experts from OECD countries. The draft framework was initially proposed as an output of Phase One of the OECD project. In Phase Two, the framework and indicators were reviewed then finalised based on extensive feedback. A draft survey instrument was then developed by a joint task force of OECD and Cetic.br and subsequently subjected cognitive testing by Cetic.br.

Following revisions based on feedback, Phase Three involved a pilot of a survey instrument with FERMA. The pilot provides additional feedback from the field as to the interpretability of questions and the concepts they involve as well as the usefulness and suitability of data collected for each of the indicators. Its results are introduced in section 3 of this report. As technology and policy priorities evolve, and lessons from the pilot survey are taken into account, the survey will need to be reviewed and adapted. In some cases, countries may choose to add new country-specific indicators based on policy needs or context-specific legal and regulatory requirements, less technical terms and/or provide further specificity based on policy needs or the relative maturity of the respondent. However, this should not affect the international comparability of the results.

The measurement framework drew heavily from the OECD Principles contained in the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity (‘Security Recommendation’). Representing a consensus amongst OECD countries as to what constitutes desirable practices with regard to digital security risk management, the Security Recommendation provides a solid foundation on which to develop indicators to assess the digital security risk management practices of businesses. A diagram of how the individual modules correspond or are conceptually linked to the Principles in the Security Recommendation is provided below in Figure 5. The multiplicity of links between the framework and the Principles reflects the interrelated nature of the Principles.

Figure 5. Connections between OECD measurement framework and OECD Principles



Source: OECD.

The framework adopts a modular approach as per the OECD "model survey" framework (OECD, 2011). To be broadly useful, the OECD model survey comprises separate, self-contained modules that ensure flexibility and adaptability to a rapidly changing environment. Core modules can be added-on to existing national surveys or administered as a stand-alone survey while supplemental modules can be used as needed by countries. The approach allows broad measurement of core concepts on an internationally comparable basis while allowing countries to tailor some of the content they collect to address country-specific needs.

Table 5 shows the full measurement framework, which was used to structure the pilot survey instrument. It comprises six modules and eighteen indicators. The number of indicators differs across modules as do the number of questions asked to collect data for each indicator through the survey instrument. Each indicator seeks to measure the percentage of the total number of enterprises (respondents).

Table 5. Measurement framework as applied in the pilot survey instrument

Module/Indicator number	Description
A	**DEMOGRAPHICS**
A1	Proportion of enterprises by geographic location
A2	Proportion of enterprises by size
A3	Proportion of enterprises by economic activity
A4	Proportion of enterprises by turnover
A5	Proportion of enterprises by digital intensity
B	**DIGITAL SECURITY RISK GOVERNANCE**
B1	Proportion of enterprises that have responsibilities for digital security risk allocated to a specific role within the organisation
B2	Proportion of enterprises that have a policy in place to manage digital security risk
B3	Proportion of enterprises that have a process in place to monitor and review digital security risk management
B4	Proportion of enterprises that had structures or processes in place to enable cooperation and for reporting on digital security risk management within the enterprise
C	**DIGITAL SECURITY RISK ASSESSMENT PRACTICES**
C1	Proportion of enterprises that assess digital security risk as part of the overall enterprise risk management
C2	Proportion of enterprises that regularly take specific actions as part of the digital security risk assessment
D	**DIGITAL SECURITY RISK REDUCTION PRACTICES**
D1	Proportion of enterprises that took risk reduction measures
D2	Proportion of enterprises that share information on threats, vulnerability, incidents and risk management practices or security measures
E	**DIGITAL SECURITY RISK TRANSFER PRACTICES**
E1	Proportion of enterprises that use insurance to transfer digital security risk
E2	Proportion of enterprises that did not purchase an insurance policy, by reason for non-adoption
E3	Proportion of enterprises that transfer digital security risks through an insurance policy, by type of risks transferred
E4	Proportion of enterprises that adopt other risk transfer practices
F	**DIGITAL SECURITY RISK MANAGEMENT AWARENESS AND TRAINING**
F1	Proportion of enterprises that adopted awareness-raising and training practices on digital security risk management

Below is an explanation of each module; its associated indicators; and how they translate into the pilot survey instrument. Where appropriate the indicator and/or question is tied back to the OECD Principle to which it is associated. The full pilot survey instrument can be found in Annex B.

Module A: Demographics

Rationale: Module A includes indicators and questions intended to permit stratified samples and subsequent analysis based on sub-populations of enterprises.

Indicator A1: Records the geographic location of the enterprise and the geographic location of the parent company in the event that the respondent is a subsidiary.

Indicator A2 and A4: Registers the size of enterprise by full-time headcount (Indicator A2) or by annual turnover (Indicator A4). The thresholds for headcount allows for SMEs to be partitioned-off based on the specific definition of the country in question. The field for annual turnover provides a continuous variable, which allows for SME thresholds to be set wherever desired.

Indicator A3: Determines the economic activity (i.e. industry) of the respondent's enterprise based on the ISIC rev. 4 standard.

Indicator A5: Measures the digital intensity (or reliance) of the respondent's enterprise. This is important because subsequent modules related to the digital security risk management practices of the enterprise in question can be assessed in context (i.e. if the enterprise does not use many digital technologies then subsequent answers that suggest low digital security risk management practices/maturity would be of relatively less concern).

Module B: Digital security risk governance

Rationale: Module B is intended to assess whether the enterprise has an appropriate digital security risk management governance framework in place. Such a framework is a requirement for effective digital security risk management, particularly for relatively large organisations in which the complexity of digital security risk management often requires the adoption of a formal framework. That this module appears early reflects a consideration of governance as an over-arching concept that touches all aspects of and is a key determinant in successful digital security risk management in an enterprise.

Indicator B1: Allocation of responsibility to specific roles within an enterprise is a cornerstone of effective digital security risk governance. This is reflected in Principle 2 of the OECD Principles and in the FERMA/European Confederation of Institutes of Internal Auditing (ECIIA) report on corporate governance and cyber security (2017)[5]. For this reason, indicator B1 and its associated questions attempt to elicit whether the enterprise has a role/department dedicated to overall risk management; whether this role/department is also in charge of managing digital security risk; and which role specifically is in charge of managing digital security risk and determining the acceptable level of digital security risk for each business activity.

Indicator B2: A governance framework is generally reflected in a corporate or organisational policy or governance document. Such a framework can take as many shapes as there are organisations' cultures and styles of management (OECD, 2015a). For this reason, indicator B2 and its associated questions (B2a, B2b, B2c) aim to determine whether a policy – written or unwritten – is in place within the enterprise and, if so, what it covers.

Indicator B3: The OECD Security Recommendation insists that effective digital security risk management requires continuous review of digital security risk as a part of an on-going assessment process (ibid). Indeed, Principle 5 of the Recommendation is 'risk assessment and treatment cycle', which reflects its importance in the overall OECD Security Recommendation. For this reason, indicator B3 attempts to determine whether there is a process in place to monitor and review digital security risk management within the enterprise; which monitoring practices are performed and; in the event that they are, how often these practices occur.

Indicator B4: The OECD Security Recommendation, under Principle 4 'Co-operation', says that co-operation, "should take place within governments, public and private organisations"(ibid). This co-operation is, "essential for security measures, innovation and preparedness measures to be fully implemented" (ibid). The reason it is essential is that effective digital security risk management requires the interaction between the technical side of an enterprise (e.g. the ICT team) and the business side of the enterprise that it supports (e.g. the executive team, risk management department, etc.). Only by bringing these parties together can decisions be made that balance the need for security with the need to promote the economic activities and thus prosperity of the enterprise in question.

For this reason, indicator B4 seeks to determine whether interaction occurs in a structured way between staff in charge of business management and ICT when assessing digital security risk exposure.

Module C: Digital security risk assessment practices

Rationale: Continuous risk assessment and treatment is essential to ensure that security-related decisions are appropriate to and commensurate with the risk and the economic and social activity at stake (ibid). For this reason, module C aims to measure certain practices that constitute an appropriate risk assessment process.

Indicator C1: The OECD Security Recommendation calls for digital risk to be approached as an economic risk rather than solely be considered as a technical problem that calls for technical solutions. Doing so requires that digital risk, "be an integral part of an organisation's overall risk management and decision-making processes" (OECD, 2015a). For this reason, indicator C1 seeks to determine whether there is an overall risk management process in place within the enterprise and, if so, if the digital security risk management process is a part of this overall process.

Indicator C2: The digital security risk assessment should ideally comprise three stages. Risks should be: identified, analysed, and evaluated[6]. For this reason, indicator C2 seeks to determine not just whether these three stages are followed in some form within the enterprise but, additionally, who within or outside of the enterprise fulfills the tasks that each of these stages imply. Moreover, the OECD Security Recommendation says that this process should be continuous/ongoing. For this reason, a question in the survey instrument seeks to determine how often the enterprise assesses the possible consequences of digital security incidents that could affect the enterprise's activities. This specific element (i.e. the possible consequence of digital security incidents) was chosen owing to the dynamic nature of digital security threats and vulnerabilities, which require greater cyclical monitoring than other elements owing to their dynamic nature.

Module D: Digital security risk reduction practices

Rationale: Risk reduction is one of the four broad categories of risk treatment options that those responsible for risk management within a business can choose from when treating risk.

Indicator D1: Risk reduction should aim to reduce the digital security risk to the acceptable level determined in the risk assessment (ibid). Question D1a (cf. annex B) seeks to determine whether any digital security risk reduction practices were in place owing to a risk assessment. To reduce risk, security measures can be selected and operated, innovation can be considered in relation to both the security measures and the activity at stake; and preparedness and continuity measures can be defined and applied when an incident happens (OECD, 2015a). This indicator seeks to determine if any of these three forms of risk reduction practices was undertaken in the enterprise in question over the previous twelve months.

Indicator D2: As per Principle 4 'Co-operation' of the OECD Security Recommendation, "Since stakeholders are both interdependent and dependent on the digital environment, co-operation is essential" (ibid). One way in which this co-operation can be operationalised is in the form of information sharing between stakeholders. Indicator D2 thus seeks to determine if the enterprise has shared information on digital security threats, vulnerability,

incidents, risk management practice or security measures with any one of a number of external stakeholders.

Module E: Digital security risk transfer practices

Rationale: Risk transfer is one of the four broad categories of options that those responsible for risk management within an enterprise face when choosing to treat risk. Risk transfer involves, "moving the unwanted effects of uncertainty on the activity's objectives to someone else" (ibid).

Indicator E1: One of the common ways in which risk might be transferred to another stakeholder is via a contract, particularly through insurance. Indicator E1 measures directly whether the respondent's enterprise has any current insurance policy that covers digital security risk.

Indicator E2: In many OECD countries, enterprise take-up of insurance policies that cover digital security risk exposures remains at a relatively low level. Policymakers in these OECD countries often seek to understand why this take-up is low as a basis on which to implement measures that might alleviate these perceived obstacles. Indicator E2 therefore seeks to determine the reason why respondents do not have any such insurance policy.

Indicator E3: Insurance policies that cover digital security risk exposures (sometimes referred to as 'cyber insurance') come in many shapes and forms. Sometimes they are 'stand-alone' policies (i.e. policies that only cover digital security risk exposures) and other times they are bundled into existing insurance lines (e.g. Directors and Offices [D&O] or Property and Casualty [P&C]) (Romanosky, et al, 2017). Indicator E3 and its associated question therefore seeks to determine which risk exposures are covered by the enterprise's single or potentially numerous insurance policies that may cover such risks.

Indicator E4: Insurance is one form of many risk transfer mechanism. Indicator E4 seeks to determine which other commonly used contractual and non-contractual transfer mechanisms are used by the respondent's enterprise.

Module F: Digital security risk management awareness and training

Rationale: "Managing digital security risk requires first to understand that such risk exists" (ibid). Awareness is therefore a foundation for all the other OECD Principles. Stakeholders who are not aware that risk exist end up unwittingly accepting the risk instead of assessing then treating it. Awareness is the first step towards taking responsibility (Principle 2 of the OECD Security Recommendation). The ability to make responsible decisions (i.e. effective manage risk) requires the skills to do so. For these reasons, this module measures various practices, including training, are in place to create and/or raise awareness of digital security risk and its management within the enterprise.

Indicator F1: Awareness might be raised by one of many specific practices (e.g. workshops, conferences, etc.). Skills are acquired via various means including education, training, experience, etc. Indicator F1 seeks to determine which of these practices and means are pursued in the enterprise in question. It also seeks to determine who receives the awareness raising or training given that different levels of awareness and different kinds of skills (acquired via training) are required by people so as to fulfil their role in the effective management of digital security risk. Directors and business line managers are particularly important in this regard. Without awareness and the ability to effectively manage risk from above, efforts to do so from below are less likely to succeed (FERMA & ECIIA, 2017 and WEF, 2016). For this reason, the final question in the survey instrument attempts to

ascertain why training was not provided to people in these roles (in the event that such training was not).

3. The pilot survey and its outcomes

This section provides an analysis of the responses to the pilot survey undertaken in conjunction with FERMA between July and September 2018. FERMA brings together 22 risk management associations across 21 European countries. Their membership provides access to a targeted population of 4,800 risk managers across Europe. Within an enterprise, risk managers are responsible for understanding the risks that can affect the enterprise's abilities to achieve its objectives and subsequently implementing a coordinated set of practices and methods to treat (control) those risks (ISO, 2009). This implies that they possess an understanding of the economic trade-offs associated with security practices within an enterprise.

The 2015 OECD Security Recommendation has a focus on:

> *"the economic and social objectives of public and private organisations and the need to adopt an approach grounded in risk management. Instead of being treated as a technical problem that calls for technical solutions, digital risk should be approached as an economic risk; it should therefore be an integral part of an organisation's overall risk management and decision making processes."*

Surveying risk managers made it possible to determine in what ways and to what extent the Principles of the OECD Security Recommendation are presently operationalised within a target population of enterprises with what should be relatively sophisticated risk management practices. In the event that the enterprise did not have a risk manager, the requested respondent to the survey included: Internal Auditor; Accountant; Risk (and Audit) Management Committee Chair/Member; Chief Executive Officer; Chief Operating Officer; or Chief Finance Officer. Note that none of these roles are technical/IT roles. This reflects the Recommendation's stance that digital security risk be approached as an economic risk rather than as a technical one.

The approach adopted for the pilot comes with shortcomings though. In the event that digital security risk management practices are not integrated within the enterprise's overall risk management structure (i.e. it is treated as a technical risk), a target population of risk managers will not be able to accurately respond to the questions as they require an understanding of the technical security decisions made within the IT department. As the results from this pilot demonstrate, even within a relatively sophisticated population in terms of risk management, a large proportion of enterprises still do not integrate digital security within their overall risk management framework. A more comprehensive picture of the digital security risk management practices in enterprises would need to include both the risk managers' perspective and the IT perspective.

Moreover, a large proportion of the population of respondents available via FERMA are large enterprises. This OECD project originally sought to gain insights into the digital security risk management practices of SMEs. Unfortunately, such insights could not be gleaned from the target population of the pilot. The pilot survey instrument reflects the characteristics of the target population in that it uses relatively advanced risk management concepts and terms. This vocabulary would not be appropriate for a target population containing a greater proportion of SMEs. In the future, the measurement framework used to design the pilot survey instrument could be used to develop a revised instrument for surveying SMEs.

The analysis of the pilot survey results in this section is provided with the goal of identifying strong and weak elements of the pilot survey instrument as suggested by anomalous or unusually consistent patterns in the complete responses. The analysis is split into two parts. The first part examines the complete responses while the second part briefly examines the incomplete responses.

The goal of this analysis not to provide representative statistics on the current digital security risk management practices of enterprises. This is because the pilot could not adhere to the methodological best practices explained in section 1 of this report. Specifically, the population is not representative of the general enterprise population; the respondents were not randomly selected; and the results are subject to selection and response bias amongst other biases. In order to have estimates for the entire population of enterprises, information on the target population – a sample frame – is required. This involves each unit of the population of interest being available for selection with a probability greater than zero. Such a survey should be conducted following a probabilistic approach that permits randomised selection of enterprises.

Throughout the analysis, suggestions are made as to how future iterations of the survey instrument might be directed so as to provide better quality responses and data. As an overall suggestion and in order to improve the quality of the data collection process in the future, it is important that field control reports are generated during the data collection process. This includes, but is not limited to: field training manuals for interviewers, instruction manuals for respondents and performance reviewers.

Results

FERMA started circulating the pilot survey to thirteen volunteer member associations on 11 July 2018. The associations then forwarded the pilot survey to their respective memberships on differing dates due in part to the impending holiday break. The population of recipients differed across associations and countries with some opting to send the survey to all members (e.g. AIRMIC in the UK) while others preferred to send it to certain populations (e.g. GVNW in Germany sent only to large enterprise members). Associations and their members did not have the same time windows and length of time to respond to the survey. Reminders to circulate the survey to members were sent in mid-August, end-August and mid-September.

In total, 80 completed responses were received across all countries. The bulk of these responses came from enterprises in Belgium (16 responses), Finland (15 responses) and France (14 responses). The response rate varied across associations with the highest seen in BELRIM (Belgium) with 18%. The overall response rate was approximately 3% though this is somewhat suppressed by the conspicuous lack of responses from AIRMIC (United Kingdom), which constituted almost 50% of the survey recipients (1058 of 2602 recipients). Removing AIRMIC from the total brings the overall response rate up to 5%, which still remains low. The low response rate is likely to be due to a combination of: the holiday time period during which the pilot survey was circulated; the chained mode of survey administration, the narrow sample selection in some national associations; and the length of the survey.

Table 6. Recipients of pilot survey, number of responses and response rates

Risk management association	Number of recipients	Total responses	Response rate (%)
AGERS (Spain)	57	3	5
AIRMIC (United Kingdom)	1058		0
AMRAE (France)	795	14	2
APOGERIS (Portugal)	23	2	9
BELRIM (Belgium)	91	16	18
DARIM (Denmark)	81	9	11
FINNRIMA (Finland)	95	15	16
GVNW (Germany)	85	9	11
ALRiM (Luxembourg)	na	1	na
MARM (Malta)	22	1	5
NARIM (The Netherlands)	148	0	0
POLRISK (Poland)	39	3	8
SIRISK (Slovenia)	21	3	14
SIRM (Switzerland)	87	4	5
TOTAL	**2602**	**80**	**3**

Table 7. Country in which the head office of the group is located

Country	Number of responses	Percentage of total
Belgium	11	14
Bermuda	1	1
Denmark	7	9
Finland	8	10
France	9	11
Germany	9	11
Luxembourg	1	1
Malta	1	1
Netherlands	2	3
Poland	2	3
Portugal	2	3
Slovenia	1	1
Spain	5	6
Switzerland	4	5
United Kingdom	1	1
NA	15	19
Total	80	

Table 8. Country in which the enterprise is located

Country	Number of responses	Percentage of total
Belgium	16	20
Denmark	9	11
Finland	15	19
France	14	18
Germany	9	11
Luxembourg	1	1
Malta	1	1
Poland	3	4
Portugal	2	3
Slovenia	3	4
Spain	3	4
Switzerland	4	5
Total	80	

Module A: Demographics

Indicators A2 and A4 collect data on the size of the respondent's enterprise by headcount and revenue. By both measures, the vast majority of respondents would be considered large enterprises (90% by both headcount and by annual turnover)[7]. Indicator A3 collects information on the main industry of the enterprise. The largest proportion of respondents belong to the manufacturing industry (24%) followed by financial and insurance activities (16%) as well as transportation and storage (13%).

Table 9. Industries to which the respondent enterprises belong

ISIC rev. 4	Industry	Number of responses	Percentage of total
B	Mining and quarrying	1	1
C	Manufacturing	19	24
D	Electricity, gas, steam and air conditioning supply	5	6
E	Water supply; sewerage, waste management and remediation activities	2	3
F	Construction	5	6
G	Wholesale and retail trade; repair of motor vehicles and motorcycles	5	6
H	Transportation and storage	10	13
I	Accommodation and food service activities	2	3
J	Information and communication	3	4
K	Financial and insurance activities	13	16
M	Professional, scientific and technical activities	5	6
N	Administrative and support services	2	3
Q	Arts, entertainment and recreation	2	3
P	Education	1	1
R	Other service activities	5	6
Total		80	

Table 10. Size of respondent enterprises, by headcount

Size class	Number of responses	Percentage of total
Under 10	1	1
10 to 49	3	4
50 to 249	4	5
250 to 499	5	6
500 to 999	6	8
1000 to 2499	32	40
2500 to 4999	5	6
5000 to 9999	6	8
10000 or more	18	23
Total	80	

Indicator A5 measures the digital intensity of the respondent's enterprise. Assessed with nine different technologies/uses of technology, the output gives a snapshot of the extent to which the enterprise is reliant upon and thus must manage the risk associated with the digital technologies in question. Across all respondents, the digital intensity of the cohort

is relatively high, which might be expected given the size of the enterprises in question. The mean number of technologies used is 7.8 with a median of 8. All respondents had a website and almost all (98%) ran an intranet. e-Commerce was the least prominent use of digital technology (73%). Interestingly broadband (76%) was also not as widely used as one might expect given the widespread availability of broadband internet in the European countries where these enterprises are based. The high incidence of "Don't know" as a response to this particular option (21%) suggests that there may be a need to clearly define what constitutes a broadband connection. It is also possible that this question may be redundant given that all the other technologies require internet access (broadband or not) and so it should be assumed that some form of internet connection (broadband or not) exists.

A key element missing from the demographics section has to do with determining the role of the respondent in their enterprise. While this is potentially less of an issue for this pilot survey with FERMA, owing to the large respondent enterprises and the associated higher probability of the respondent being responsible for risk management, it should be rectified in future iterations of the survey instrument, particularly in the event that more SMEs are present in the sample population.

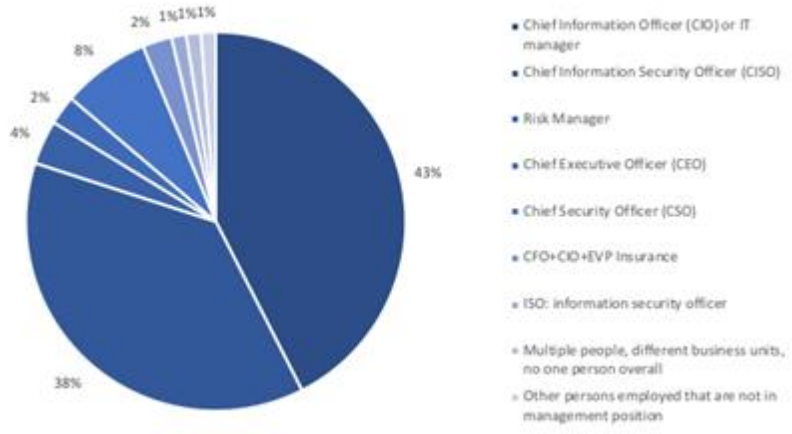
Module B: Digital security risk governance

The majority (85%) of respondents had a department or person employed who was primarily in charge of overall enterprise risk management. However, of this sub-set[8], only a third (32%) had that person or department in charge of managing the digital security risk of the enterprise. Instead, the Chief Information Officer or IT manager (43%) or the Chief Information Security Officer (38%) took on this responsibility. By contrast, the Chief Executive Officer (33%) was most likely to be responsible for deciding the acceptable level of digital security risk for each business activity, followed by the Chief Information Officer or IT manager (19%). In a small number of instances, the Board of Directors (4%) was responsible, which was manually input via 'Other (please specify)'.

Figure 6. Indicator B1: Proportion of enterprises that have responsibilities for digital security risk allocated to a specific role within the organisation (QB1c)

Who is in charge of managing digital security risk of the enterprise?[9]

As a percentage



Note: n = 80.

The vast majority of respondents (84%) had either a written or unwritten digital security policy. Of this sub-set, again the vast majority (90%) had a written digital security policy[10]. Given this high proportion, it may be more expedient in the future to only ask the question related to the type of policy with an additional response option of "Do not have policy". The actual contents of these policies varied substantially, which provides some interesting insights. Almost all (91%) allocated roles and responsibilities for digital security risk management in the enterprise as well as covering awareness raising and training (93%). Risk transfer was unlikely to appear in these policies (37% answering 'Yes') though the high proportion of "Don't know" (15%) for this and for 'risk treatment processes' suggest that these response options may not have been well understood by respondents. The response option 'risk treatment process' may be redundant given that other subsequent options contain elements of such a process (e.g. 'decision on digital security measures', 'risk transfer').

Another way to interpret the data collected for this indicator is to consider the 'depth' of the security policies. Depth could be measured by considering how many practices are covered by the policies across the cohort given nine options were provided in the survey instrument. When measured this way, the mean and median number of practices covered is approximately 6.6 out of a maximum of 9 with a standard deviation of 2.7 for a sample of 80 respondents. This suggests that the enterprises in this cohort had relatively deep security policies in the highly likely event that the enterprise had such a policy to begin with.

Table 11. Indicator B2: Proportion of enterprises that have a policy in place to manage digital security risk (QB2c)

Does the digital security policy cover any of the following?

As a percentage

	Roles & responsibilities	Cooperation processes	Audit, review & cycle of improvement	Risk assessment
Yes	91	84	82	79
No	6	7	13	13
Don't know	3	9	4	7

	Risk treatment processes	Digital security measures	Business continuity and resilience	Risk transfer	Awareness raising and training
Yes	45	79	75	37	93
No	42	12	19	48	6
Don't know	13	9	6	15	1

Note: n = 67.

The results for indicator B3, which attempts to measure the frequency of certain monitoring activities, can be difficult to interpret visually. The uniformity in responses across different activities suggests that respondents chose the same response across all monitoring activities without discerning between them. Nevertheless, of those that did undertake the activities, the majority did so on an annual basis. A small proportion did not do any of the monitoring activities. In future iterations of the survey it may be preferable to allow respondents to answer in the negative to question B2a (which asks if there is a written or unwritten policy) then subsequently to be permitted to answer question B3. It is possible that the respondent's enterprise does not have a written or unwritten plan yet still undertakes certain monitoring activities. By excluding these respondents by design, information from these enterprises (which constituted 15% of the total in the pilot) cannot be captured.

Table 12. Indicator B3: Proportion of enterprises that have a process in place to monitor and review digital security risk management (QB3)

How often does your enterprise undertake the following monitoring activities?

As a percentage

	Assess performance of the enterprise against a digital security policy	Report internally the results of previous assessment	Update policy and practices based on results of digital security audit and review process
Yearly	64	67	67
Every two years	9	3	6
More than every two years	7	6	10
Does not undertake	7	6	6
Don't know	12	18	10

Note: n = 67.

Most respondents (70%) organised physical or virtual meetings with staff in charge of business management and ICT to determine digital security risk exposure over the prior year. Only 10% did not though 20% did not know. This question is useful as it can be compared with subsequent questions related to internal and external co-operation and communication as a check on the consistency of responses.

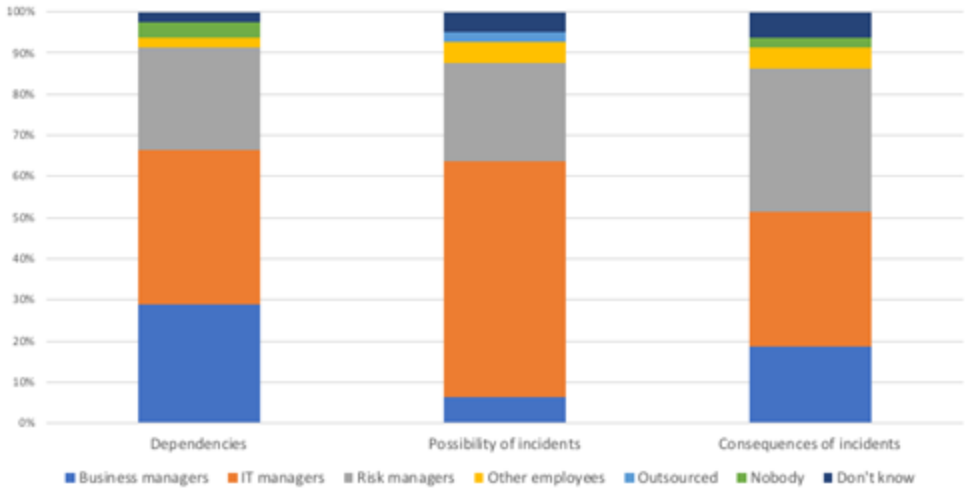
Module C: Digital security risk assessment practices

A large proportion (81%) of respondents had a regular overall process to assess the risk to which the enterprise's business activities were exposed. Of this sub-set[11], again the majority (88%) integrated digital security risk into this overall risk assessment. There was quite a deal of variation in terms of the person who undertakes the activities that constitute the digital security risk assessment. This is a positive feature of this question as it demonstrates the multi-faceted nature of digital security risk and its management. Notably, a combination of either business managers, IT managers or risk managers performed the various activities. Very few outsourced any of these activities, which might be due to the relatively large respondent enterprises. The relatively low incidence of "Don't know" responses indicates that this is a well-phrased question with quite clearly delineated and defined response options.

Figure 7. Indicator C2: Proportion of enterprises that regularly take specific actions as part of the digital security risk assessment (QC2a)

Who carries out the following activities as part of digital security risk assessment for your enterprise?[12]

As a percentage

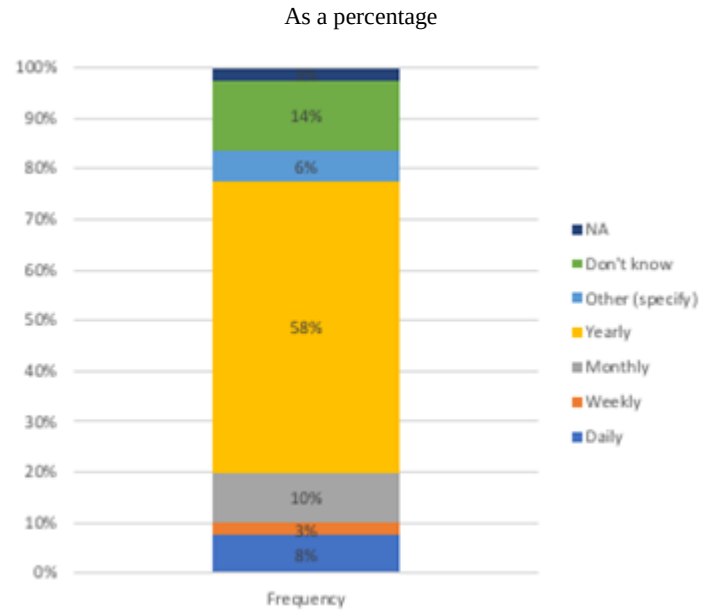


Note: n = 80

There was also great variation in terms of the frequency at which an assessment was undertaken of the possible consequences of digital security incidents that could affect the enterprise's activities. Again, this is a positive feature of the question as it demonstrates nuance in terms of the ways in which different enterprises manage their digital security risk. Most (58%) undertook this practice annually. A small proportion (14%) did not know and an even smaller proportion (6%) input their own frequency. Their responses ('bimonthly', 'semi-annually', 'once so far', 'permanent' and 'ad hoc') might be considered as additional options in future iterations of the survey instrument.

Figure 8. Indicator C2: Proportion of enterprises that regularly take specific actions as part of the digital security risk assessment (QC2b)

How often do you assess the possible consequences of digital security incidents that could affect your business activities?



Note: n = 80.

Module D: Digital security risk reduction practices

Over the previous year, most (81%) of respondents had digital security measures in place as a result of a digital security assessment. 8% did not while 11% did not know. This is important because this collective 18% did not subsequently have to answer the following question, which asks about what digital security measures were in place. There is a good chance that there were such measures in place, though they were not put in place due to the digital security assessment. Consequently this part of their digital security risk management process is not captured. This should be changed in future iterations of the survey instrument.

In terms of the aims of the measures themselves, there was great variation across respondents. Unsurprisingly, all (100%) had measures in place with the aim of protecting the activities against potential threats. Such an overwhelming majority might suggest that this option has low utility alone but it does set a benchmark against which the other options might be assessed. More interestingly, less than half (42%) had measures in place that aimed to change the business activity while a majority (80%) had measures in place that aimed to cope with the occurrence of incidents[13].

An issue with the way this question translated across to the software platform used for the pilot survey was that respondents were forced to provide an answer for the fourth option ('Other (please specify)'). Confused respondents answered "Don't know" to this option

(75%) given that they were being forced to provide other options when no such options existed. This issue recurs in a number of subsequent questions in the pilot survey[14].

It might be advisable, for simplicity's sake, to rephrase this question to ask about what kinds of measures were in place (e.g. those that involved protecting activities against potential threats, those that involved changing the business activity, etc.) rather than asking for the aim of the measures.

Table 13. Indicator D1: Proportion of enterprises that took risk reduction measures (QD1b)

Do the digital security measures in place aim to do any of the following?

	Protect the activities against potential threats	Change the business activity (by redesigning or operating it differently)	Cope with the occurrence of incidents
Yes	100	42	80
No	0	45	8
Don't know	0	14	12

Note: n = 65.

There was great variation in terms of the proportion of respondents whose enterprises shared different forms of information with external stakeholders. Compared to the 70% of respondents that shared information between management and IT internally on digital risk exposure (indicator B4), the highest proportions that shared related information with external stakeholders were 'IT suppliers' (48%) and 'insurance providers' (45%). Only 8% of respondents shared information with 'Information sharing and analysis centres'[15]. The least likely external stakeholders to receive information were 'customers' (22%).

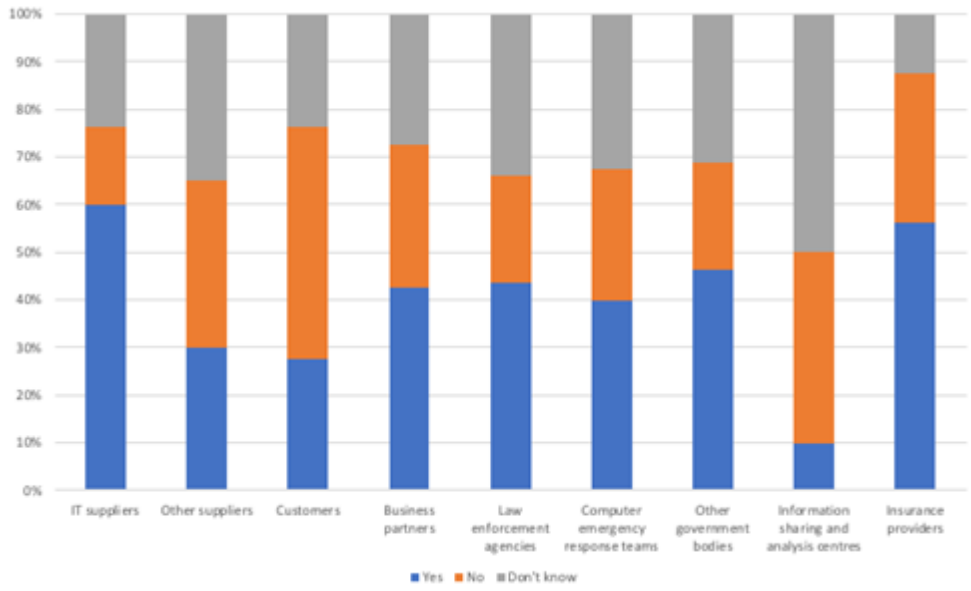
This question performs several useful tasks in that it both provides useful insights and can also be used as a check on responses to other questions. For instance, a majority (45%) shared information with insurance providers and, later in the survey, a similar majority (55%) respond that they possess insurance that covers digital security risk.

An issue with this question can be seen in the high proportion of "Don't know" responses. Ascertaining why respondents do not know answers to these questions, and whether this can be overcome in future survey instrument design changes, might be considered. It is possible that the information is shared by people in the IT department but not with those in the risk management department (who are the desired respondents to the pilot survey). Moreover, the mandatory 'Other (please specify)' response yielded two suggestions that might be appropriate for future iterations of the survey instrument: 'investors/shareholders' and 'ratings agencies'. However, this would only be appropriate in the event that there is a high proportion of publicly listed enterprises in the population of respondents.

Figure 9. Indicator D2: Proportion of enterprises that share information on threats, vulnerability, incidents and risk management practices or security measures (QD2)

Do you share information on digital security threats, vulnerability, incidents and risk management practices or security measures?

As a percentage



Note: n = 80

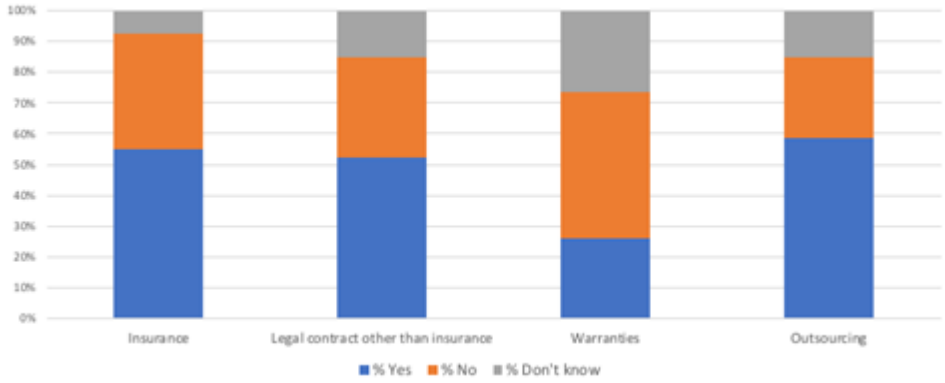
Module E: Digital security risk transfer practices

It seems that respondent enterprises fall into one of two broad groups: 1. those that (are aware that they) engage in the transfer of risk; or 2. those that do not. Similar majorities of respondents used insurance (55%), other legal contracts (53%) or outsourcing (59%) to transfer digital security risk. Only a small proportion (21%) used warranties to transfer risk. A relatively large proportion (26%) did not know if warranties were used, which perhaps points to ambiguity in the definition of this term for respondents.

Figure 10. Indicator E1: Proportion of enterprises that use insurance to transfer digital security risk (QE1) and Indicator E4: Proportion of enterprises that adopt other risk transfer practices (QE4)

Does your enterprise have any insurance policies that cover digital security risk and/or use other practices to transfer digital security risk?[16].

As a percentage



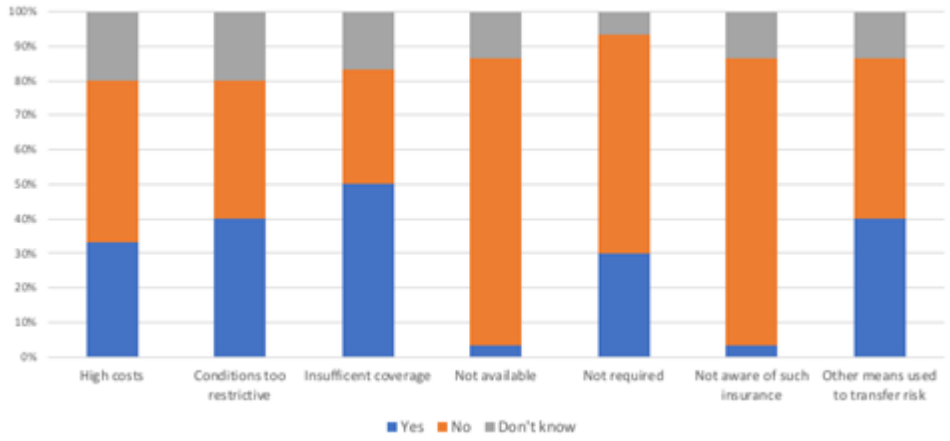
Note: n = 80

Of those that did not have insurance that covered digital security risks, the most common reasons for not doing so was that the policies available did not provide sufficient coverage (50%). Very few (3%) indicated that they were unaware of such coverage existing or that such coverage was not available in their country. Many of the respondents had multiple reasons for not having such insurance (mean = 2.13 , median = 2, n = 30). This supports the current design of the question, which allows multiple answers rather than restricting responses to the single most important one. Two of the respondents, when forced to answer the mandatory 'Other (please specify)' option, indicated that they were currently analysing their needs and planned to make a decision over the coming year.

Figure 11. Indicator E2: Proportion of enterprises that did not purchase an insurance policy, by reason for non-adoption (QE2)

What were the reasons for not taking out an insurance policy covering digital security risks?

As a percentage



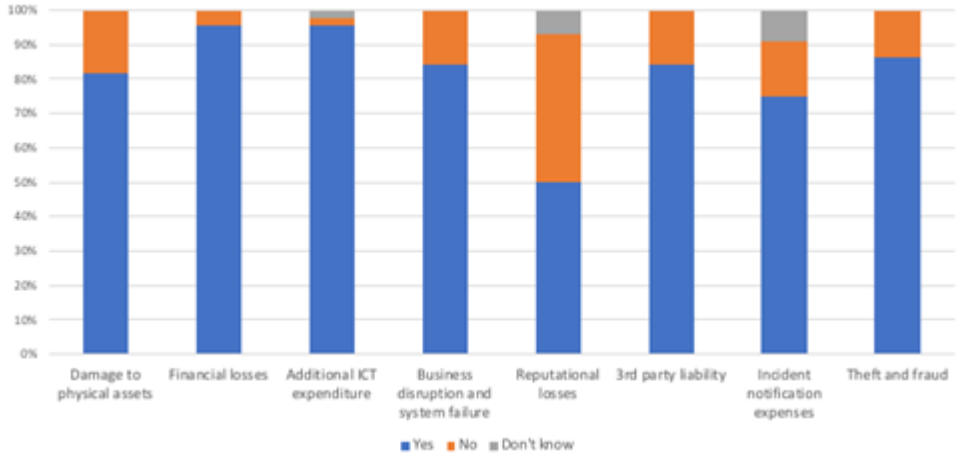
Note: n = 30.

Of those that did possess insurance that covered digital security risks, the actual coverage of these policies was relatively uniform. Very high proportions of respondents had insurance policies that covered the options provided in the survey instrument. This may be due to the relatively uniform nature of insurance policies in terms of the coverage that they typically provide. This may alternately be due to the small number of responses and some ambiguity between some response options. For instance, it may not be clear how 'financial losses' differs from 'theft and fraud'. The greatest variation was seen in 'reputational losses', which is consistent with the industry practice to not commonly cover such losses[17].

Figure 12. Indicator E3: Proportion of enterprises that transfer digital security risks through an insurance policy, by type of risks transferred (QE3)

Which of the following risks are covered through your insurance policy/policies?

As a percentage



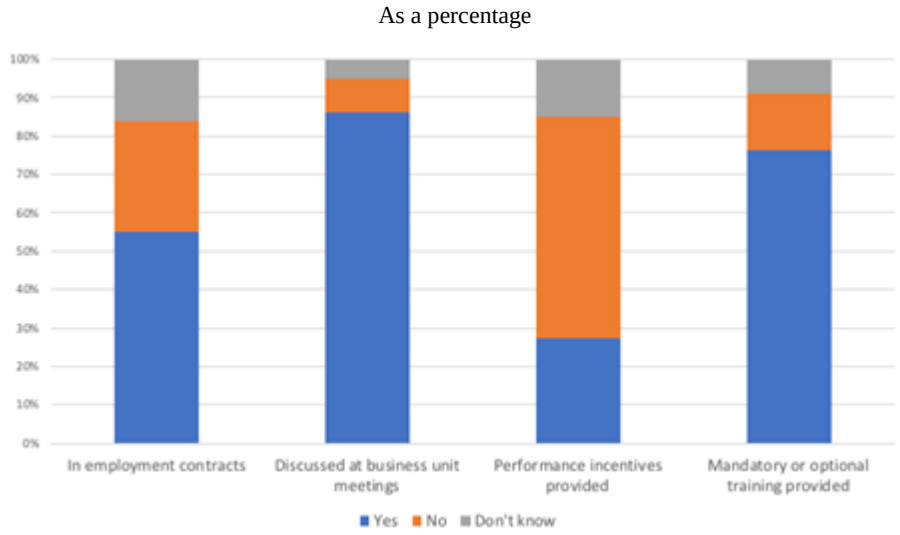
Note: n = 44.

Module F: Digital security risk management awareness and training

As a whole, a high proportion of the cohort performed a number of awareness and training practices. Most commonly digital security risks were discussed at business unit meetings (69%), followed by mandatory or optional training (61%) and inclusion of references to digital security risk in employment contracts (44%). Very few (22%) provided performance incentives to employees whose actions reduced digital security risk. The variation in responses across different options suggests that this is a useful question in uncovering the differing digital security risk management practices in enterprises.

Figure 13. Indicator F1: Proportion of enterprises that adopted awareness-raising and training practices on digital security risk management (QF1a)

Over the past year did your enterprise perform any of the following practices?



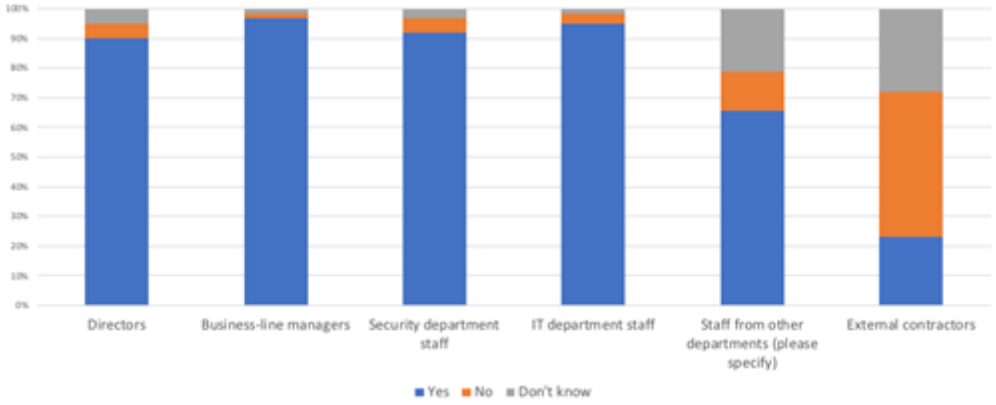
Note: n = 80; full terms used in the survey instrument were: 1. Refer to digital security risks in employment contracts, 2. Discuss digital security risks at business unit meetings, 3. Give performance incentives to persons employed due to behaviour that reduced digital security risk, 4. Provide mandatory or optional training on managing digital security risk (e.g. online courses, workshops, seminars, conferences or training provided through internal meetings).

Of those that did provide either mandatory or optional training, almost all provided it to the directors (89%), business-line managers (95%), security department staff (91%) and IT department staff (95%). Very few (18%) provided any form of training to external contractors though a larger proportion (31%) did not know, which suggests that this may not be a particularly meaningful option and could be removed in future iterations of the survey instrument.

Figure 14. Indicator F1: Proportion of enterprises that adopted awareness-raising and training practices on digital security risk management (QF1b)

Who was the training provided to?

As a percentage



Note: n = 61

The final question in the survey instrument asks those who did not provide training to directors or business-line managers why this was the case. Only four respondents fell into this sub-set and their responses tell little as to their reasons for not providing training. This suggests that this question is redundant and could be removed from future iterations of this survey instrument.

Incomplete responses

This section provides some brief insights from the relatively large number of incomplete responses to the pilot survey. The goal is to identify reasons why these responses were not completed. It is hoped that this will serve as a means by which to make changes to the survey instrument design in the future and thereby reduce the incidence of incomplete responses.

In total there were 311 incomplete responses. Of those 311, 290 clicked-on and entered the survey portal but did not register a single response to a question. Those respondents may have seen the estimated time requirement to complete the survey (10-15min) and decided at this point that they did not have this amount of time free to complete the survey.

Of the remaining 21 respondents who answered at least one question, 8 dropped-off at exactly the same point: question B1a. Another 3-4 dropped-off either just before or just after this question. These questions immediately followed the demographic module, which ends with a series of questions aimed at assessing the digital intensity/reliance of the enterprise. That is to say, these respondents did not have enough time to make it to the substantive questions in the survey instrument.

Table 14. Point at which those which answered at least one question dropped-off

Respondent number	Drop-off point
1	B1a
2	D1b
3	B1a
4	B1a
5	C1a
6	B1a
7	E2
8	D1a
9	B1a
10	B2a
11	B1a
12	B2c
13	A2
14	B2c
15	E2
16	B2c
17	E2
18	E3
19	E3
20	B1a
21	B1a

While it is not possible to determine how much time these respondents spent on their incomplete survey responses, this outcome may suggest that the survey instrument as it stands is too long, in terms of time required to answer, for voluntary responses without any form of compensation. For the most part (72%), these respondents work for enterprises with greater than five thousand employees. A risk manager in such an enterprise is likely to be time pressed and, as a result, more likely to respond to a brief and succinct survey instrument. There was no noticeable predominance in terms of the geographic location of the enterprise nor its industry.

If indeed this is the point at which a large proportion of potential respondents decide not to continue with the survey, this suggests that more responses might be acquired in the future using a truncated survey instrument with a maximum of 5-7 questions.

Recommendations for future improvement

This section provides recommendations for future work with the goal of improving measurement of the digital security risk management practices of businesses. The measurement framework and survey instrument developed over the course of this OECD project represent major steps forward. Nevertheless, there are many ways in which future efforts can build on these tools so as to continue to improve measurement in this area.

Improving response rates to future survey instruments

The response rate to the pilot of the survey instrument varied substantially across risk management associations. The highest response rate was seen in BELRIM (Belgium) with 18%. The overall response rate was approximately 3%, which increases to 5% when AIRMIC (United Kingdom), which constituted almost 50% of the survey recipients (1058 of 2602 recipients), is removed. There are many reasons why the response rate varied and, in some countries, was low. The first and likely most substantial reason was due to the pilot being undertaken during the holiday time period in Europe. It goes without saying that ideally future survey exercises should be undertaken during periods of the year when respondents are more likely to be at work and therefore more likely to respond to the survey. Nevertheless, additional measures could be taken at a survey design level to increase the probability of completed responses independent of the time of year during which the survey is undertaken. They are explained below and include: a reduced list of 'key' indicators; additions or removal of questions or response options; and simplified language for non-expert respondents.

A reduced list of 'key' indicators

The measurement framework is intentionally extensive. Following the model survey format allows for issue-specific modules to be picked-up or dropped depending on the needs of policy makers in OECD countries. However, policy makers may wish to have small snapshots across many issues, which is not something that the model survey format readily permits. Moreover, the large number of incomplete responses from the pilot suggests that the current, full survey instrument requires too much of the desired respondents' time for them to completely and/or accurately fill it out.

To overcome this situation, it might be possible to select one or a couple of indicators from each module and combine their associated questions in a truncated survey instrument. The selection of these 'key' indicators should be subjected to more rigorous debate and the outcome will likely change depending on the context-specific interests of the policymakers in question. Nevertheless, below is a proposed set of indicators that may be candidates for a truncated set of key indicators.

Table 15. Proposed set of 'key' indicators for truncated survey instrument

Module	Indicator(s)	Question
A	A1, A2, A3, & A5	Key demographics: country of enterprise, headcount, industry, digital maturity (reduced set of options)
B	B1	B1c – Who is in charge of managing digital security risk in your enterprise?
B	B2	B2c – If you have a digital security policy, what does it cover?[1]
C	C2	C2b – How often do you assess the possible consequences of digital security incidents that could affect your business activities?[2]
D	D1	D1a - In the past (reference period), did your enterprise have digital security measures in place as a result of a digital security assessment?
E	E1 & E3	E3 – If your enterprise has insurance that covers digital security risks, which of the following risks are covered?[3]
F	F1	F1a – In the past (reference period), did your enterprise perform any of the following practices?

Additions to or removal of questions or response options

The analysis in Section Three of this report(, identified a number of changes that might be made, based on the responses to the pilot, to improve the survey instrument. Some additional response options might be added to certain questions e.g. question D2 could benefit from the option of 'shareholders', 'investors' and/or 'rating agencies'. Changes such as these should be made in line with the likely population of respondents. For instance, the aforementioned additions would be more appropriate were the population of respondents to comprise a large proportion of publicly-traded companies.

Another useful addition might be made to Module A and could involve asking the respondent what role they hold within their enterprise. This would be helpful in better interpreting the results of future survey exercises were they to include more SMEs or cover larger companies that might not have a well-developed risk management department. Another option might be creating a fork whereby those respondents likely to have a sophisticated understanding of risk management are directed down one path, with similarly sophisticated risk management vocabulary used in questions, while those that do not are directed down a path with simpler, non-expert vocabulary.

A final addition might be questions that elicit a more thorough understanding of *why* businesses undertake certain activities. Such questions might provide relevant insights for the development of policies intended to raise awareness, training, insurance take-up or other risk management practices.

In terms of elements to be removed from the survey instrument, the most important one would be the mandatory 'Other (please specify)' response option that appears in questions D1b, D2, E2, E3, E4 and F1c. Forcing respondents to respond to this option when they may not have any other practice to respond with adds a substantial and unnecessary time and effort burden. This was an artifact of the software used to conduct the pilot though its presence should be noted in the event that future work attempts to build on the pilot survey instrument in its current form. The final question in the survey instrument (F1c) asks why training was not provided to directors or business-line managers. Very few respondents (4 out of 80 complete responses) had to respond to this question and, when they did, the answers across response options was relatively consistent (i.e. 'no' including for the

mandatory 'Other (please specify)' option). If this question is to be maintained the options for response may have to be revised. In any case, given that this question was relevant to so few respondents, it may be possible to remove it without an excessive loss of utility.

Simplified language for non-expert respondents

The desired respondent of the pilot survey instrument was risk managers and sample population through FERMA included a relatively high number of risk managers. If the survey instrument were sent to a sample population of companies that included more SMEs it would be less likely that a specific risk manager or risk management department would exist. This would mean that the respondent might have issues understanding the risk management vocabulary used in the survey instrument and the quality of the subsequent responses would suffer. Useful future work would translate risk management terms into terms that would be more accessible to a non-expert audience. This would allow for a future survey instrument to be developed for the majority of the enterprise population. However, a survey instrument targeting risk managers specifically would still remain useful as this population is strategically positioned in many businesses when it comes to risk management. The best way to manage this situation may be to implement a 'fork approach' in Module A, as explained above.

Moving from measuring practices to a maturity model

The framework developed in the course of this project was originally conceived as a way in which to better measure the digital security risk management *practices* of businesses, particularly SMEs. Practices, in their aggregate, provide a snapshot of the overall maturity of the business in question (i.e. maturity as an aggregate of the individual practices). With the framework now in place, and many insights having been gathered over the course of two years, it has become apparent that a useful contribution might be adaptation or extension of this framework that would constitute a model for the assessment of the digital security risk management *maturity* of businesses. Such a model might apply weights to certain practices or rank practices in terms of some metric such as desirability, importance, effectiveness, etc. given the digital intensity, size and industry of the enterprise in question. However, the process of developing this model would have to avoid a situation where a normative view of what constitutes 'mature' or 'not mature' emerges, which may lead to data being generated that confirm the pre-determined concept of maturity.

A benchmarking exercise could be conducted whereby the digital security risk management practices of enterprises with similar characteristics (e.g. same size class, industry and/or digital intensity) are scored against their peers. The actual practices themselves, and whether they represent an appropriate or requisite level of maturity, might thereby be determined for the individual enterprises themselves or from country-to-country.

If this maturity score were to be combined with information on risk factors (i.e. threats, vulnerabilities and incidents), potentially from other reliable sources (e.g. anti-virus companies, technology vendors, computer emergency response teams, etc.), then policymakers would be able to compile a highly-detailed and sophisticated view as to how well-prepared businesses are to effectively manage digital security risks as those risks evolve.

Development of depth measures

A number of the questions lend themselves toward the development of depth measures of certain aspects related to the digital security risk management of the respondent's enterprise. The term 'depth measure' is used to refer to measures that allow assessment of the sophistication of specific practices within the enterprise itself. This is in contrast to what might be termed 'population measures', which are intended more to measure practices of the enterprise in comparison to some larger population. For instance, the data collected with question A4, which is related to indicator A5 'proportion of enterprises by digital intensity', provide a potential measure of the 'depth' of the digital intensity of the respondent's enterprise based nine different digital technologies or their uses. So too does question B2c, which is related to indicator B2 'proportion of enterprises that have a policy in place to manage digital security risk, collects data on nine elements that a digital security policy might cover. The 'depth' of both indicators could be measured based on the number of elements that the enterprise possesses/uses/includes within their policy as a proportion of the total possible elements.

Measuring incidents and their economic impacts

At an earlier stage of this OECD project, the possibility was entertained of a dedicated module to collect data on the frequency and types of digital security incidents incurred by the respondent's enterprise as well as an estimate of their economic impact. It was decided not to pursue this avenue at this stage given the substantial methodological issues that afflict measurement in this area (see the end of Section One of this report for an explanation of these issues). Future work could review methodologies used across a variety of different data sources to measure incidents and their economic impact. Such data sources could include past and existing surveys, anti-virus and security vendors, computer emergency response teams, and national incident reporting systems set-up as a consequence of GDPR/NIS Directive in the EU and reporting obligations created under similar mandatory reporting requirements in other OECD countries. Existing work by the OECD (2015b), IRT-System X (2016) and CRO Forum (2018) might provide useful starting points in this respect.

References

Anderson R., Barton C., Böhme R., Clayton R., van Eeten M. J. G., Levi M., Moore T. and Savage S. (2012), "Measuring the cost of cybercrime", *Workshop on the Economics of Information Security*, http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf

Challice G. (2009), "The Australian Business Assessment of Computer User Security (ABACUS) survey: methodology report", AIC Reports: Technical and Background Paper 32, http://www.aic.gov.au/media_library/publications/tbp/tbp032/tbp032.pdf

CRO Forum (2018), Supporting on-going capture and sharing of digital event data. Achieving a common language to enable understanding of and communicate digital risk/events – Findings from the CRO Forum trial data of a common categorisation methodology for cyber events. www.thecroforum.org/wp-content/uploads/2018/02/201802_CROF_Capture_and_sharing_of_digital_event_data.pdf.

Edwards B., Hofmeyer S. and Forrest S. (2014), "Hype and Heavy Tails: A Closer Look at Data Breaches", Workshop on the Economics of Information Security.

Eurostat (2014), "Community survey on ICT usage and e-commerce in enterprises", http://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Community_survey_on_ICT_usage_in_enterprises

FERMA/European Confederation of Institutes of Internal Auditing (ECIIA) (2017), "At the junction of corporate governance and cybersecurity, available from: http://www.ferma.eu/sites/default/files/2017-09/WEB-FERMA-Brochure2017%2029%20June_0.pdf (accessed 30 September 2017).

Geer D. (2016), "Prediction and the future of cybersecurity", presentation delivered to UNC Charlotte, available from: http://geer.tinho.net/geer.uncc.5x16.txt

Gordon L. A. and Loeb M. P. (2006), "Managing cybersecurity resources: a cost-benefit analysis", McGraw-Hill: New York.

IRT-SystemX (2016), Cyber Risk Governance throughout the value chain and its transfer to the Insurance Market. www.irt-systemx.fr/wp-content/uploads/2017/01/ISX-IC-EIC-transfert-risque-LIV-0401-v10_2016-10-25-ang-v2.pdf

International Standards Organisation (ISO) (2009), ISO 31000 – Risk Management, available from: https://www.iso.org/iso-31000-risk-management.html (accessed 11 October 2018).

Klahr R., Shah J. N., Sheriffs P., Rossington P. and Pestell G. (2017), Cyber Security Breaches Survey 2017: Annex, available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609190/Cyber_Security_Breaches_Survey_2017_annex_PUBLIC.pdf (accessed 14 August 2017).

OECD (2011), "Enhancing Consumer Policy Making: The Role of Consumer Surveys", DSTI/CP(2011)3/FINAL, available at:

http://search.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP282011293/FINAL.

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. http://dx.doi.org/10.1787/5k4dq3rkb19n-en

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

OECD (2015b), 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.

Ponemon Institute (2016), "State of Cybersecurity in Small and Medium-Sized Businesses", https://keepersecurity.com/assets/pdf/The_2016_State_of_SMB_Cybersecurity_Research_by_Keeper_and_Ponemon.pdf

Rantala R. (2005), "Cybercrime against businesses", US Department of Justice, Bureau of Justice Statistics, https://www.bjs.gov/index.cfm?ty=pbdetail&iid=769

Richards K. (2009), "The Australian Business Assessment of Computer User Security: a national survey", AIC Reports, Research and Policy Series 102.

Romanosky S. (2016), "Examining the costs and causes of cyber incidents", Journal of Cybersecurity, 2016, 1–15 doi: 10.1093/cybsec/tyw001

Romanosky S., Ablon L., Kuehn A. andJones T. (2017), "Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?", Workshop on the Economics of Information.

Taleb N. N. (2015), "On the Super-Additivity and Estimation Biases of Quantile Contributions", www.fooledbyrandomness.com/longpeace.pdf

World Economic Forum (2016), "Advancing cyber resilience: Principles and tools for boards", available from: https://www.zurich.com/en/knowledge/articles/2017/02/advancing-cyber-resilience-wef-report (accessed 30 September 2017).

Annex A. Surveys covered in stock-taking exercise

Survey name	Organisation(s) that undertook and/or sponsored survey	Number of questions categorised
Official surveys		
The Australian Business Assessment of Computer User Security (ABACUS) Survey	Australian Institute of Criminology	29
Canadian Survey of Cyber Security and Cybercrime	Statistics Canada; Investment Science and Technology Division	35
Community survey on ICT usage and e-commerce in enterprises	National statistical offices of relevant EU member countries	12
Computer Crime and Security Survey	Computer Security Institute and Federal Bureau of Investigation	14
Information Security Breaches Survey	HM Government, U.K.; conducted by PWC	77
National Computer Security Survey	US Department of Justice, Department of Homeland Security, RAND Corporation	30
National Small Business Study	National Cyber Security Alliance; sponsored by Symantec; conducted by JZ Analytics	84
OECD model surveys on ICT access and usage by businesses	National statistical offices of relevant OECD member countries	7
Survey on Information Security	Korea Internet and Security Agency; Ministry of Science, ICT and Future Planning	25
Unofficial surveys		
Cybersecurity survey	Confédération générale du patronat des petites et moyennes entreprises (CGEPME) [The General Confederation of Employers of Small and Medium Enterprises]	18
Risk Management Benchmarking Survey	Federation of European Risk Management Associations in collaboration with XL Group, EY, Zurich, Marsh and AXA Corporate Solutions	5
State of Cybersecurity in Small and Medium-sized Businesses	Ponemon Institute sponsored by Keeper Security	43
Study of the Impact of Cybercrime on Businesses in Canada	International Cyber Security Protection Alliance (ICSPA)	20
Survey on Cybersecurity for SMEs and intermediate-sized enterprises with a digitised production method (or to have a digitised production method)	Alliance Industrie du Futur [Industry of the Future Alliance] and E□cole d'Inge□nieurs, Te□le□com ParisTech [Engineering School, Telecom ParisTech]	15

Annex B. Pilot Survey Instrument

PILOT SURVEY INSTRUMENT ON DIGITAL SECURITY RISK MANAGEMENT PRACTICES IN BUSINESSES

Version sent to FERMA for pilot testing.

11 June 2018

This survey is intended to assess the digital security risk management maturity of businesses. It will provide data that helps businesses benchmark their relative maturity against peers. It will also provide data to help inform government policies intended to raise the level of digital security risk management in OECD countries.

The purpose of digital security is to preserve the confidentiality, availability and integrity of the activities of an organisation that rely on digital technologies and data. The management of digital security is done through the management of digital security risk. Through a governance structure, this process involves the assessment of digital security risk, the treatment of these risks and the overall monitoring, evaluation and refining of these processes.

Risk is a way of representing the uncertainty of achieving a particular objective. Digital security risk is the expression used to describe risk that a business faces when it uses digital technologies to fulfil its economic and social objectives. This risk comes from vulnerabilities in digital technologies that could be exploited by a range of threats. Digital security incidents that arise from these threats and vulnerabilities ultimately affect the confidentiality, integrity and availability of the activities of the business.

The person who responds to the questionnaire should have an understanding of the business activities and economic and social risks that the business faces and not simply someone who is in charge of the information communication technologies (ICTs). Depending on the business size, this person may have the title:
- Chief Risk Officer
- Chief Risk Manager
- Internal Auditor
- Accountant
- Risk (and Audit) Management Committee Chair/Member
- Chief Executive Officer
- Chief Operating Officer
- Chief Finance Officer

If your enterprise is part of a group, please answer all further questions about your enterprise only for its own activities.

Section A. Basic information on your enterprise

A1 - Proportion of enterprises by geographic location
of the total number of enterprises

QA1a. In (REFERENCE PERIOD), was your enterprise part of an enterprise group?

A group consists of two or more legally defined enterprises under common ownership. Each enterprise in the group can serve different markets, as with national or regional subsidiaries, or serve different product markets. The head office is also part of an enterprise group.

Yes	1	Follow to QA1b
No	2	Skip to QA1c
Does not know	98	
Did not answer	99	

QA1b. In which country is the head office of your group located? _____

QA1c. In which country is your enterprise located? _____

A2 - Proportion of enterprises by size
of the total number of enterprises

QA2 - How many persons employed worked in your enterprise in (REFERENCE PERIOD)?
Persons employed include employees, employers, own account workers, members of producers' cooperatives and contributing family workers. A person employed may be paid or unpaid (for instance, a contributing family worker may be paid in kind rather than cash). An employee may be employed on a short-term, casual or seasonal basis.

A	Under 10	1
B	10 to 49	2
C	50 to 249	3
D	250 to 499	4
E	500 to 999	5
F	1 000 to 2 499	6
G	2 500 to 4 999	7
H	5 000 to 9 999	8
I	10 000 or more	9
J	Does not know	98
K	Did not answer	99

A3 - Proportion of enterprises by economic activity

of the total number of enterprises

QA3 – What is the main economic activity of your enterprise?

A	Agriculture, forestry and fishing	1
B	Mining and quarrying	2
C	Manufacturing	3
D	Electricity, gas, steam and air conditioning supply	4
E	Water supply; sewerage, waste management and remediation activities	5
F	Construction	6
G	Wholesale and retail trade; repair of motor vehicles and motorcycles	7
H	Transportation and storage	8
I	Accommodation and food service activities	9
J	Information and communication	10
K	Financial and insurance activities	11
L	Real estate activities	12
M	Professional, scientific and technical activities	13
N	Administrative and support service activities	14
O	Education	15
P	Human health and social work activities	16
Q	Arts, entertainment and recreation	17
R	Other service activities	18
S	Does not know	98
T	Did not answer	99

A4 - Proportion of enterprises by turnover
of the total number of enterprises

QA4 – Please provide the turnover of your enterprise for the most recent budget year.

Year : _____

Amount : _____

A5 - Proportion of enterprises by digital intensity
of the total number of enterprises

QA5 - In the last (REFERENCE PERIOD), did your enterprise use any of the following digital technologies and/or applications?

		Yes	No	Does not know	Did not answer
A	Broadband connection	1	2	98	99
B	Website for your business	1	2	98	99
C	Intranet (e.g. internal or private network)	1	2	98	99
D	Enterprise resource planning (ERP) software package	1	2	98	99
F	Customer relation management (CRM) software package	1	2	98	99
G	Social media accounts (e.g. Facebook, Twitter, LinkedIn)	1	2	98	99
H	E-commerce platforms and solutions (e.g. online payment and ordering)	1	2	98	99
I	Cloud computing services	1	2	98	99
J	Voice Over Internet Protocol (VOIP) services (e.g. Skype)	1	2	98	99

Section B. Digital security risk governance

B1 - Proportion of enterprises that have responsibilities for digital security risk allocated to a specific role within the organisation
of the total number of enterprises

QB1a - Is there currently a department or person employed primarily in charge of the overall risk management of your enterprise?

Yes	1	Follow to QB1b
No	2	
Does not know	98	Skip to QB1c
Did not answer	99	

QB1b - Is this department or person also in charge of managing digital security risk of your enterprise?

Yes	1
No	2
Does not know	98
Did not answer	99

QB1c - Who is in charge of managing digital security risk of your enterprise?

A	Chief Executive Officer (CEO)	1
B	The business line manager of each business activity	2
C	Chief Information Officer (CIO) or IT manager	3
D	Chief Information Security Officer (CISO)	4
E	Chief Security Officer (CSO)	5
F	Risk Manager	6
G	Other persons employed that are not in management position	7
H	External service provider	8
I	Other (please specify)	9
J	Nobody	10
K	Does not know	98
L	Did not answer	99

QB1d - Who is responsible for deciding the acceptable level of digital security risk for each business activity?

A	Chief Executive Officer (CEO)	1
B	The business line manager of each business activity	2
C	Chief Information Officer (CIO) or IT manager	3
D	Chief Information Security Officer (CISO)	4
E	Chief Security Officer (CSO)	5
F	Risk Manager	6
G	Other persons employed that are not in management position	7
H	Other (please specify)	8
I	Nobody	9
J	Does not know	98
K	Did not answer	99

B2 - Proportion of enterprises that have a policy in place to manage digital security risk
of the total number of enterprises

QB2a - Does your enterprise have a written or unwritten digital security policy?

Yes	1	Follow to QB2b
No	2	
Does not know	98	Skip to QB4
Did not answer	99	

QB2b - Is the digital security policy:

Written in a document	1
A set of unwritten rules and practices	2
Does not know	98
Did not answer	99

QB2c - Does the digital security policy cover any of the following?[18]

		Yes	No	Does not know	Did not answer
A	Roles and responsibilities for digital security risk management in the organisation	1	2	98	99
B	Processes to enable co-operation and for reporting within the organisation	1	2	98	99
C	Audit, review and cycle of improvement	1	2	98	99
D	Risk assessment	1	2	98	99
E	Processes to decide how much risk should be taken, reduced, transferred and avoided	1	2	98	99
F	Decision on digital security measures	1	2	98	99
G	Business continuity and resilience	1	2	98	99
H	Digital security risk transfer	1	2	98	99
I	Awareness raising and training	1	2	98	99

B3 - Proportion of enterprises that have a process in place to monitor and review digital security risk management
of the total number of enterprises

QB3 - How often does your enterprise undertake the following monitoring activities?

		Yearly	Every two years	More than every two years	Does not undertake	Does not know	Did not answer
A	Assess the performance of the enterprise against a digital security policy	1	2	3	4	98	99
B	Report internally the results of previous assessment	1	2	3	4	98	99
C	Update policy and practices based on results of digital security audit and review process	1	2	3	4	98	99

B4 - Proportion of enterprises that had structures or processes in place to enable cooperation and for reporting on digital security risk management within the enterprise
of the total number of enterprises

QB4 - In the last (REFERENCE PERIOD), did your enterprise organise physical or virtual meetings with staff in charge of business management and ICT, to determine digital security risk exposure?

Yes	1
No	2
Does not know	98
Did not answer	99

Section C. Digital security risk assessment practices

C1 - Proportion of enterprises that assess digital security risk as part of the overall enterprise risk management

of the total number of enterprises

QC1a - Does your enterprise have a regular overall process to assess the risk to which its business activities are exposed?

Yes	1	Follow to QC1b
No	2	
Does not know	98	Skip to QC2a
Did not answer	99	

QC1b - Is digital security risk assessment part of this overall risk assessment process?

Yes	1
No	2
Does not know	98
Did not answer	99

C2 - Proportion of enterprises that regularly take specific actions as part of the digital security risk assessment

of the total number of enterprises

QC2a - Who carries out the following activities as part of digital security risk assessment for your enterprise?

		Business managers	IT managers	Other employees	Outsourced	Nobody	Does not know	Did not answer	
A	Regular assessment of the dependency of business activities on digital technologies and data	1	2	3	4	5	98	99	
B	Regular assessment of the possibility of digital security incidents	1	2	3	4	5	98	99	Follow to QD1a except If "1", "2", "3" or "4" in item C then follow to QC2b
C	Regular assessment of the consequences of possible digital security incidents on business activities	1	2	3	4	5	98	99	

QC2b - How often do you assess the possible consequences of digital security incidents that could affect your business activities?

A	Daily	1
B	Weekly	2
C	Monthly	3
D	Yearly	4
E	Other (specify)	5
F	Does not know	98
G	Did not answer	99

Section D. Digital security risk reduction practices

D1 - Proportion of enterprises that took risk reduction measures
of the total number of enterprises

QD1a - In the last (REFERENCE PERIOD), did your enterprise have digital security measures in place as a result of a digital security assessment?

Yes	1	Follow to QD1b
No	2	
Does not know	98	Skip to D2
Did not answer	99	

QD1b – Do the digital security measures in place aim to do any of the following?

		Yes	No	Does not know	Did not answer
A	Protect the activities against potential threats	1	2	98	99
B	Change the business activity (e.g by redesigning or operating it differently)	1	2	98	99
C	Cope with the occurrence of incidents	1	2	98	99
D	Other (please specify)	1	2	98	99

D2 - Proportion of enterprises that share information on threats, vulnerability, incidents and risk management practices or security measures
of the total number of enterprises

QD2 - Do you share information on digital security threats, vulnerability, incidents, risk management practice or security measures with the following stakeholders outside your enterprise:

		Yes	No	Does not know	Did not answer
A	IT suppliers (e.g. software, Internet service providers or digital service vendors)	1	2	98	99
B	Other Suppliers	1	2	98	99
C	Customers	1	2	98	99
D	Business partners	1	2	98	99
E	Law enforcement agencies	1	2	98	99
F	Computer Emergency Response Teams (CERTs)	1	2	98	99
G	Other government bodies in charge of receiving data breach notifications	1	2	98	99
H	Information Sharing and Analysis Centres (ISACs) or equivalent	1	2	98	99
I	Insurance providers	1	2	98	99
J	Other (please specify)	1	2	98	99

Section E. Digital security risk transfer practices

E1 - Proportion of enterprises that use insurance to transfer digital security risk[19]
of the total number of enterprises

QE1 - Does your enterprise have any insurance policies that cover digital security risk?

Yes	1	Skip to QE3
No	2	Follow to QE2 and Skip to QE4
Does not know	98	Skip to QE4
Did not answer	99	

E2 - Proportion of enterprises that did not purchase an insurance policy, by reason for not adopting them
of the total number of enterprises

QE2 – What were the reasons for not taking out an insurance policy covering digital security risk?

		Yes	No	Does not know	Did not answer
A	High costs associated with such insurance	1	2	98	99
B	Conditions in policies too restrictive	1	2	98	99
C	Insufficient coverage	1	2	98	99
D	Such insurance is not available in the country	1	2	98	99
E	Such insurance is not required in the enterprise	1	2	98	99
F	Not aware that digital security risk can be covered by insurance	1	2	98	99
G	Use other means to transfer the risk	1	2	98	99
H	Other (please specify)	1	2	98	99

E3 - Proportion of enterprises that transfer digital security risks through an insurance policy, by type of risks transferred
of the total number of enterprises

QE3 - Which of the following risks are covered through your insurance policy/policies?

		Yes	No	Does not know	Did not answer
A	Damage to physical assets	1	2	98	99
B	Financial losses	1	2	98	99
C	Additional ICT expenditure (e.g. restoration of hardware, software and data)	1	2	98	99
D	Business disruption and system failure (e.g. loss of productive time)	1	2	98	99
E	Reputation losses	1	2	98	99
F	Third-party liability (e.g. fines, legal expenses)	1	2	98	99
G	Incident notification expenses	1	2	98	99
H	Theft and fraud	1	2	98	99
I	Other (please specify)	1	2	98	99

E4 - Proportion of enterprises that adopt other risk transfer practices
of the total number of enterprises

QE4 - Does your enterprise transfer digital security risk via any of the following practices?

		Yes	No	Does not know	Did not answer
A	Legal contract other than insurance policy	1	2	98	99
B	Warranties	1	2	98	99
C	Outsourcing	1	2	98	99
D	Other (please specify)	1	2	98	99

Section F. Digital security risk management awareness and training

F1 - Proportion of enterprises that adopted awareness-raising and training practices on digital security risk management
of the total enterprises

QF1a - In the last (REFERENCE PERIOD), did your enterprise perform any of the following practices?

		Yes	No	Does not know	Did not answer	
A	Refer to digital security risks in employment contracts	1	2	98	99	
B	Discuss digital security risks at business unit meetings	1	2	98	99	
C	Give performance incentives to persons employed due to behaviour that reduced digital security risk	1	2	98	99	
D	Provide mandatory or optional training on managing digital security risk (e.g. online courses, workshops, seminars, conferences or training provided through internal meetings)	1	2	98	99	If "Yes", follow to QF1b

QF1b - Who was the training provided to:

		Yes	No	Does not know	Did not answer	
A	Directors	1	2	98	99	If "No", follow to QF1c
B	Business-line managers	1	2	98	99	
C	Security department staff	1	2	98	99	
D	IT department staff	1	2	98	99	
E	Staff from other departments (please specify)	1	2	98	99	
F	External contractors and partners	1	2	98	99	

QF1c - What were the reasons for not providing training in digital security risk management to directors or business line managers?

		Yes	No	Does not know	Did not answer
A	High costs associated with such training	1	2	98	99
B	Lack of organisation or supplier that provides such training	1	2	98	99
C	Directors or business line managers are not responsible for digital security risk management	1	2	98	99
D	Digital security is a matter of IT personnel	1	2	98	99
E	Other (please specify)	1	2	98	99

Annex C. Summary of cognitive testing and key findings

Cognitive interviews were carried out between March 26 and April 11, 2018 in three municipalities in Brazil: São Paulo, Recife and Porto Alegre. A total of 16 face-to-face interviews were carried out with selected respondents who were employed at enterprises of different sizes, economic activities and geographic locations (Table A C.1.). In cases where it was not possible to conduct interviews in prepared interview rooms, respondents were contacted on-site. All interviews – whether in interview rooms or on-site – were fully recorded and internationally accepted ethical recommendations were applied.

The concept of size of enterprises considers small (10 to 49 employed persons), medium (50 to 249 employed persons) and large enterprises (250 or more employed persons). Microenterprises, those with 1 to 9 employed persons, were not included in the scope of the cognitive testing. As for the concept of employed persons, it refers to those with or without employment contracts who are remunerated directly by the enterprise. The number of employed persons included salaried employees, freelancers paid directly by the company, employees and associates, family members and temporary workers. Third parties and consultants were not included.

The type of economic activity of the companies interviewed (see table below) was classified according to the International Standard Industrial Classification of All Economic Activities (ISIC 4.0) and referred only to legally constituted enterprises in Brazil categorised and registered in official registries.

Target respondents were employed persons with knowledge or understanding of the economic and social risks faced by the organisation, such as risk managers. In most cases, if there was no employed person who was explicitly assigned the responsibility for risk management within the enterprise, the interview was carried out with owners, CEOs, senior business managers or other persons with an overall view of the economic or commercial side of the business in question.

In the particular case of Brazil, it is worth noting that several respondents considered digital security risks primarily as a technical matter, and indicated that technical staff (such as IT managers) were the best respondents within their enterprises to answer questions about digital security risk management decisions. Although the questionnaire is aimed at small and medium enterprises (SMEs), some large companies were interviewed, in order to control for the influence of size and complexity of the organisation on the overall understanding of the questionnaire.

Table A C.2. Cognitive interviews carried out by Cetic.br

Interview	Municipality	Interview location	Economic activity	Size of business (employed persons)	Respondent's position
1	São Paulo	Interview room	Real estate	50 to 249	Infrastructure coordinator
2	São Paulo	Interview room	Transportation and storage	50 to 249	Administrative manager
3	São Paulo	Interview room	Arts, entertainment and recreation	10 to 49	Operations manager
4	São Paulo	Interview room	Information and communication	50 to 249	Financial and infrastructure manager
5	São Paulo	Interview room	Arts, entertainment and recreation	10 to 49	Project manager
6	São Paulo	On-site	Transportation and storage	1,000 or more	Risk manager
7	São Paulo	Interview room	Wholesale and retail trade	10 to 49	Owner
8	São Paulo	Interview room	Arts, entertainment and recreation	50 to 249	IT manager
9	São Paulo	On-site	Real estate	1,000 or more	IT manager
10	São Paulo	On-site	Accommodation and food service	500 to 999	IT manager
11	Recife	On-site	Wholesale and retail trade	1,000 or more	IT manager
12	Recife	On-site	Real estate	10 to 49	Managing partner
13	Porto Alegre	On-site	Accommodation and food service	10 to 49	Owner
14	Porto Alegre	On-site	Construction	50 to 249	IT manager
15	São Paulo	On-site	Information and communication	10 to 49	Infrastructure manager
16	São Paulo	On-site	Construction	250 to 499	IT manager

KEY FINDINGS

In general, most questions and concepts presented in the questionnaire were associated with a rather technical or incident management-related perspective, even among respondents who had no IT background. Examples provided by the interviewees, such as data breaches and recent cases of ransomware attacks, reinforced this perception. Media coverage about such security incidents in other companies also seems to influence how respondents frame the debate about digital security risk management (DSRM).

Another relevant aspect that clearly emerged from the cognitive interviews was that companies appear to have very low maturity in terms of implementing DSRM policies. Among the enterprises interviewed, the practices reported were put in place in a more reactive manner, rather than through a systematic and regular process of DSRM. Practices, information sharing and internal awareness-raising actions were directly associated with the occurrence of concrete security incidents rather than with an organisational culture of risk management.

According to respondents, digital security risk management is combined with many organisational practices that permeate the routine of organisations, rather than being configured as a separate process. It is important for professionals in charge of corporate information security to raise awareness of all types of risks involved in the digital

environment; otherwise, DSRM will be mainly understood as an IT matter. In recent years, issues related to digital risk have increasingly been discussed in the media, gaining the appreciation of the general public and specialised media. As a result, the task of providing information about best practices and risks has become easier, especially in terms of alerting owners and managers to the necessity of more investments in security technology. In other words, in most cases DSRM is seen as a technical issue, not as a management issue.

It is worth noting that problems of comprehension increased among SMEs, especially those that did not have IT teams. For larger enterprises and those with experts in the field, the level of understanding of the concepts and definitions underlying the questions was noticeably higher. Nevertheless, it is important to note that most respondents were aware of digital incidents such as ransomware and data leaks, which have been much discussed in the media in recent years.

Responses also varied according to the level of digital intensity across different economic activities. In general, the questionnaire performed well among large companies with a more comprehensive understanding of concepts such as risk management and risk transfer. However, even the large enterprises interviewed assigned digital security practices to IT departments. This decision might have influenced how they answered the questions. Respondents from businesses that use personal data more intensively expressed more concern about digital risks. Most companies showed concern about reputation damage and ransomware attacks, but did not relate these risks and their effects to the core business of the organisations. The perception of digital risks as an exclusively technical matter seems to lead to uncoordinated levels of DSRM practices. In fact, the present study did not find any companies with structured processes that take the results of digital risk assessment into account in their managerial actions.

Departments dedicated or in charge of DSRM were not found in the enterprises selected to participate in the cognitive interviews. IT departments (or CIOs, CTOs or even CFOs) were mostly responsible for managing digital risks. In addition, most companies had no written DSRM policies. Here again, the size of the enterprise matters: Larger enterprises were more likely to have written and disseminated DSRM policies. In most cases, companies reported informal practices, such as warnings or general rules about expected behaviours in case of security incidents. When practices related to DSRM did exist, they were merged into more routinised processes and were not recognised as originating in risk assessment. Overall, it was difficult for respondents to connect digital risks to social and economic risks of the organisation. Technical aspects of dealing with digital risks were seen as separate from the main processes in the organisation, and IT departments had a narrower view of their role within the organisational structure.

Specific variations in different regional locations were not noticeable. Differences in terms of economic activities and size appeared to be more relevant to influencing responses: Companies from the information and communication segment, even small ones, had a stronger tendency to adopt DSRM practices; in contrast, one large company that was part of a restaurant franchise was one of the most structured organisations in terms of IT activities. SMEs whose core business did not rely heavily on IT technologies showed a low level of DSRM. Market segment and the complexity of the business may influence the level of adoption of information and communication technologies in the company's internal and external processes, but not necessarily leads to the establishment of DSRM practices.

Notes

[1] Respondents had their head office in one of fifteen countries. The respondents themselves were based in one of twelve countries.

[2] The full list of surveys can be found in Annex A

[3] The GDPR and NIS Directives in the European Union, as well as new legislation for mandatory breach notification in countries such as Australia and others, might provide new and potentially useful sources of incident data.

[4] Future work could build on the solid foundation set by the Cyber Breaches Survey in the United Kingdom.

[5] This report proposes the concept of 'Three Lines of Defense in the Digital Context' for effective digital security risk governance within businesses. While the full three lines and associated roles may not be present, and thus practical, in micro and small businesses, the principle that they uphold of clear allocation of responsibility to specific roles remains important.

[6] **Identified**: i.e. risk factors are recognised, often on the basis of experience, historical data, theoretical analysis, experts' views and opinions, etc.; **Analysed**: i.e. the risk is understood and the level of risk is determined. As noted above, this level is often expressed in terms of likelihood and impact on the economic and social activity at stake; and **Evaluated**: i.e. the risk is compared to the acceptable level of risk relative to the activity and the economic and social objectives and benefits expected from it.

[7] Following the European Union definition of an SME as having headcount less than 250 employees or annual turnover below EUR 50,000,000.

[8] N = 68

[9] In the future, rephrasing of this question as "managing the digital security of the enterprise" would be more appropriate.

[10] N = 67

[11] N = 64

[12] Slight rephrasing of this question to include 'the' before 'digital security risk assessment' is advised in the future.

[13] All percentages in this paragraph refer to a sample n = 65.

[14] The full list of affected questions includes: D1b, D2, E2, E3, E4 and F1c.

[15] There are no such centres in Europe, where the respondents' enterprises were based, which explains this low proportion.

[16] This figure combines the outputs for questions related to indicator E1 and E4.

[17] N = 44

[18] An additional response category could be included to capture personal data protection.

[19] This section could also include an indicator to capture enterprises that attempted to make a claim on their insurance policy after the digital security incident(s) in (REFERENCE PERIOD).